Tallinna Ülikool
Informaatika Instituut

Martin Palm

INFOTURVE VOSK PÕHIMÕTTE RAKENDAMISEL AS EESTI TELEKOMI NÄITEL

Magistritöö

Juhendaja: PhD Andro Kull

Autor: ……..... „ … …….. 2015.a.
Juhendaja: ……..…… „ … …….. 2015.a.
Instituudi juhataja: ……..……..... „ … …….. 2015.a.

Tallinn 2015

AUTORIDEKLARATSIOON

Deklareerin, et magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

…… ……..

(kuupäev) (autor)

LIHTLITSENTS LÕPUTÖÖ REPRODUTSEERIMISEKS JA LÕPUTÖÖ ÜLDSUSELE KÄTTESAADAVAKS TEGEMISEKS

Mina MARTIN PALM (sünnikuupäev: 12.10.1987)

(autori nimi)

1. annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
   INFOTURVE VOSK PÕHIMÕTTE RAKENDAMISEL AS EESTI TELEKOMI NÄITEL

   (*lõputöö pealkiri*)

   mille juhendaja on ANDRO KULL,

   (*juhendaja nimi*)

   säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.
2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

(digitaalne) allkiri ja kuupäev

SISUKORD

MÕISTED JA LÜHENDID 5
JOONISED JA TABELID 8
SISSEJUHATUS 9
1 KIRJANDUSE ÜLEVAADE 11
2 TEOREETILINE ALUS 19
2.1 VOSK nähtus 19
2.2 VOSK kasutegurid 21
2.3 VOSK arhitektuurilised ja tehnoloogilised lahendused 23
2.4 VOSK infoturbe ohud 26
2.5 VOSK infoturbe tagamise meetmed 32
3 UURING 39
3.1 Ülevaade organisatsioonist AS Eesti Telekom 39
3.2 Metoodika 40
3.3 Tulemused 40
3.4 Analüüs 50
4 ARUTELU 58
KOKKUVÕTE 62
SUMMARY 64
KASUTATUD KIRJANDUS 66
LISA 1: AS EESTI TELEKOMI STRUKTUUR 71
LISA 2: CISCO ANYCONNECT MOBIILSETELE SEADMETELE FUNKTSIONAALSUSE KIRJELDUS 72
LISA 3: CITRIX XENMOBILE FUNKTSIONAALSUSE KIRJELDUS 74

MÕISTED JA LÜHENDID

BYOD (*Bring Your Own Device*) – vt VOSK.

DMZ (*Demilitarized Zone*) – usaldatavat võrku ebausaldatavast võrgust "neutraalse tsoonina" eraldav füüsiline ja/või loogiline alamvõrk (Veldre, Hanson, Laur, Buldas, & Krasnosjolov, 2015).

DTLS (*Datagram Transport Layer Security)* – "datagrammitranspordikihi turve" protokolli TLS variant; peab lahendama pakettide kaotsimineku ja järjestuse muutumise, välistades sõnumite pealtkuulamise, muutmise ja võltsimise (Veldre et al., 2015).

EMM (*Enterprise Mobility Management*) – ettevõtte mobiilsuse haldus.

IPsec (*IP Security*) – "IP turve" on TCP/IP-mudeli (neljakihiline standardmudel: 1. lülikiht, 2. võrgustikukiht, 3. transpordikiht, 4. rakenduskiht) võrgustikukihis töötav (ja seega ka kõrgemaid kihte kaitsev) standardne protokollistik ja raamstruktuur otspunktide vaheliseks IP-võrgusuhtluse turbeks krüptograafiliste vahenditega; rakenduste jaoks läbipaistev, tagab iga IP-paketi autentimise ja krüpteerimise andmevoos (Veldre et al., 2015).

IPTV (*Internet Protocol Television*) – televisiooniteenuste standardne voogedastus pakettkommutatsioonvõrgu (kohtvõrgu või interneti) kaudu IP-protokollistiku abil (Veldre et al., 2015).

Juursertifikaat – PKI hierarhia tipus olev (enda signeeritud) sertifikaat (Veldre et al., 2015).

MAM (*Mobile Application Management*) – mobiilseadmete rakendusprogrammide haldus.

MCM (*Mobile Content Management*) – mobiilsedemete infosisu haldus.

MDM (*Mobile Device Management*) – „mobiilseadmete haldus“: lisaks korralduslikele arvestus- ja turvameetmetele hõlmab tehnilisi meetmeid tarkvara, andmete ja konfiguratsioonide kaugseadmiseks ja –seireks (Veldre et al., 2015).

MITM *attack* (*Man-In-The-Middle attack*) – „vahendusrünne“ on suhtluspoolte teabevahetust manipuleeriv rünne, eeskätt autentimisprotseduuri aktiivne pealtkuulamisrünne, mille puhul ründaja valikuliselt muudab edastatavaid andmeid ja teeskleb tundliku teabe saamiseks üht sidepartneritest; kui ründaja vahetab ühe poole avaliku võtme enda omaga, saab ta dekrüpteerida tollele saadetud krüptogrammi; lühidalt on tegemist ründega, mille sooritaja on võimeline salaja lugema, lisama ja muutma sõnumeid kahe poole vahel (Veldre et al., 2015).

Oht – süsteemi või organisatsiooni kahjustada võiva tulevase soovimatu sündmuse võimalik põhjus, nt objekt, aine, isik vm (Veldre et al., 2015).

OS (*Operating System*) – operatsioonisüsteem on muude programmide käitust reguleeriv ja riistvaraga suhtlemist vahendav tarkvarakomplekt, mille laadib alglaadur arvuti käivitamisel ja mille põhiosa (tuum) jääb resideerima; jaotab programmidele ressursse (protsessoriaega, põhimälu, välisseadmeid), haldab andmeid, korraldab andmevahetust ja võrgusuhtlust, rakendab mõningaid turvameetmeid, liidestab kasutajaga, väljastab teateid ning täidab muid juhtimisfunktsioone; tüüp määrab kasutatavusnõuded muule tarkvarale ja andmetele. Levinud operatsioonisüsteemi(pere)d on näiteks Linux/Unix, Windows, Mac OS, iOS, Android. (Veldre et al., 2015).

Pilveteenus – pilveteenusteks nimetatakse selliseid IT-teenuseid, mida pilvandmetöötluse serverite omanikud pakuvad üle interneti (Vallaste, 2015).

PKI (*Public Key Infrastructure*) – „avaliku võtme taristu“ on IT vahendite, inimeste, poliitikate ja protseduuride süsteem avalike võtmete sidumiseks kasutajate identiteetidega, tavaliselt digitaalsertifikaatide abil (Veldre et al., 2015).

Risk – infoturbe kontekstis on risk ohu potentsiaal ära kasutada mingi vara või varade rühma nõrkusi ja tekitada seeläbi organisatsioonile kahju; mõõdetakse sündmuse võimalikkuse ja tagajärgede kombinatsiooniga (Veldre et al., 2015).

SaaS (*Software as a Service*) – „tarkvara teenusena“ on tarkvara tarnimise meetod, kus klient saab kaugpääsuga kasutada teenuseandja rakendusi; pilvteenuste liik, mille puhul pilvteenuse kliendile antav pilvvõimete tüüp on rakendusevõime (Veldre et al., 2015).

Sandbox – „aedik“ ehk võimalikke ohtlikke toiminguid ja funktsioone tõkestav keskkond ebausaldatavaist allikaist pärit koodi või programmi käituseks (Veldre et al., 2015).

SSL (*Secure Sockets Layer*) – „turvasoklikiht“ on krüpteerimisprotokoll, protokolli TLS eelkäija (Veldre et al., 2015).

TLS (*Transport Layer Security*) – "transpordikihi turve" protokolli SSL variant, milles kasutatakse avaliku võtmega krüptograafilist süsteemi; võimaldab enne andmevahetust kliendi ja serveri vastastikku autentimist ning leppida kokku krüpteerimisalgoritmi ja võtmed (Veldre et al., 2015).

Virtuaalmasin – tegeliku või hüpoteetilise arvuti arhitektuuri ja funktsioonide emuleering (Veldre et al., 2015).

VOSK (Võta Oma Seade Kaasa) – olukord, kus isiklikke IT-vahendeid kasutatakse nii eraelu kui ka töö kontekstis (Beckett, 2014; Caldwell, Zeltmann, & Griffin, 2012; Disterer & Kleiner, 2013; Longo, 2013); poliitikasäte, mis lubab töö- või õppekohal kasutada isiklikke seadmeid (Veldre et al., 2015).

VPN (*virtual private network*) – virtuaalne privaatvõrk on võrk, milles IT-süsteeme ühendavad läbi ebaturvalise avaliku võrgu (näiteks interneti) kulgevad krüptograafia vahenditega loodud turvalised tunnelid; ettevõtted kasutavad VPN-tehnoloogiat partnerivõrkude ja ulatuslike sisevõrgu osade loomiseks (Veldre et al., 2015).

JOONISED JA TABELID

JOONISED

Joonis 1. Cisco kujunemine nn virtuaalseks ettevõtteks 21
Joonis 2. Arhitektuurilised ja tehnoloogilised lahendused 23
Joonis 3. Mida ründetarkvara mobiilses seadmes teeb?. 29
Joonis 4. Võltsitud rakenduste pood Venemaal 30
Joonis 5. Cisco AnyConnect kasutajaliides Apple iOS ja Android operatsioonisüsteemidel. . 42
Joonis 6. Citrix XenMobile kasutajaliides administraatorile 43
Joonis 7. Citrix XenMobile turvapoliitikate haldamine administraatori kasutajaliideses. 44
Joonis 8. Citrix XenMobile tüüparhitektuuri joonis. 44
Joonis 9. ISO27k riskide register – maatriks. 46
Joonis 10. RISK IT raamistiku riskistsenaariumi komponendid. 50
Joonis 11. Tüüpiline kikilips-diagramm. 51
Joonis 12. Kikilips-diagramm VOSK infoturbe intsidendi kohta. 56
Joonis 13. AS Eesti Telekomi struktuur. 71

TABELID

Tabel 1. Kirjanduse ülevaade 17
Tabel 2. Erinevate tehnoloogiate selgitused 26
Tabel 3. MDM süsteemi tüüpilised funktsioonid 35
Tabel 4. ISO27k riskide register – tüüpinfo 46
Tabel 5. ISO27k riskide register – riskide ja võimalike mõjude kirjeldused 47
Tabel 6. ISO27k riskide register – tõenäosused, mõjud, meetmed ja kommentaarid 49

SISSEJUHATUS

Tehnoloogia areng ja muutused inimeste käitumisharjumustes on tekitanud olukorra, kus üha enam töötajaid kasutab töö tegemiseks isiklikke IT-vahendeid (nt süle- ja tahvelarvutid, mobiil- ja nutitelefonid). Tegemist on globaalse ja kiiresti areneva nähtusega, mida nimetatakse „Võta Oma Seade Kaasa“ ehk VOSKiks. VOSKi võimaldamine võib ettevõttele palju kasu tuua (nt suurem produktiivsus, töötajate mobiilsus ja rahulolu, madalamad kulud), aga püstitab selle IT juhtidele ja infoturbe eest vastutajatele ka suure väljakutse – kuidas tagada isiklike seadmete kasutamise võimaldamise juures piisav infoturve?

Olukorra muudavad infoturbe tagamise aspektist keeruliseks mitmed tegurid: lai kontekst; kiired arengud; ühtsete standardite puudumine; seadmete paljusus ja suur variatiivsus, vähearenenud turvaelemendid; veebiteenuste ja -rakenduste suur populaarsus; töötajate vähene teadlikkus, hoolimatu või pahatahtlik käitumine jm. Ilma VOSKi võimaldamiseta on infoturbe tagamine ettevõtte jaoks lihtsam, sest kui töötajad kasutavad tööandja seadmeid, siis kontrollib ja haldab neid ettevõtte IT osakond. Seejuures omatakse selget ülevaadet, millised seadmed millises seadistuses eksisteerivad, kes ja kuidas neid kasutab ning millised on varundamise ja turvalisuse reeglid. Enamasti piiratakse ka lõppkasutaja õigusi (nt ei saa tavakasutaja rollis töötaja ise paigaldada uut tarkvara) jne – eksisteerib väljakujunenud süsteem ja parim praktika. VOSKi puhul ollakse aga alles parimate lahenduste otsinguil.

Magistritöös uuritakse VOSK põhimõtte rakendamise infoturvet AS Eesti Telekomi näitel, mis on Eesti kontekstis suur ja mainekas ettevõte ning saab potentsiaalselt olla teistele organisatsioonidele VOSKi edukal ning turvalisel juurutamisel heaks eeskujuks. Autorit seob valitud organisatsiooniga töösuhe, mistõttu omatakse ligipääsu ettevõtte siseinformatsioonile ja ollakse huvitatud töö tulemuste rakenduslikust väärtusest. 2014. a. võeti AS Eesti Telekomis vastu otsus VOSK võimaldada ja praegu otsitakse aktiivselt lahendusi, kuidas seda turvaliselt teha. Tulenevalt on magistritöö probleem sõnastatud järgnevalt: kuidas tagada AS Eesti Telekomis turvaline VOSKi võimaldamine? Magistritöö eesmärk on kaardistada ja hinnata VOSK võimaldamisega kaasnevad infoturbe riskid ja nende leevendamise võimalused AS Eesti Telekomis. Uurimisküsimusi on kolm:

1) Millised on VOSK võimaldamisega kaasnevad infoturbe riskid AS Eesti Telekomis?
2) Millised on kaardistatud VOSK riskide võimalikud mõjud ja esinemise tõenäosused?

3) Millised on võimalused kaardistatud VOSK riskide leevendamiseks?

Magistritöö tulemusena valmib nähtuse spetsiifiline riskianalüüs valitud ettevõtte näitel – s.o kasulik teadmine, mille pinnalt saab VOSK korraldamist ja infoturbe tagamist valitud ettevõttes edukalt edasi planeerida ja teostada. Magistritöö käigus viiakse läbi kvalitatiivne ühe ettevõtte põhine juhtumiuuring, kus nähtust uuritakse selle loomulikus keskkonnas. Info kogumiseks kasutatakse struktureerimata süvaintervjuu meetodit. Andmete analüüsimisel tuginetakse eksperthinnangule, koostatakse riskistsenaariumid ning kasutatakse kikilipsu riskihindamise meetodit.

Töö jaguneb nelja sisupeatükki, mis tervikuna täidavad tööle püstitatud eesmärgi ning vastavad kõigile uurimisküsimustele. Esimeses peatükis antakse ülevaade asjakohasest kirjandusest. See on oluline, et mõista, mida on juba valitud teemaga seoses uuritud ning kuhu tänaseks välja jõutud. Teises peatükis luuakse teoreetiline alus teema mõistmiseks: kirjandusele tuginedes antakse ülevaade VOSK nähtusest, võimalikest kasuteguritest, arhitektuurilistest ja tehnoloogilistest lahendustest, levinud ohtudest ning infoturbe tagamise meetmetest. Kolmandas peatükis tutvustatakse valitud organisatsiooni, kirjeldatakse läbiviidud uuringut ja selle metoodikat ning esitatakse uuringu tulemused koos analüüsiga. Neljandas peatükis arutletakse tulemuste üle.

1 KIRJANDUSE ÜLEVAADE

Peatükk annab ülevaate magistritöö teema kontekstis olulisest kirjandusest.

Kirjanduse ülevaade on koondatud tabelisse 1, mille koostamise protsess ja loogika oli lühidalt järgnev:

- otsinguportaalist Discovery otsiti töö kontekstis olulisi märksõnu olemasolevate ingliskeelsete infoallikate pealkirjadest (*subjects*) ja märksõnadest (*subject terms*);
- otsingutulemustele rakendati järgnevad filtrid: täistekst (*full text*), akadeemilised ajakirjad (*academic journals*);
- leitud infoallikad loeti läbi, lugemise käigus analüüsiti nende sisu ja asjakohasust;
- kõige olulisem info sünteesiti tabelisse 1; seejuures lähtuti autori tunnetusest, milline on teema kontekstis relevantne kirjandus ja soovitusest, et õnnestunud kirjanduse ülevaade keskendub eelkõige sellele, mida on varasemate uuringute abil teema kohta teada saadud (Webster & Watson, 2002);
- kõige hilisem otsing viidi läbi 8. veebruaril 2015.

Pealkiri	**Aasta**	**Autor(id)**	**Fookuseasetus**	**Põhiteemad**	**Oluline teadmine või peamine sõnum**
A mobile device management framework for secure service delivery	2008	Leung, A	Eelkõige tehnilisel tasandil tegeletakse turvaprobleemide lahendamisega teenuste edastamisel pakkujalt lõppkasutajale. Seda olukorras, kus kasutajal on palju seadmeid.	Turvalise teenuse edastuse väljakutsed ja lahendused. Turvalise seadmete haldamise raamistiku loomine, lahenduse kontseptsioon ja analüüs.	Mõeldakse välja tehniline lahendus, mille abil lahendada eelnevalt kaardistatud turvalisuse väljakutseid.
The rise of Mobile Device Management	2008	Wong, K	Informeeriv artikkel eesmärgiga tõsta teadlikkust.	MDM kui kasvav vajadus organisatsioonide jaoks.	Juhitakse tähelepanu kasvavale vajadusele mobiilsete seadmete haldamise (MDM) lahenduste osas.
From desktop to mobile: Examining the security experience	2008	Botha, R.A.; Furnell, S.M.;	Otsitakse vastust küsimusele, kui turvaline on mobiilsete seadmete kasutamine	Võrreldakse tavaarvuti ja mobiilsete seadmete turvalisust järgnevates aspektides:	Jõutakse järeldusele, et mobiilsete seadmete kasutamine pole sama turvaline ja

		Clarke, N.L.	võrreldes tavaarvutiga.	kasutaja autentimine; ühenduvus; informatsioon.	kasutajasõbralik kui tavaarvutite.
BYOD (Bring Your Own Device)	2012	Caldwell, C.; Zeltmann, S.; Griffin, K.	Arutletakse VOSK võimalike plusside ja miinuste üle ning uuritakse, kuidas mõned organisatsioonid nähtusele praktikas lähenevad.	VOSK plussid ja miinused. Kuidas organisatsioonis VOSKi võimaldada? VOSK poliitika ja MDM.	Jõutakse järeldusele, et VOSKi puhul pole küsimus "kas" vaid pigem "millal". VOSKi võimaldades soovitatakse luua vastav poliitika ja leida sobiv MDM lahendus.
BYOD: Security and privacy considerations	2012	Miller, K.W.; Hurlburt, G.F.; Voas, J.	Informeeriv artikkel eesmärgiga tõsta teadlikkust.	Järgmise põlvkonna kasutajad. Turvalisuse murekohad. Privaatsuse murekohad.	Peamine sõnum on, et nooremal generatsioonil eksisteerib ootus VOSKi võimaldatuseks. Oluline on võimaldamise puhul mõelda nii riskidele kui ka kasuteguritele.
BYOD: enabling the chaos	2012	Thomson, G	Üleskutse võimaldada VOSK ja mõelda laiemalt kui vaid seadmete keskselt.	VOSK võimaldamine ja turvalisus. Koostöö IT ja kasutajate vahel. Kompromiss turvalisuse ja võimaluste vahel. Kasutajakogemuse terviklikkus. "'*Cisco ConnectedWorld Technology Report'*. Cisco, 2011" raporti tulemuste tõlgendamine.	Peamine sõnum on, et tuleks mõelda, kuidas organisatsioonina muutuda "virtuaalseks", olles seadmetest ja teenustest vähem sõltuvad.
BYOD security challenges: control and protect your most sensitive data	2012	Morrow, B	Juhtida tähelepanu VOSK ebaturvalisuse temaatikale.	VOSK on enamat kui vaid nutiseadmed. Mobiilsete seadmete nõrkused. Olemasolevate turvasüsteemide puudujäägid. Oluliste andmete infoturve.	Antakse ülevaade 2012. a. ilmunud mitmest olulisest uuringust, läbi mille viidatakse erinevatele turvalisusega seotud väljakutsetele VOSK nähtusega seoses. Organisatsioonidel soovitatakse teema tõsisemalt fookusesse võtta ja antakse selleks

					ka konkreetseid soovitusi.
A New Open Door: The Smartphone's Impact on Work-to-Life Conflict, Stress, and Resistance	2012	Yun, H.; Kettinger, W.J.; Lee, C.C.	Ei käsitle VOSK infoturvet. Fookuses on nutiseadmete kasutamine töö tegemiseks ja sellega kaasnevad töö ning eraelu tasakaalu ja produktiivsuse küsimused. Magistritöö kontekstis oluline, sest VOSK võimaldamise puhul tuuakse tihti välja võimalik produktiivsuse kasv organisatsioonis kui üks oluline argument, miks seda teha. Aitab paremini mõista temaatika "pehmet" poolt.	Millised tegurid on omased nutiseadme kasutamisele nii tööl kui ka kodus? Kas need tegurid mõjutavad töötaja töö- ja eraelu tasakaalu; kui jah, siis millised on mõjud töötajatele? Kas töö- ja eraelu segmenteeriv org.kultuur mõjutab töö- ja eraelu konflikti?	Töö- ja eraelu vaheline konflikt suureneb, kui nutiseadmeid kasutatakse vaid tööaja ja -koha laiendamiseks. Kui nutiseadmete abil on võimalik tõesti "nutikamalt" töötada ja suurendada töö kvaliteeti ja produktiivsust, siis töö- ja eraelu vaheline konflikt väheneb.
Addressing the Challenges of the 'Bring Your Own Device' Opportunity	2013	Ansaldi, H	Lühiülevaade aktuaalsetest VOSK võimalikest kasuteguritest, väljakutsetest ja lahendustest.	VOSK "revolutsioon". VOSK kasutegurid ja väljakutsed. Tuleviku väljakutsed ja võimalikud lahendused.	Eksisteerivad küll väljakutsed aga niisamuti ka lahendused. Pakutakse konkreetseid soovitusi, aga seda üsna üldisel tasandil ja vähedetailselt.
An Approach to Implement Bring Your Own Device (BYOD) Securely	2013	Gupta, V.; Sangroha, D.; Dhiman, L.	Turvalisuse probleemid seoses VOSKiga ja võimalikud lahendused.	VOSK mõiste, turvalisuse probleemid ja 3 sammu nende lahendamiseks.	Pakutakse välja konkreetseid tegevusi, mis peaksid aitama VOSKi turvalisemalt võimaldada.

BYOD, open source and security - business as usual?	2013	Ng, V	Intervjuu *Gartner Researchi Mobile and Client Computing group* direktori Song Chuangiga.	Põhilised turvalisuse probleemid nutiseadmete kasutamisel tööl. VOSK trendi mõju IT osakondade tööle. Androidi ja iOSi riskide erinevused. Parimad praktikad.	Esitatakse arvamusliidri seisukohad ja soovitused.
Auditing the BYOD Program	2013	Semer, L	Artikkel annab juhiseid VOSK programmi auditeerimiseks ja hindamiseks.	MDM. Turvapoliitikad, mis peaksid kindlasti jõustatud olema. Alternatiivne (MDMi vaba) lähenemine.	Pakutakse välja konkreetseid tegevusi, mis peaksid aitama VOSKi turvalisemalt võimaldada ja mida tuleks audiitorina kontrollida ja hinnata.
Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime	2013	Longo, B	VOSK nähtust avatakse eelkõige (UK) seadusandlusest tulenevalt.	Muutused valdkonnas, ajalooline taust. Turvalisuse küsimused ja standardid. Seadusandlusega seotud küsimused. Küberkuritegevus.	VOSK nähtus leiab aset kontekstis, mis ei saa olla täielikult ettevõtte IT osakonna poolt kontrollitud. *Wireless* ühenduste valdkond vajaks tervikuna paremat regulatsiooni.
Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage	2013	Moyer, J. E	Kirjanduse ülevaade 2007-2012 VOSKi võimaldamisest ja haldamisest USA haiglates.	Milliseid tingimusi on vaja, et toetada turvalist VOSKi võimaldamist haiglates? Millist rolli omavad seejuures haiglate informatsiooni valdkonna töötajad?	Jõutakse järeldusele, et teema kohta oleks vaja rohkem uuringuid, aga praktikas pole aega oodata, sest VOSKi kasutamine on juba laialtlevinud. Haiglatel soovitatakse luua VOSK poliitikad ja informatsiooni valdkonna töötajatel teemaga aktiivselt tegeleda.
BYOD Bring Your Own Device	2013	Disterer, G.; Kleiner, C.	VOSK nähtus on üha kasvav trend, millega tuleb tegeleda. Pakutakse välja erinevaid tehnilisi lahendusi suurema turvalisuse tagamiseks.	VOSKi võimalused ja riskid. Arhitektuurilised ja tehnilised kontseptsioonid. Erinevate lahenduste võrdlus. MDM.	Antakse ülevaade võimalikest tehnilistest lahendustest ja võrreldakse neid omavahel.

Threat modeling of a mobile device management system for secure smart work	2013	Rhee, K.; Won, D.; Jang, S.W.; Chae, S.; Park, S.	MDM lahenduste turvalisus.	MDM lahenduste ülesehitus ja võimalikud ohud.	Kaardistati MDM lahenduste võimalikud ohud. Tegevuse tulemusena omandati parem arusaam, kuidas tagada MDM lahenduste turvalisus.
Bring Your Own Device - Challenges and Solutions for the Mobile Workplace	2014	Smith, K.J.; Forman, S.	Käsitletakse aktuaalseid juriidilisi küsimusi, mis USA tööandjatel seoses VOSK nähtusega on tekkinud.	VOSKi plussid ja miinused. VOSKi seosed tasustamisega. Privaatsusküsimused. Omandiõigus. VOSK poliitika sisu.	Pakutakse välja vastused konkreetsetele küsimustele.
Formal modeling and automatic enforcement of Bring Your Own Device policies	2014	Armando, A.; Costa, G.; Verderame, L.; Merlo, A.	VOSK turvalisuse tagamine Android seadmete näitel rakenduste tasandil.	Programmeerimise raamistik. Turvapoliitikad. BYODroid prototüüp ja selle testimine.	Õnnestunult luuakse prototüüplahendus, mille funktsioon on tuvastata, kas kasutaja poolt paigaldada soovitav mobiilirakendus vastab turvapoliitikale.
Securing the 'bring your own device' paradigm	2014	Armando, A.; Costa, G.; Verderame, L.; Merlo, A.	Rakenduste turvalisus ja vastavus organisatsiooni turvapoliitikale.	Probleem, mida VOSK kontekstis lahendatakse, on turvarisk, mis tekib kasutajapoolse rakenduse allalaadimise ja seejärel rakendusele erinevate õiguste ja ligipääsude andmisega ning nende vastavusega asutuse turvanõuetele.	Tutvustatakse prototüüplahendust, mis põhineb SMM (*Secure Meta-Market*) kontseptsioonil. SMM vahendab ligipääsu traditsioonilistele rakenduste poodidele (Google Play, Apple Store, Windows Store), omab ülevaadet paigaldatud rakendustest ja võrdleb nende õigusi asutuse turvapoliitikatega.
BYOD – popular and problematic	2014	Beckett, P	Informeeriv artikkel eesmärgiga tõsta teadlikkust.	VOSK arengud, pilvelahendused, sotsiaalmeedia, probleemid ja nende ärahoidmine.	Soovitatakse VOSK nähtusega läbimõeldult tegeleda ja jagatakse pealiskaudselt nõu, kuidas seda teha.
Securing BYOD	2014	Chang, J.M.; Ho, P.C.; Chang, T.C.	VOSK infoturve - väljakutsed ja võimalikud lahendused.	Väljakutsed: seadme turvalisus, ründetarkvara, turvapoliitika jõustamine. Lahendused: turvapoliitikad,	Antakse ülevaade, mis on hetkel aktuaalsed väljakutsed ja võimalikud lahendused VOSK infoturbe valdkonnas.

				MDM, lahutustehnikad.	
BYOD Business Issues	2014	Coates, S	Soovitusi VOSK turvalisuse auditeerimiseks.	Reeglid, planeerimine, harimine, kokkulepped, juhtimine, valik, poliitika, hindamine, failide jagamine, monitoorimine	Antakse konkreetseid soovitusi VOSK turvalisuse auditeerimiseks.
Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap	2014	Crossler, R.E.; Trinkle, B.S.; Long, J.H.; Loraas, T.M.	Uuritakse tegureid, mis mõjutavad töötajate VOSK poliitika järgimist.	Teoreetiline taust, uuringu kirjeldus ja tulemused koos aruteluga.	Töötajate soov VOSK poliitikat järgida on enim mõjutatud enesetõhususest (*self-efficacy*; uskumus, et suudetakse soovitud viisil toimida) ja järgimise tõhususest (*response efficacy*; uskumus, et soovitud käitumine aitab vältida ohtu).
Real-world BYOD security. BYOD security strategies from two distinct healthcare organizations	2014	Free, J	Soovitusi VOSK turvalisuse tagamiseks asutuste praktikast tulenevalt.	VOSK korraldus väikeses haiglas. VOSK korraldus suures mahus meditsiiniandmeid käsitlevas asutuses.	Kahe meditsiiniasutuse näitel antakse juhiseid VOSK turvalisuse tagamiseks.
Best practices for BYOD security	2014	Romer, H	Juhtida tähelepanu VOSK aktuaalsetele turvariskidele ja suurendada teadlikkust võimalike lahenduste osas.	VOSK uued turvariskid. Parimad praktikad: MDM, MCM jt.	Pakutakse välja praktilisi soovitusi, kuidas VOSK turvalisust suurendada.
BYOD: Where the Employee and the Enterprise Intersect	2014	Waterfill, M.R.; Dilworth, C.A.	Arutletakse VOSKi võimalike plusside ja miinuste üle ning antakse soovitusi, kuidas tagada suuremat turvalisust.	VOSK võimalikud kasutegurid. VOSK riskid. VOSK juurutamine.	Koondatakse olemasolevat infot, millest järeldatakse, et VOSKi puhul ei tohiks olla küsimus "kas võimaldada?" vaid pigem "kuidas võimaldada?".
A framework of cloud-based virtual phones for secure intelligent information management	2014	Ding, J.-H.; Lin, Y.-L.; Kuo, C.-Y.; Chung, Y.-C.; Chien, R.;	Pakutakse välja uudne lahendus, mis põhineb pilvepõhise virtuaalseadme (*cloud-based virtual phones* e. CVP)	Detailne ülevaade pakutavast lahendusest.	Pakutav lahendus omab väärtust, aga vajab ka edasist arendamist ja uurimist.

		Hung, S.-H.; Hsu, C.-H.	tehnoloogial. Peaeesmärk on suurendada VOSKi turvalisust.		
Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach	2015	Dang-Pham, D.; Pittayachawan, S.	VOSK teemaline uurimus Austraalia ülikooli näitel.	Kirjanduse ja seniste uuringute ülevaade, uuringu kirjeldus ja tulemused koos arutelu ning soovitustega.	Uuringu tulemustest selgub, et oleks vajalik tegeleda kasutajate järjepideva koolitamisega ja teadlikkuse tõstmisega.
A mobile business information system for the control of local and remote workforce through reactive and behavior-based monitoring	2015	Ríos-Aguilar, S.; Lloréns-Montes, F.-J.	Lahendatakse probleemi, kuidas VOSK nähtuse kontekstis paremini monitoorida ja kontrollida distantsilt töötajaid.	Probleemi defineerimine, infosüsteem ja prototüüp, asukohapõhise info analüüsimise metoodika, uuringu tulemused.	Pakutakse välja prototüüplahendus, kuidas töötajate asukohta läbi nutiseadmete jälgida.

Tabel 1. Kirjanduse ülevaade.

VOSKi puhul on tegu veel võrdlemisi uue ja akadeemiliselt väheuuritud nähtusega (Crossler, Trinkle, Long, & Loraas, 2014). Seetõttu hakkas VOSK infoturbe temaatika ka akadeemilises kirjanduses figureerima alles hiljuti. Ilmunud kirjanduse osas on siiski selgesti täheldatav kasvutrend alates aastast 2012. Käsitletud teemad varieeruvad ja lahkavad VOSK infoturvet eri tahkudest. Seejuures keskendutakse üldistatult eelkõige järgnevatele alateemadele:

- *nähtuse selgitamine;*
- *infoturbe alased väljakutsed;*
- *võimalikud kasutegurid;*
- *tehnoloogiad;*
- *mobiilsete seadmete haldamine (MDM);*
- *turvapoliitikad;*

- *juhtumiuuringud;*
- *seadusandlus ja privaatsusküsimused;*
- *lahendused ja soovitused.*

Tänaseks eksisteerib piisavalt kirjandust, millele tuginedes on võimalik luua teoreetiline alus (vt järgmine peatükk).

2 TEOREETILINE ALUS

Peatükis luuakse teoreetiline alus teema mõistmiseks. Kirjandusele tuginedes antakse ülevaade VOSK nähtusest, võimalikest kasuteguritest, arhitektuurilistest ja tehnoloogilistest lahendustest, levinud ohtudest ning infoturbe tagamise meetmetest.

2.1 VOSK nähtus

Alapeatükis defineeritakse VOSK mõiste, selgitatakse ja kirjeldatakse VOSK nähtust.

Enamasti tagab organisatsioon oma töötajatele infotehnoloogilised vahendid, aga see mudel on muutumas (Caldwell et al., 2012). Eksisteerib üha kasvav surve, et organisatsoonid laseksid töötajatel kasutada oma isiklikke seadmeid, mille vahendusel nad pääseksid ligi asutuse võrgule, infole ja teenustele (A. Armando, Costa, Verderame, & Merlo, 2014). Olukorda, kus isiklikke IT-vahendeid (nt sülearvutid, mobiil- ja nutitelefonid, tahvelarvutid) kasutatakse nii eraelu kui ka töö kontekstis, nimetatakse VOSKiks (Beckett, 2014; Caldwell et al., 2012; Disterer & Kleiner, 2013; Longo, 2013).

Inglise keeles on VOSKi vasteks BYOD (*Bring Your Own Device*). Magistritöö kirjutamise ajal tundub eestikeelne vaste olevat ingliskeelsega võrreldes küll veel vähem levinud, aga siiski juba ka laialt kasutatav („BYOD site:.ee“ päringule Google'i otsingus 5490 tulemust, „VOSK site:.ee“ päringule Google'i otsingus 1160 tulemust, „"*bring your own device*" site:.ee“ päringule Google'i otsingus 7810 tulemust, „„võta oma seade kaasa" site:.ee“ päringule Google'i otsingus 159 tulemust). Magistritöös kasutatakse läbivalt eestikeelset akronüümi VOSK.

VOSKi laiaulatuslik esilekerkimine on saanud võimalikuks tänu erinevatele tehnoloogilistele arengutele ja käitumisharjumuste muutumisele (Caldwell et al., 2012; Disterer & Kleiner, 2013; Waterfill & Dilworth, 2014):

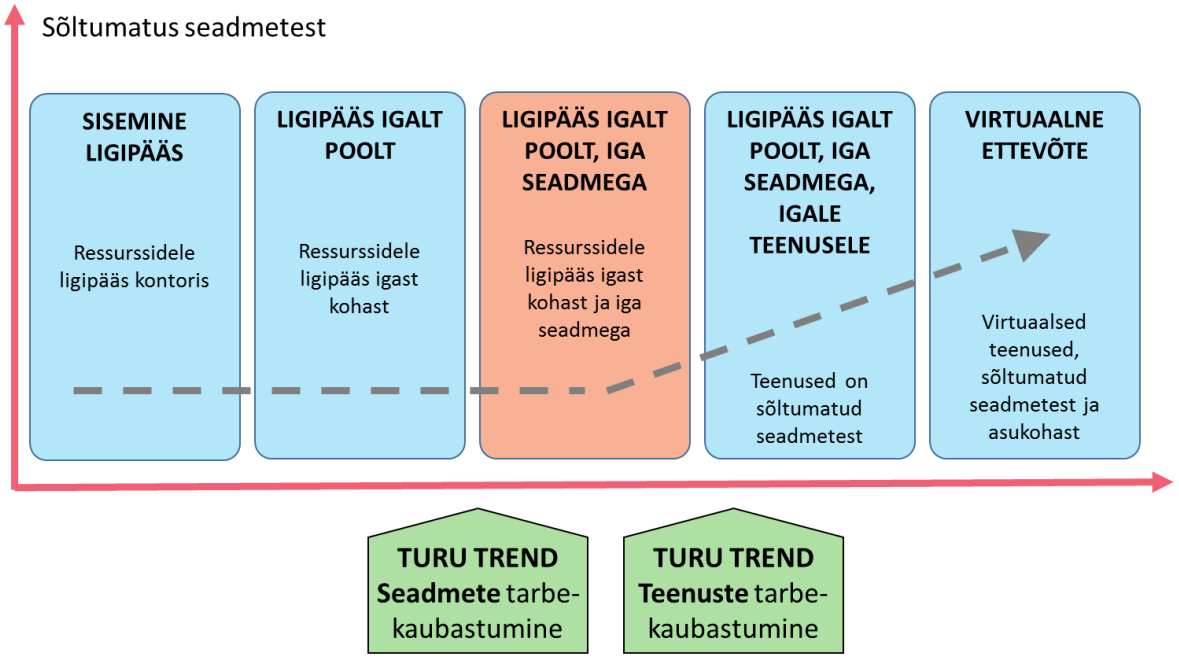
- internetiühendus on üha kättesaadavam, internetipõhised rakendused ja pilveteenused pakuvad üha laiemat funktsionaalsust;
- kvaliteetsed ja võimekad nutiseadmed on eraisikutele üha kättesaadavamad ja üha enam kasutusel;

- ollakse „mobiilsed“, st et seadmeid ja teenuseid kasutatakse igal pool ning igal ajal;
- sama seadet on võimalik kasutada nii era- kui ka tööasjade ajamiseks;
- piir era- ja tööelu vahel on muutunud üha hägusamaks, seda nii töötajate kui ka tööandjate jaoks.

VOSKi on kirjeldatud ka generatsioonikeskse nähtusena, viidates statistikale, et vanemas eas inimesed omavad veel väga vähe nutiseadmeid ja uskumusele, et pealekasvav nn digipõlvkond nõuab seda (Keyes, 2013; Miller, Hurlburt, & Voas, 2012). TNS Emori läbiviidud uuringust selgub, et ka Eestis on nutiseadmete omamine ja aktiivne kasutus just nooremas vanuses väljapaistev: „*Ootuspäraselt on tulemustes suured erinevused vanuse lõikes. Nutiseadmete omamine langeb järsult peale 50.ndat eluaastat. --- ...kasvab selgelt peale uus nutimaailmas elav põlvkond – nii omab juba 38% 6-8-aastastest lastest isiklikku nutitelefoni ja 21% isiklikku tahvelarvutit. Põhikooliks (vanusegrupis 12-14 a) on nutitelefoni omanike osakaal kasvanud juba märkimisväärse 76%-ni. Isiklike tahvelarvutite omanike osakaal ei kasva proportsionaalselt küll sama palju, kuid ulatub siiski 27%-ni 12-14-aastastest lastest.*“ (EMOR, 2014)

2012. a ennustati VOSKile üha kasvavat populaarsust (Caldwell et al., 2012; Miller et al., 2012). Ennustus on seni täitunud, sest VOSK muutub üha tavalisemaks ja levinumaks, muutes inimeste töötamise viise ja tungides eri sektoritesse ning tegevusvaldkondadesse (Ansaldi, 2013; Chang, Ho, & Chang, 2014; Romer, 2014). VOSK on viimase kahe aasta jooksul olnud üks kiiremini esile kerkivamaid ja laiaulatuslikumaid nähtusi, millega ettevõtete IT juhid on pidanud tegelema (Longo, 2013), olles enim levinud 2500 kuni 5000 töötajaga organisatsioonides (Gartner, 2013). Uuringufirma Gartner Research ennustab, et juba 2017. aastaks nõuavad pooled tööandjad töötajatelt töö tegemiseks isikliku seadme kasutamist. (Gartner, 2013). Prognoositakse, et 2016 a. müüdavast 500 miljonist mobiiltelefonist 65% kasutatakse VOSK kontekstis (Beckett, 2014). VOSK võimaldamise puhul pole organisatsioonide jaoks täna enam küsimus: „Kas seda teha?“, vaid pigem: „Kuidas seda teha?“ (Waterfill & Dilworth, 2014).

Sellest, mis suunas VOSK võib edasi arendada, on huvitavaks näiteks Cisco. Cisco on lisaks VOSK võimaldamisele võtnud suunaks saada nn virtuaalseks ettevõtteks, mis oleks asukohast ja seadmetest sõltumatu, tagades samas andmete turvalisuse. Tegemist on pikema protsessiga, mida illustreerib kokkuvõtlikult joonis 1. (Thomson, 2012).



Joonis 1. Cisco kujunemine nn virtuaalseks ettevõtteks (Thomson, 2012).

2.2 VOSK kasutegurid

Alapeatükis kirjeldatakse, milliseid kasutegureid võib VOSKi võimaldamine organisatsioonile kaasa tuua.

VOSKi võimaldamisel on organisatsioonides täheldatud mitmeid võimalikke kasutegureid (Ansaldi, 2013; Caldwell et al., 2012; Longo, 2013; Miller et al., 2012; Morrow, 2012; Stevenson, 2013; Waterfill & Dilworth, 2014):

- suurem töötajate rahulolu;
- suurem produktiivsus;
- suurem mugavus;
- suurem loomingulisus ja innovaatilisus;
- paindlikum töökorraldus;
- rohkem mobiilset (ja distantsilt) töötamist;
- madalamad kulud;
- konkurentsieelise saavutamine;

- äriprotsesside tõhusus;
- tõhusam suhtlus töötajate vahel;
- kiirem kliendipäringutele vastamine;
- IT osakonna koormuse vähenemine.

VOSKi võimaldamisega kaasneb suurem efektiivsus, produktiivsus, rahulolu, autonoomsus ja paindlikkus. Töötaja seisukohast on väga oluline ka mugavus, mida VOSK loob. Sisuliselt saab teha kõike, igal pool ja igal ajal, kasutades selleks meelepärast seadet; samas kui alternatiiv on pidevalt vahetada eri seadmete vahel, olla piiratud statsionaarsetest seadmetest või kanda kaasas mitut seadet. (Caldwell et al., 2012; Disterer & Kleiner, 2013; Morrow, 2012). Oluline on ka vabadus ise valida. Kui töötajad on juba investeerinud oma isiklikku energiat, et valida välja meelepärane seade ja õppida seda kasutama, aga siis selgub, et töökoht nõuab alternatiivse seadme kasutamist, on tõenäoline tulemus töötajapoolne vastupanu (Miller et al., 2012). Samas on vähetõenäoline, et organisatsioon suudab pakkuda töötajale sama suurt valikut kasutatavate seadmete osas. Töötajate nõudmised on kõrged, väga erinevad ja kiiresti muutuvad. (Disterer & Kleiner, 2013).

Organisatsioonil on võimalik alandada kulusid, nt soetamis – ja halduskulud, sest VOSKi puhul ostab ja haldab töötaja seadmeid ise; ning suurendada tulusid, eelkõige läbi produktiivsuse ja efektiivsuse kasvu (Miller et al., 2012; Morrow, 2012; Waterfill & Dilworth, 2014). Lisaväärtusena võib kasvada ka ettevõtte maine ja atraktiivsus tööandjana, seda eriti noorte tehnoloogiahuviliste töötajate jaoks (Disterer & Kleiner, 2013). Ettevõtte seisukohast on VOSKi puhul oluline näha „suurt pilti“ – kuidas kasutada tehnoloogiat konkurentsieelise saavutamiseks, mitte takerduda konkreetsete seadmete lubamise/keelamise tasandile (Thomson, 2012).

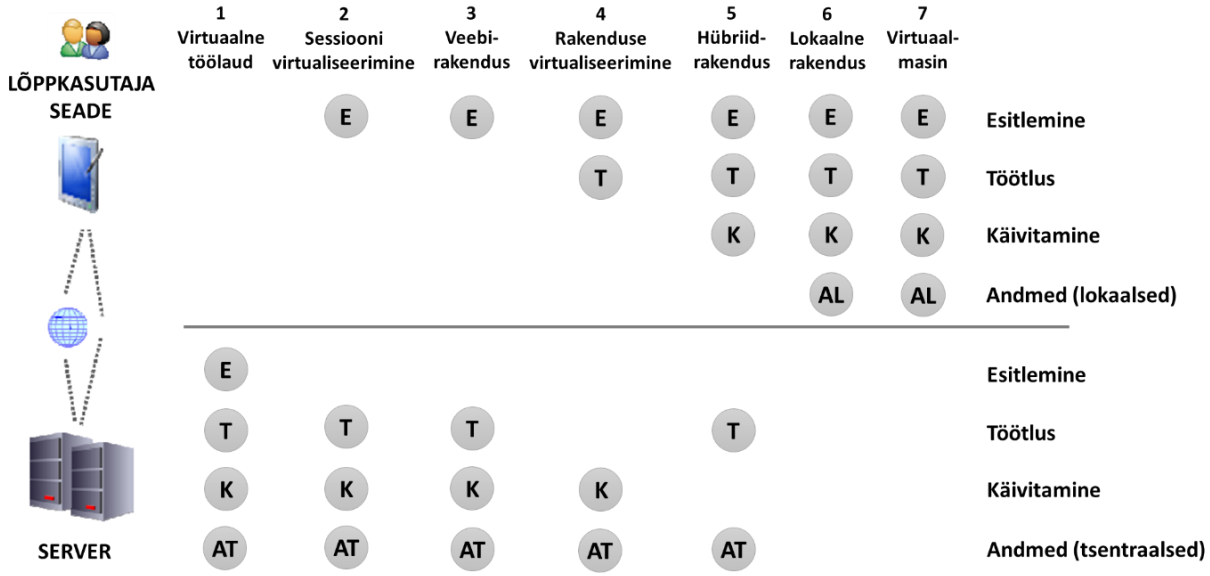
Organisatsioonina on VOSKi võimaldamise puhul heaks positiivseks näiteks Intel, mis juba varakult (alates 2008. aastast) on olnud VOSKi juurutamisel innovatsiooniliider ja suunanäitaja teistele ettevõtetele. Intel oli üks esimestest suurtest ja nimekatest ettevõtetest, kes avalikult VOSKi propageerima asus. (Waterfill & Dilworth, 2014). Inteli 2012.-2013. aasta IT tulemuste koondaruandes kirjutatakse: „*Meie VOSK programm on jätkuvalt kasvamas, hõlmates laiemat hulka seadmeid ja rakendusi. Meie programmis on nüüd 23 500 seadet, 38% rohkem kui 2011. aastal. Programmi tulemusena võidavad töötajad keskmiselt 57 minutit päevas. See võit on*

võrdeline produktiivsuse kasvuga 5 miljonit töötundi aastas VOSKi tulemusena 2012. a põhjal." (Stevenson, 2013).

2.3 VOSK arhitektuurilised ja tehnoloogilised lahendused

Alapeatükis antakse ülevaade, milliseid arhitektuurilisi ja tehnoloogilisi lahendusi VOSKi puhul organisatsioonides tüüpiliselt kasutatakse. Samuti tuuakse välja erinevate lahenduste plussid ja miinused.

VOSKi võimaldamiseks eksisteerib mitmesuguseid arhitektuurilisi ja tehnoloogilisi lahendusi. Need baseeruvad suuresti virtualiseerimisel ja erinevad üksteisest eelkõige lähtuvalt ligipääsu ja võimaluste ulatusest. Eesmärk on töötaja isiklikes seadmetes äritarkvara ülejäänud süsteemist isoleerida. (Chang et al., 2014; Disterer & Kleiner, 2013). Joonis 2 illustreerib erinevaid tehnoloogilisi lähenemisi, eristades need lähtuvalt sellest, kus toimub info esitlemine/mahamängimine (*presentation*), töötlus (*application execution*), tarkvara käivitamine (*application launch*) ja andmete hoidmine (*data component*). Tabel 2 selgitab erinevate tehnoloogiate olemust ja tööpõhimõtteid.



Joonis 2. Arhitektuurilised ja tehnoloogilised lahendused (Disterer & Kleiner, 2013).

Tehnoloogia	**Selgitus**	
1. Virtuaalne töölaud *(Virtual Desktop)*	Isiklik seade käivitab virtuaalmasina või rakenduse serveril, mis asub ettevõtte võrgus. Server genereerib kasutajaliidese, mida töötaja seadmesse kuvatakse ja töötleb talle antud käsud.	
	Plussid: • tuttav lahendus laua- ja sülearvutitelt.	Miinused: • vajab ülikiiret ja püsivat internetiühendust.
2. Sessiooni virtualiseerimine *(Session Virtualization)*	Käivitamine ja töötlus toimub ettevõtte serveris, aga mahamängimine töötaja seadmes, kuhu kuvatakse kasutajaliides, mida pidevalt käskudest lähtuvalt uuendatakse (striimimine).	
	Plussid: • ühendus ei pea olema nii kiire ja püsiv kui virtuaalse töölaua puhul; lihtsam üles seada kui virtuaalset töölauda; • toetab palju erinevaid seadmeid (pole otseselt platvormi/tarkvara spetsiifiline).	Miinused: • vajab internetiühendust.
3. Veebirakendus *(Web Application)*	Serveriks on veebiserver, ligipääsuks kasutatakse tavalist veebibrauserit. Klassikalise HTMLi puhul toimub seadmes vaid mahamängimine (aga levinud HTML5 ja JavaScripti puhul on tegemist juba hübriidlahendusega).	
	Plussid: • ühendus ei pea olema ülikiire; • levinud ja tõenäoliselt juba niigi kasutusel olevate tehnoloogiate tõttu lihtne üles seada ja hallata; • erinõuded töötaja seadmetele on minimaalsed, madalate kuludega saab toetada suurt hulka seadmeid.	Miinused: • vajab internetiühendust; • infoturbe seisukohalt riskantsem kui eelnevad 2 lahendust (veebibrauser võib salvestada andmeid lokaalselt, nõrkus ründetarkvarale); • kasutajakogemus võib olla halb.
4. Rakenduse virtualiseerimine *(Application Virtualization)*	Rakendus asub serveris. Käivitamisel laeb seade alla vastava faili, mille töötlus toimub samuti seadmes, tavaliselt isoleeritult aedikus (*sandbox*/konteiner).	
	Plussid: • ühendus vajalik vaid esialgseks faili allalaadimiseks;	Miinused: • rakendus ei pääse hästi ligi seadme andmetele (lokaalsete

	• versioonihaldus lihtne, sest serverist käivitatakse alati uusim fail; • VPNi ja aediku kasutamisel küllaltki turvaline.	andmete kasutamine raskendatud, vajab käsitööd kasutajalt); • nõrkus ründetarkvarale.
5. Hübriidrakendus *(Hybrid Application)*	Kombineerib veebi- ja lokaalse rakenduse omadused vastavalt vajadustele.	
	Plussid: • samad plussid, mis veebi- ja lokaalse rakenduse kasutamisel; • eraldi välja toomist väärib, et lokaalse rakenduse komponent võimaldab kasutada seadmespetsiifilisi funktsionaalsusi.	Miinused: • samad miinused, mis veebi- ja lokaalse rakenduse kasutamisel.
6. Lokaalne rakendus *(Native Application)*	Erakasutuses laialt levinud lahendus, kus rakendus on arendatud konkreetsele süsteemile, muudetud kättesaadavaks rakenduste poes (nt App Store, Play Store) ja kasutaja poolt paigaldatav.	
	Plussid: • ühendus vajalik esialgseks rakenduse allalaadimiseks ja uuendamiseks, muidu enamasti võimalik kasutada ka ilma püsiühenduseta; • kasutajakogemus võib olla väga hea, sest rakendus on loodud konkreetsele süsteemile; • võimalik mugav ettevõtte ja isiklike failide vastastikune andmevahetus.	Miinused: • ettevõtte ja isiklike failide vastastikune andmevahetus muudab keeruliseks era- ja tööandmete lahutamise; • distantsilt andmete kustutamine tähendab enamasti tehase seadete taastamist ja kogu info kustutamist; • iga rakendus spetsiifiline, vajab eraldi paigaldamist ja haldamist.
7. Virtuaalmasin *(Virtual Machine)*	Seadmesse paigaldatakse virtuaalmasin millega emuleeritakse tavasüsteemi. See on levinud meetod tavaarvutite puhul, aga vähemlevinud mobiilsetel seadmetel.	
	Plussid: • ei vaja internetiühendust;	Miinused: • era- ja tööandmed lahus (võib olla töötajale ebamugav);

	• saab töötada mitme rakendusega korraga (erinevalt rakenduse virtualiseerimisest); • era- ja tööandmed lahus (turvaline); • suur kasutajamugavus, sest saab seadistada lähtuvalt kasutajaeelistustest.	• koondhaldus (ettevõtte seisukohast) hetkel veel ebamugav ja ajamahukas, sest vastavad tööriistad mobiilsetele seadmetele pole levinud; • turvalisuse aspektist oluline tagada jätkuvalt ka kogu seadme (st mitte ainult virtuaalmasina) turve.

Tabel 2. Erinevate tehnoloogiate selgitused (Disterer & Kleiner, 2013).

2.4 VOSK infoturbe ohud

Alapeatükis antakse ülevaade, millised on üldlevinud VOSK infoturbe ohud.

Kuigi VOSK on tänaseks juba küllaltki laialt levinud, on nähtusel ka oma varjukülg – kuidas tagada piisav infoturve? Just mobiilsed seadmed on küberkurjategijatele üha ihaldusväärsemad sihtmärgid, sest reeglina on neis talletatud seadme omaniku „digitaalne elu“ tervikuna: e-kirjad, sotsiaalmeedia, lennupiletid, pangaandmed, asukohainfo jm (*The State of IT Security in Germany*, 2014). Erinevatest VOSKiga seotud väljakutsetest ongi just infoturbe tagamine kõige esilekerkivam (Ansaldi, 2013; Gartner, 2013; Keyes, 2013) ja seejuures tuleb arvestada väga mitmesuguste ohtudega (Romer, 2014). Olukorda teevad infoturbe tagamise aspektist keerulisemaks mitmed tegurid:

- üha enam kasutatakse pilveteenuseid, veebirakendusi ja tarkvara teenusena (*Software as a Service* ehk SaaS) lahendusi (Morrow, 2012);
- veebikanalite ja serverite kõrge turvalisus, millesse tänapäeval organisatsioonides palju panustatakse, ei taga lõppseadmete turvet (Morrow, 2012);
- puuduvad ühtsed VOSK standardid ja protokollid (Ansaldi, 2013);
- enamikel mobiilsetest seadmetest puuduvad kõrgeltarenenud turvaelemendid (Romer, 2014);
- kontekst on lai – VOSK leiab aset organisatsiooni sees, aga samuti ka väljaspool seda ja ei ole seetõttu täiel määral kontrollitav (Longo, 2013).

Kirjandusele tuginedes on enamlevinud VOSKiga seotud infoturbealased ohud järgnevad:

- andmete leke;
- andmete saaste;
- ründetarkvara;
- õngitsemine;
- tüssamine;
- urkimine;
- ebaturvaline failijagamine;
- seadme kaotus või vargus;
- turvapoliitikate jõustamine;
- MDM süsteem kui täiendav oht;
- inimtegur.

Järgnevalt on iga loetletud oht pikemalt lahti selgitatud.

Andmete leke (*data disclosure*)

VOSKi puhul kasutatakse samu seadmeid nii ettevõtte sisevõrgus kui ka välistes ebaturvalistes võrkudes, kus konfidentsiaalsed andmed võivad lekkida. Nutitelefonid, tahvel- ja sülearvutid, mis ühendatakse ettevõtte sisevõrku, suurendavad märkimisväärselt andmelekke ohtu. Operatsioonisüsteemid tekitavad teatud kujul logisid, ajutisi faile või muud „ajalugu“, mis seadmesse salvestub. Kui antud seade ühendatakse internetti, siis on oht andmete lekkeks alati olemas. (Gupta, Sangroha, & Dhiman, 2013; Morrow, 2012). Tavakasutajale täiesti igapäevased tegevused (nt kopeeri ja kleebi), veebilehitsejas salvestatud kasutajakontod jms jätavad palju infojälgi, mis on lihtsasti ligipääsetavad (Morrow, 2012).

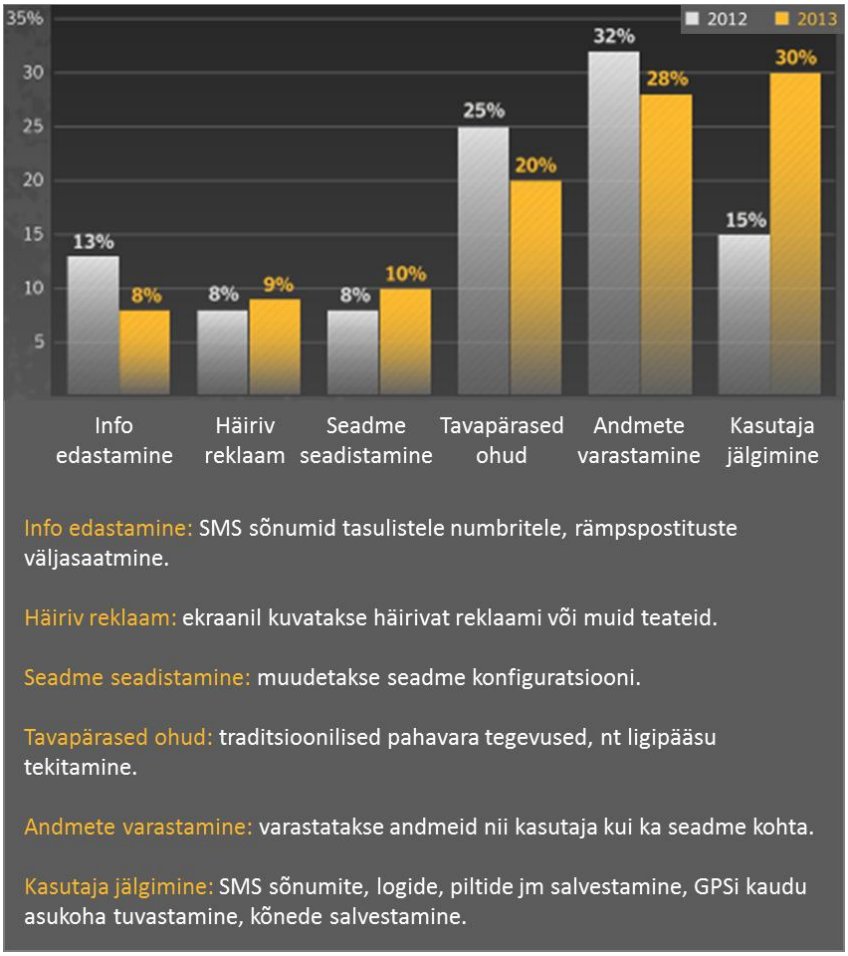
Andmete saaste (*data contamination*)

Andmete saaste on andmete terviklust rikkuv sihilik või stiihiline protsess/toiming (Veldre et al., 2015). Töötajate isiklikud andmed (kontaktid, aadressid, pildid, dokumendid) peaksid ettevõtte ligipääsu eest kaitstud olema, aga samas tuleks ettevõttele tekitada ligipääs tööalastele failidele. VOSKi puhul on era- ja tööandmed seadmes tihti kõrvuti, kui mitte läbisegi. Selline olukord suurendab üleüldist infoturbe tagamise keerukust ja tekitab täiendavaid infoturbe riske. (Disterer & Kleiner, 2013). Nii võivad ebaolulised, konfidentsiaalsed või lausa kahjulikud (nt ründetarkvaraga nakatunud) andmed hooletusest sattuda tagavarakoopiatele või

failiserveritesse ning sealt edasi levida. (Romer, 2014). Nn saastunud või segunenud andmeid võivad töötajad (samuti hooletusest) jagada ka oma isiklike kontaktidega (Chang et al., 2014).

Ründetarkvara (*malware*)

Ründetarkvara ehk kahjurvara on sihilikult infosüsteemi talitluse kahjustamiseks või häirimiseks, tundliku teabe kogumiseks, lubamatu juurdepääsu saamiseks või konfidentsiaalsuse, tervikluse või käideldavuse ründamiseks määratud programm, koodilõik, skript, makro vms vahend (nt viirus, uss, troojahobu, klahviloger, lunavara, soovimatu reklaamvara) (Veldre et al., 2015). Ettevõtte IT spetsialistid ei saa töötajate isiklikke seadmeid ründetarkvara osas kontrollida (Morrow, 2012). Ründetarkvara ohustab mobiilseid seadmeid rohkem kui eales varem. Häkkerid ja kuritegelikud ühendused on mõistnud, et mobiilsed seadmed on palju ebaturvalisemad kui näiteks sülearvutid ja asunud neid ründama. Ründed ise varieeruvad ulakatest naljadest salaja andmeid kopeerivate ja edastavate ründetarkvaradeni. Kahjurvara on järjest nutikamalt koostatud ja traditsioonilised tõrjevahendid tuvastavad seda halvasti. Näiteks võivad ühe organisatsiooni töötajad saada küll sama sisuga kirju, ent kirjaga kaasnev ründetarkvara on igaühel pisut erinev. Keerulisem ründetarkvara on sageli konstrueeritud nii, et suudab mõista, kui teda lihtsamate vahenditega analüüsida üritatakse ning näiteks virtuaalmasinas käivitatakse - sellisel juhul käitub ründetarkvara hoopis teisiti ja ohutumalt kui ohvri arvutis. (RIA, 2014). Spetsiaalselt mobiilseid seadmeid ründava ründetarkvara arv on viimastel aastatel kasvanud (*The State of IT Security in Germany*, 2014). Nt Android operatsioonisüsteemile teadaolevat ründetarkvara eksisteeris 2014. a. jaanuaris koguni 14 korda rohkem kui 2012. a. jaanuaris. IBM ennustab mobiilsetele seadmetele mõeldud ründetarkvara kasvu järgnevateks aastateks 15% aastas. (Chang et al., 2014; Dang-Pham & Pittayachawan, 2015; Morrow, 2012; Romer, 2014). Töötaja ise ei pruugi ründetarkvara olemasolust teadlik olla, sest tema jaoks töötab seade tavapäraselt (Leung, 2008). Niipea kui ründetarkvaraga nakatunud töötaja seade ettevõtte võrku ühendatakse, võib ründetarkvara seal edasi levida (Miller et al., 2012). Ülevaate sellest, millised funktsioonid on ründetarkvara puhul mobiilses seadmes levinud annab joonis 3.



Joonis 3. Mida ründetarkvara mobiilses seadmes teeb? (Symantec Corporation, 2014).

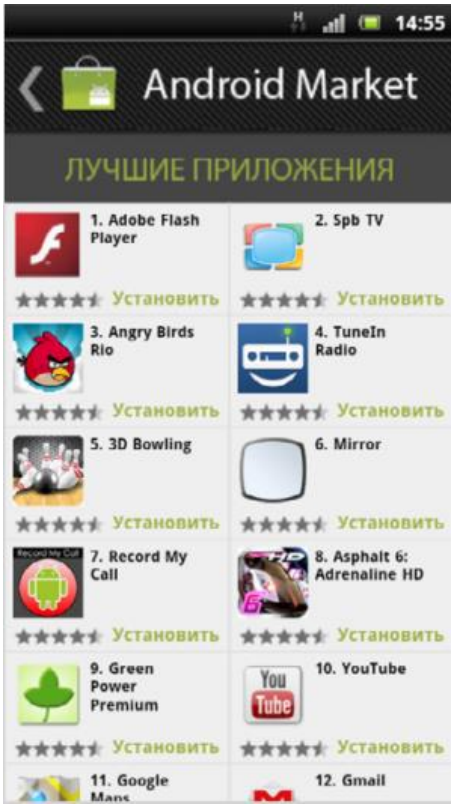
Õngitsemine (*phishing*)

Õngitsemine on „*teesklus, mille sooritaja saadab tundliku teabe saamiseks sõnumeid, mis näivad tulevat sotsiaalvõrgust, oksjonisaidist, pangast vm usaldatavast allikast*“ (Veldre et al., 2015). Häkkerid disainivad hästitoimivaid õngitsemisründeid spetsiaalselt puhkeajale, mil on tõenäoline nutiseadme kasutamine ja kaitsevõime madalam, kui kontoris viibides. Selliste rünnetega võidakse seadmesse paigaldada nuhk- ja ründetarkvara, mis saadavad infot ja võimaldavad kavandada suuremaid rünnakuid ettevõtte infosüsteemidele. (Romer, 2014). Ka Eestis on üheks 2014. a oluliseks küberturvalisuse trendiks just oskuslik pilveteenuste kontode (nt Gmail, Hotmail) andmepüük, mis on RIA hinnangul jätkunud seninägematu hooga ka 2015. a algul. E-kirjad saabuvad sageli justkui usaldusväärsest allikast ja on nii sisult kui ka keeleliselt teinud kvaliteedihüppe. Nt jõudsid 2014. a suvel Eestisse maailmas levinud õngitsuskirjad, mis pärinesid justkui Apple’ilt ja hoiatasid sealse kasutajanime ja parooli aegumise eest. Veebilehel, mis oli äravahetamiseni sarnane Apple’i enda teenusega, paluti kasutajatel sisestada oma

kasutajanimi ja parool; seejärel ohvrite kontod lukustati ning nende avamise eest nõuti lunaraha. (RIA, 2014).

Tüssamine/spuufimine (*spoofing*)

Tüssamine/spuufimine ehk teesklus on „*kellegi või millegi teisena esinemine, seadusliku ressursi või kasutaja kehastamine*“ (Veldre et al., 2015). Pahatahtlikud isikud võivad etendada usaldusväärseid teenuseosutajaid, et käivitada võltssuhtlemist või vastupidiselt etendada usaldusväärset kasutajat teenusepakkujatele (Leung, 2008). Näiteks Venemaal on laialt levinud ametlike rakenduste poodide libakoopiad (vt joonis 4), kust originaalrakenduste asemel laetakse alla hoopis ründetarkvara (Symantec Corporation, 2014).



Joonis 4. Võltsitud rakenduste pood Venemaal (Symantec Corporation, 2014).

Urkimine (*tampering*)

Urkimine on „*lubamatu manipuleerimine, sekkumine, muutmine, avamine (eriti riistvara sisemuse, kiipkaartide ning pakendite ja dokumentide puhul) vms rünne*“ (Veldre et al., 2015). Suhtlemist võib pealt kuulata või jälgida; info edastamise käigus võib kolmas osapool sellega manipuleerida, nt lisada pahatahtlikku valeinfot. Pealtkuulamise/jälgimise risk on eriti suur juhtmeta/traadita (*wireless*) kommunikatsiooni puhul. (Leung, 2008).

Ebaturvaline failijagamine

Mobiilsete seadmetega kasutatakse tihti ebaturvalisi failijagamise teenuseid, kus ei ole turvaline ettevõtte andmeid hoida ja puuduvad piisavad infoturbe tagamise meetmed. Näiteks võis ilma paroole teadmata 2012. a. pääseda nelja tunni vältel ligi Dropboxi kasutajate failidele. Lisaks on selliste keskkondade puhul küsitav, kellele andmed kuuluvad ja mil viisil neid edasi kasutada ja töödelda võib. (Romer, 2014).

Seadme kaotus või vargus

Mida rohkem seadmeid töötajad kasutavad ja kaasas kannavad, seda suurem on tõenäosus neid kaotada. Mobiilsete seadmete kaotamise või vargusega on 2014. a jooksul pidanud tegelema 44% ettevõtetest (ISACA, 2015). Töötajate seadmed võivad sisaldada tundlikku informatsiooni (kontaktandmed, e-kirjad, kontode andmed, klientide andmed, ettevõtte rakenduste poolt salvestatud info jpm). Isegi kui kaotatud või varastatud seade otseselt konfidentsiaalseid andmeid ei sisalda, võib seal ikkagi leiduda kontode ligipääse või rakendusi, mille abil pääseb kurjategija ligi ettevõtte sisevõrgule. (Chang et al., 2014; *ENISA Threat Landscape 2014*, 2014; Leung, 2008; Miller et al., 2012; Romer, 2014)

Turvapoliitikate jõustamine (*enforcement*)

Kui isiklikke seadmeid kasutatakse ettevõtte sisevõrgus, siis on väga oluline tagada turvapoliitikate jõustamine (Chang et al., 2014). Näiteks organisatsioonile kuuluvate sülearvutite puhul on saanud tavaks ettevõtte turvapoliitikate jõustamine, kohustuslik parool ja andmete krüpteerimine (Miller et al., 2012). VOSK põhineb aga eeldusel, et töötajad omavad seadmeid ja ettevõtte turvapoliitikaid on töötajate isiklikes seadmetes väga keeruline jõustada. Probleemi süvendab riist- ja tarkvara suur variatiivsus ning väljakutseks on ka pidev uuendamisvajadus. (Chang et al., 2014; Miller et al., 2012). IT-osakond ei saa VOSKi puhul kontrollida, millist veebilehitsejat töötaja kasutab või millised turvauuendused ja lisamoodulid on seadmesse paigaldatud. Neil puudub ülevaade, millist infot on töötaja seadmesse salvestatud. (Morrow, 2012).

***Mobile Device Management* (MDM) süsteem kui täiendav oht**

VOSKi juurutamisel võtavad ettevõtted tihti kasutusele mobiilseadmete halduse ehk MDM (*Mobile Device Management*) süsteeme, selleks et suurendada mobiilsete seadmete turvalisust. Seda tehes luuakse aga juurde ka täiendav oht. Kui MDM süsteemi sisse tungitakse, siis on

võimalik kontrollida kõiki ettevõtte mobiilseid seadmeid ja nendes sisalduvaid andmeid. (Rhee, Won, Jang, Chae, & Park, 2013).

Inimtegur

Pahatahtlik töötaja saab VOSKi puhul vähese vaevaga ettevõtte ärisaladusi, kliendiandmeid jm tundlikku infot varastada (Morrow, 2012). Töötaja võib ligipääsu omavat seadet kõrvalistele isikutele edasi anda, nt sõprade või pereliikmetega jagada või maha müüa (Leung, 2008). Nt tahvelarvutit jagatakse Eestis meeleldi pereliikmetega ja neljal juhul viiest tegutsetakse seejuures sama kasutajakonto alt (EMOR, 2014). Töötaja võib tahtlikult või tahtmata rikkuda majandusharu või ettevõtte reegleid, kahjustada töötaja ja tööandja vahelist usaldust ning õõnestada äritegevust (Beckett, 2014). Töötaja võib kehtestatud turvapoliitikaid tahtlikult eirata (Waterfill & Dilworth, 2014) ning ei ole alati hoolikas ründetarkvara vältimisel (Dang-Pham & Pittayachawan, 2015). Isegi kui ettevõte on omalt poolt sobilikud turvatingimused taganud, võib probleemiks osutuda, et töötaja (kui lõppkasutaja) ei oska tema käsutuses olevat turvafunktsionaalsust õigesti kasutada (Botha, Furnell, & Clarke, 2008).

Alapeatükis esile toodud ohtudest selgub, et VOSK nähtuse puhul on ohus andmete turvalisuse kõik põhikomponendid ("ISKE rakendusjuhend versioon 7.00," 2014; Keyes, 2013):

- andmete käideldavus;
- andmete terviklus;
- andmete konfidentsiaalsus.

Teatud mõttes on tegemist üpris sarnaste ohtudega, mis tekkisid sülearvutite levinuks muutumisega, aga sülearvutid on nutiseadmetest palju suuremad ja seetõttu on juba nt nende kaotsiminek palju vähetõenäolisem. Lisaks on VOSKi puhul tööle kaasa võetavate seadmete arv töötaja kohta oluliselt suurem. (Miller et al., 2012). VOSKi juurutamisega kaasneb turvariskide suurenemine olulisel määral (Waterfill & Dilworth, 2014).

2.5 VOSK infoturbe tagamise meetmed

Alapeatükis antakse ülevaade, millised on üldlevinud VOSK infoturbe tagamise meetmed.

VOSKi üha kasvav populaarsus peaks kõigile ettevõtetele mõjuma üleskutsena, et teemaga tuleb tegeleda, eriti kui tahetakse tagada piisav infoturve. Samas ei tohiks VOSKi

võimaldamine ettevõttes olla töötajate või meedia poolt initsieeritud, vaid ikkagi läbimõeldud otsus. (Beckett, 2014). VOSKiga kaasnevate väljakutsete puhul on oluline mõelda ettevõtte suurtele eesmärkidele ning kuidas saab tehnoloogia organisatsiooni hüvanguks tööle panna (Ansaldi, 2013). Samas on vaja tagada turvatingimuste vastavus valdkonna standarditele, seadusest tulenevatele nõuetele ja regulatsioonidele (Semer, 2013). Eksisteerivad mõistlikud ja strateegilised viisid, kuidas VOSKiga kaasnevaid riske leevendada (Ansaldi, 2013).

Oluline on luua infoturbe tagamise meetmed nii, et need tagaksid piisava turvalisuse ja oleksid ka töötajatele mõistetavad ja kasutatavad (Botha et al., 2008). Ettevõte peaks siinkohal võtma proaktiivse positsiooni ja veenduma, et kõik seadmed, mis sisevõrku ühenduvad, oleksid turvatud (Morrow, 2012). Enne sobilike meetmete juurutamist ei tohi töötajate isiklikke seadmeid ettevõtte andmetele ligi lasta (Waterfill & Dilworth, 2014).

VOSKi võimaldamist tasub alustada vastava turvapoliitika väljatöötamisest ja kehtestamisest ning vajalike protsesside ja süsteemide (nt MDM) juurutamisest (Caldwell et al., 2012; Ng, 2013; Semer, 2013). Seejuures tuleb mõelda, et eksisteeriksid nii ennetavad kui ka parandavad meetmed. Juurutatud tehnoloogiaid ja meetmeid tuleb järgnevalt regulaarselt testida. (Ansaldi, 2013). Töötajate privaatsust ei tohi kuritarvitada (Chang et al., 2014).

VOSK turvapoliitika (dokument)

Turvapoliitika (dokumendi) olemasolu on VOSKi puhul väga oluline seetõttu, et ettevõttel puudub võimalus töötajata isiklikke seadmeid 100% kontrollida. Lisaks on tehnoloogia (töötajate seadmed) pidevalt muutuvad. Poliitikaga sätestatakse ja kommunikeeritakse kõigile ettevõtte töötajatele selged alusreeglid ja ootused käitumise osas. (Ansaldi, 2013; Waterfill & Dilworth, 2014). Turvapoliitikast on kasu siis, kui töötajad seda ka järgivad, aga reaalsuses ei pruugi nad seda teha (Crossler et al., 2014). Seetõttu on oluline tegeleda ka töötajate koolitamisega.

Kuigi iga ettevõtte VOSK turvapoliitika peaks olema loodud vastavalt ettevõtte spetsiifikale, tasub seejuures mõelda järgnevatele aspektidele (Smith & Forman, 2014):

- millised seadmed (brändid ja/või mudelid) on lubatud, millised keelatud;
- kas seadmega seonduvad kulud kannab töötaja või ettevõte (andmeside, seadme purunemine, kadumine, vargus);
- mis saab siis, kui töötaja ettevõttest lahkub;

- nõue, et kõik töötajad seadistaksid oma seadmed lähtuvalt ettevõtte kehtestatud turvanõuetest (nt andmete krüpteerimine, lukustumine pärast mitut ebaõnnestunud parooli sisestamist, lukustumine olles teatud aja mitteaktiivne, antiviiruse kasutamine jm);
- nõue kaitsta seadmed parooliga ja vahetada parooli perioodiliselt (nt kord kvartalis);
- nõue teha koostööd, kui ettevõttel on vajadus seadmele salvestatud andmeid vm sisu uurida;
- keeld salvestada/jagada ettevõtte andmeid ebaturvalistes kanalites (nt pilveteenused, millesse on varasemalt sisse häkitud);
- nõusolek, et ettevõtte võib kustutada seadmel sisalduvad andmed, kui see kaotatakse või varastatakse; seejuures ei vastuta ettevõte kaotsi läinud andmete eest;
- kohustus, et töötaja teeb isiklikest failidest ise regulaarselt varukoopiaid;
- ettevõttel on õigus jälgida seadme sisu ja tegevusi seaduslikus ulatuses;
- keeld saata tööalaseid e-kirju läbi isiklike suhtluskontode.

Kindlasti tasub mõelda ka sellele, kas valmiv VOSK turvapoliitika on hästi koostatud, kõigile töötajatele mõistetav, reaalselt järgitav ja ettevõtte poolt jõustatav (Coates, 2014; Crossler et al., 2014).

Mobile Device Management (MDM) süsteem

Mobiilseadmete halduse ehk MDM lahendused on kasvanud välja lauaarvutite aegsest lõppseadmete haldamisest. Töötaja seadmesse paigaldatakse spetsiaalne klientprogramm, mis kontrollib seadme staatust ja vastavust turvapoliitikatele ning suhtleb pidevalt ettevõtte MDM süsteemiga. (Ding et al., 2014). See võimaldab mobiilsete seadmete tsentraalset haldamist (Disterer & Kleiner, 2013). VOSKi haldamiseks kommertskasutuses eksisteerib rohkelt MDM lahendusi paljudelt eri pakkujatelt; nt VMware, AirWatch, Maas360, MobileIron, Fiberlink, Zenprise, Good Technology (Chang et al., 2014; Disterer & Kleiner, 2013). Tavaliselt tuleb sellistes lahendustes iga uus seade registreerida, et kaughaldus saaks toimuda. MDM süsteemide funktsioonid varieeruvad lähtuvalt valitud lahendusest. (Chang et al., 2014). Näiteks on võimalik jõustada antiviiruse tarkvara paigaldamist ja kasutamist, operatsioonisüsteemi automaatset uuendamist, rakenduste lubatud/keelatud nimekirja kasutamist ja seadme eemaldamist sisevõrgust, kui see ei vasta kehtestatud turvapoliitikale (Semer, 2013). Mõned tooted võivad sisaldada ka põhjalikumat rakenduste haldust (*Mobile*

Application Management ehk MAM) ja sisu haldust (*Mobile Content Management* ehk MCM). (Chang et al., 2014). Tabelis 3 on toodud välja tüüpilised MDM süsteemi funktsioonid:

Funktsioon	**Kirjeldus**
Rakenduste haldus	Rakenduste paigaldamine ja deinstallimine. Rakenduste käivitamine ja peatamine. Rakenduste uuendamine. Rakenduste deinstallimise takistamine. Ettevõtte poolt lubamatute rakenduste blokeerimine. Sertifikaatide paigaldamine.
Seadme haldus	Erinevate funktsioonide ja komponentide sisse/välja lülitamine (nt kaamera, sinihammas, WIFI, GPS, mikrofon jne). Diagnostika.
Inventariloend	Info kogumine (logid, IP aadressid, SIM-kaardi seisund, OS-info, ID/nime/versiooni info, IMEI kood, seadme tüüp, riistvara info jne).
Turvalisuse haldus	Turvapoliitikate jõustamine. Seadme lukustamine distantsilt. Andmete kustutamine distantsilt. Seadme tehaseseadete taastamine distantsilt. Konfigureerimine distantsilt. Paroolinõuete kehtestamine (pikkus, sümbolite kasutamine, ajalugu, ebaõnnestunud sisestamise kordade arv jne). Andmete krüpteerimine. Andmete varundamine. Asukoha jälgimine. Kontode seadistamine distantsilt (Exchange, VPN jne). Raporteerimine - automaatteadete edastamine.

Tabel 3. MDM süsteemi tüüpilised funktsioonid (Keyes, 2013; Rhee et al., 2013).

MDM süsteemi abil saab ettevõtte võrku ühenduvaid mobiilseid seadmeid algusest lõpuni turvata, monitoorida, hallata ja neile ka kasutajatuge pakkuda. Seetõttu teeb MDMi olemasolu VOSKi haldamise tunduvalt lihtsamaks. (Gupta et al., 2013). Tegemist on hetkel domineeriva

tehnoloogilise lahendusega VOSK valdkonnas (Ng, 2013). MDM süsteemide kriitikana tuuakse välja järgnevat (Romer, 2014):

- MDMi puhul on fookuses eelkõige seadmed (nagu nimigi viitab), aga ettevõtte jaoks on eelkõige oluline informatsiooni ja andmete turvamine, sõltumata konkreetsetest seadmetest. MDM lahendus ei pruugi tagada kontrolli andmete ja failide üle.
- MDMi kasutamine võib IT osakonnale palju tööd juurde tekitada, nõudes pidevalt administreerimist ja rohkelt muutuva seadmete nimekirja haldamist.

Lisaks võivad MDM lahendused olla oma maksumuse tõttu paljudele kättesaamatud.

Ideaalis peaks MDM süsteem looma tasakaalu ettevõtte turvavajaduste ja töötaja kasutajakogemuse, mugavuse ning privaatsuse vahel (Semer, 2013). Ettevõttele sobivat lahendust valides tuleb hoolikalt kaardistada organisatsioonispetsiifilised vajadused ning viia läbi audit, kuidas MDM sobitub ülejäänud IT infrastruktuuriga (Disterer & Kleiner, 2013).

Töötajate privaatsus ja VOSK turvameetmed

VOSKi puhul on töötajate privaatsus väga oluline alateema, mida käsitleda ja millest tuleb teadlik olla ka turvameetmete loomisel. Ettevõte ei tohi töötaja privaatsust kuritarvitada (Chang et al., 2014). Kuidas on see teema reguleeritud EV seadusandluses? Põhiseaduse § 26 alusel on igaühel õigus perekonna- ja eraelu puutumatusele. Otseselt töötaja infovahetuse konfidentsiaalsuse kaitseks on põhiseaduse § 43s kirjas: *„Igaühel on õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele…“* Tööandjal on isikuandmete kaitse seaduse § 14 lg 1 p 4st tulenevalt õigus töödelda töötaja isikuandmeid töötaja nõusolekust sõltumata niivõrd, kui see on vajalik töölepingu täitmiseks. Töölepingu seaduse § 28 lg 2 p 11s on kirjas, et tööandja on kohustatud austama töötaja privaatsust ning kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi, aga tööandja kohustuste täpsem sisu tundub seaduses puuduvat. *„Oluline on silmas pidada, et andmete töötlemine peab olema põhjendatud. Andmete töötlemisel on kõige olulisem, mis on jälgimise eesmärk,“* on Andmekaitse Inspektsiooni (AKI) vaneminspektor Kadri Levandi öelnud (Levandi, 2014). Nt ekraanipildi reaalajas jälgimine on sama allika kohaselt juba tõsine privaatsuse rikkumine. AKI on teemaga põhjalikumalt tegelenud ja loonud ka vastavad juhendid (www.aki.ee/et/juhised):

- Isikuandmete töötlemine töösuhetes (maht: 83 lk);
- Töötajate arvutikasutuse privaatsus (maht: 11 lk).

Töötajate arvutikasutuse privaatsuse juhendis ("TÖÖTAJATE ARVUTIKASUTUSE PRIVAATSUS," 2013) on mh kirjas järgnev:

- töötajad peavad arvestama, et tehnilised lahendused võimaldavad tööandjal kontrollida, mida töötajad arvutivõrgus, sh internetis teevad;
- eritarkvara kasutamisel (nt tööajal seadme kasutuse ja töö efektiivsuse analüüsimiseks) peab kasutamine olema kirjas kas töölepingus või töökorralduse reeglites; töötaja peab olema sel viisil kogutud andmete töötlemise kavatsusest teadlik ja tal peab olema neile andmetele juurdepääs;
- ettevõttel on õigus töödelda töötaja isikuandmeid ulatuses, mis on vajalik tööandja arvutisüsteemide tõrgeteta töö tagamiseks;
- ettevõte ei pea töötajat kontrollimise faktist informeerima, kui kontrollimise võimalus tuleneb töötaja ja tööandja vahel sõlmitud lepingust ja eeldusel, et töötaja tegevust kontrollitakse üksnes töökohustuste täitmisega seoses.

Eelnevat silmas pidades tundub igati mõistlik sõlmida ettevõtte ja töötaja vahel konkreetsed kirjalikud kokkulepped, et oleks vähem vääriti mõistmist ja halbu üllatusi. Suuremad organisatsioonid (nagu ka AS Eesti Telekom) võiksid võtta oma hooleks ka töötajate teadlikkuse tõstmise antud teemal. Tehnoloogilisest aspektist pakuvad privaatsusküsimusele lahendust virtualiseerimise ja töö/isiklike andmete lahutamise tehnoloogiad (Chang et al., 2014).

Töötajate koolitamine

Kõigile tehnoloogilistele meetmetele vaatamata jääb alati oluliseks ohuallikaks inimtegur. Infoturbe intsidendid juhtuvad tihti just töötajate hooletusest või teadmatusest, mitte pahatahtlikkusest. VOSKi puhul peaksid töötajad saama põhjalikku koolitust, et mõista infoturbe tagamise olulisust, riske, turvapoliitika vajadust jm teemaga seonduvat (Ansaldi, 2013; Beckett, 2014; Disterer & Kleiner, 2013; Morrow, 2012). Koolituse olulisus on tulnud välja ka erinevatest uuringutest. Nt Clossler jt uuringust selgus, et töötajad ei pruugi olla teadlikud, kas ettevõttes üldse eksisteerib VOSK turvapoliitika või mitte (Crossler et al., 2014). Moyer, kes uuris põhjalikult VOSK kasutamist ja turvalisust USA haiglates (Moyer, 2013), jõudis järeldusele, et lühiajalises perspektiivis võib olla kõige mõistlikum just töötajate teadlikkuse tõstmisele panustada.

Ettevõtte VOSK koolitusi planeerides tasub õpiväljunditeks määrata (Crossler et al., 2014):

- suurenenud teadlikkus – töötajad teavad, kui tõsised on ohud, mis tekivad ebaturvalisest käitumisest;
- suurenenud enesetõhusus (*self-efficacy*) – töötajad usuvad, et suudavad soovitud viisil toimida ja nõuetele vastavalt käituda;
- suurenenud järgimise soov (*response efficacy*) – töötajad usuvad, et nendepoolne soovitud käitumine aitab tagada suuremat turvalisust ja mõistavad vastavate turvanõuete olulisust.

Tuginedes eelmises ja käesolevas peatükis kasutatud kirjandusele, on olemas piisav teoreetiline teadmus VOSK nähtuse mõistmiseks ja VOSK infoturbe analüüsimiseks organisatsioonis. Puudu jääb empiirilistest ja ettevõttespetsiifilistest andmetest, mistõttu viiakse järgnevalt läbi uuring AS Eesti Telekomis nende andmete kogumiseks.

3 UURING

Peatükis antakse ülevaade AS Eesti Telekomis läbi viidud uuringust. Esmalt tutvustatakse organisatsiooni, seejärel kirjeldatakse uuringu metoodikat ning esitatakse uuringu tulemused ja analüüs.

3.1 Ülevaade organisatsioonist AS Eesti Telekom

Alapeatükis antakse ülevaade organisatsioonist AS Eesti Telekom.

AS Eesti Telekom on IT- ja telekommunikatsioonieттevõte, kus töötab üle 2100 inimese. Peamiselt kahe kaubamärgi (EMT ja Elion) alt pakub ettevõte teenuseid nii eraisikutele kui ka ettevõtetele. Teenuseportfell on lai, sinna kuuluvad erinevad mobiili-, lairiba-, IPTV-, IT ja sisuteenused. AS Eesti Telekomi kliendilubadus on muuta kliendi elu mugavamaks lihtsalt kasutatavate ja kvaliteetsete teenuste ning parima teenindusega. Ettevõtte väärtused on:

- mõistan;
- loon väärtust;
- teen ära.

Ettevõte on osa rahvusvahelisest TeliaSonera grupist, millel on maailmas üle 25 000 töötaja ja üle 190 miljoni kliendi. ("www.telekom.ee," 2015). AS Eesti Telekomi struktuur on leitav lisast 1.

Magistritöö on tehtud AS Eesti Telekomi näitel järgnevatel põhjustel:

- Alates 2014. a. tegeletakse ettevõttes aktiivselt VOSK temaatikaga. Tehnoloogiadirektori poolt on antud korraldus, et VOSK tuleb töötajatele võimaldada ja tegeletakse sobilike lahenduste otsimise ja testimisega.
- Ettevõtte töötajate seas on nutiseadmete kasutamine tõenäoliselt laialt levinud, sest seadmete soetamiseks pakutakse väga soodsaid tingimusi ja kiiret mobiilset internetiühendust.
- Tegemist on Eesti kontekstis suure ja maineka ettevõttega, mis saab olla teistele organisatsioonidele VOSKi edukal ning turvalisel juurutamisel eeskujuks.

- Töö autor on ettevõttega töösuhtes ja omab seetõttu ligipääsu informatsioonile. Magistritöö tulemustest võib olla kasu ka ettevõttele.

3.2 Metoodika

Alapeatükis kirjeldatakse uurimuse metoodikat.

Tegemist on ühe ettevõtte põhise kvalitatiivse juhtumiuuringuga, kus nähtust uuritakse selle loomulikus keskkonnas. Juhtumiuuring on eelistatud lähenemisviis, kui fookuses on reaalse elu kontekstis aset leiduv nähtus ja kui uuritavat nähtust on raske uurida väljaspool selle loomulikku keskkonda (Ghauri & Grønhaug, 2004). Tulenevalt teema spetsiifilisusest kaasati uuringusse ettevõttesisene ekspert Aivo Koger, kes töötab AS Eesti Telekomis infoturbe spetsialistina (*Information Security Officer*) ja tegeleb ka VOSK infoturbe valdkonnaga.

Kuna vajaduseks oli saada võimalikult põhjalikku ja detailset ekspertteavet, siis osutus sobivaimaks andmete kogumise meetodiks struktureerimata süvaintervjuu. Intervjuud toimusid perioodil september 2014 kuni märts 2015 näost näkku kohtumistena, minnes samm-sammult teemas detailsemaks ja jõudes välja järgmises alapeatükis esitatud tulemusteni. Lisaks toimus intervjuude läbiviimise perioodil aktiivne suhtlus magistritöö autori ja Kogeri vahel e-posti ning telefoni vahendusel, mis võimaldas kogutavaid andmeid pidevalt täpsustada. Võimalike vigade vältimiseks andmete kogumisel ja tõlgendamisel esitati pärast igat intervjuud kirja pandud andmed intervjueeritavale üle vaatamiseks.

3.3 Tulemused

Alapeatükis esitatakse AS Eesti Telekomis läbi viidud uuringu tulemused.

VOSK olukord AS Eesti Telekomis

Alates 2014. a on AS Eesti Telekomis tegeletud aktiivselt VOSKi võimaldamisega. Teemaga tegeletakse eelkõige omal initsiatiivil ja lähtuvalt ettevõtte vajadustest (mitte nt emaettevõtte poolt tulenevast kohustusest). VOSKi soovitakse võimaldada kõigile töötajatele, küll aga ei ole

tõenäoline kõigi ärirakenduste võimaldamine igas seadmes, pigem teatav kompromisslahendus. Hetkeolukord on järgnev:

- sülearvutist on ligipääs kõigele – Cisco Anyconnect tarkvara (VPN);
- igast seadmest on ligipääs piiratud infole – Cisco Anyconnect portaal (veebiproksi);
- mobiilsest seadmest ligipääs piiratud infole – Cisco Anyconnect VPN mobiilis läbi Citrix XenMobile MDM lahenduse.

Võimalikud privaatsusküsimused on adresseeritud lihtsa põhimõttena: VOSK on vabatahtlik, aga kui soovid töötajana endale seda täiendavat mugavust, siis pead nõustuma ettevõtte tingimustega.

MDM lahendusena on kasutusel Citrix XenMobile, mida hetkel testitakse piiratud sihtgrupi peal (aktiivne testgrupp ca 40 töötajat) ja mida plaanitakse tulevikus võtta kasutusele ettevõtte üleselt. Töötaja jaoks toimib lahendus järgnevalt:

1. töötaja paigaldab omal soovil isiklikku mobiilsesse seadmesse MDM tarkvara;
2. MDM tarkvara paigaldab ja seadistab automaatselt seadmesse Cisco Anyconnect VPNi;
3. töötaja pääseb ligi infole ja rakendustele, mida ettevõte on otsustanud sellisel teel ligipääsetavaks teha.

Ettevõttele tekib seeläbi register mobiilsetest seadmetest, mida on võimalik distantsilt hallata. MDM lahendus on vajalik ka sellepärast, et lisaks tavapärasele paroolile on Cisco Anyconnect VPNil ka sertifikaadiga autentimine, mille digitaalse sertifikaadi ja privaatvõtme saab seade ainult läbi MDMi ettevõtte avaliku võtme taristust (PKI).

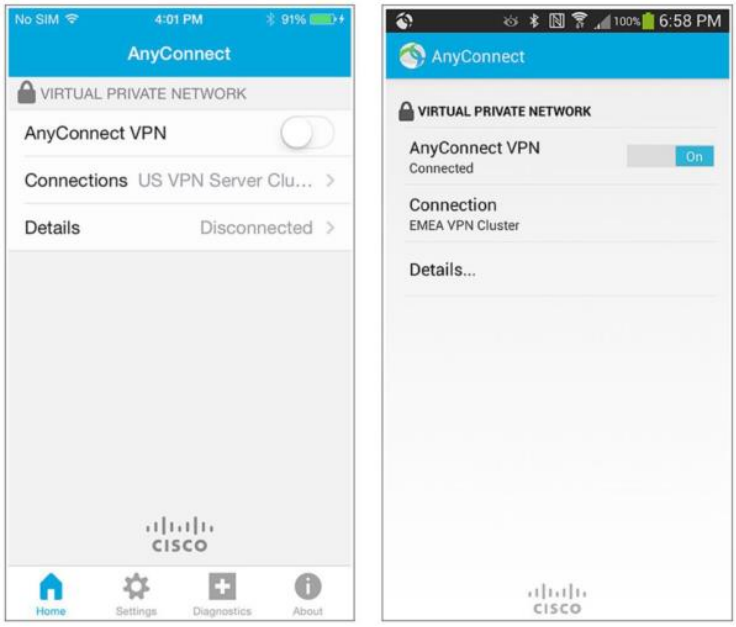
Cisco AnyConnect mobiilsetele seadmetele

AS Eesti Telekomis kasutusel olev Cisco AnyConnect tarkvara mobiilsetele seadmetele kasutab eelkõige järgnevaid turvatehnoloogiaid:

- *Datagram Transport Layer Security* (DTLS);
- IPsec (IKEv2);
- TLS (HTTP *over* TLS/SSL).

Krüpteeritud ühenduse kaudu pääseb tarkvara abil distantsilt mobiilsete seadmete kaudu ligi ettevõtte siserakendustele. Tarkvara toimib Apple iOS 6.0+, Android 4.0+, valitud Amazon Kindle ja Fire Phone operatsioonisüsteemidel, Windows Phone'i tugi puudub. (Cisco, 2015).

Kasutajaliides (vt joonis 5) on töötaja jaoks lihtne ja mugav. Cisco AnyConnect mobiilsetele seadmetele täpsem funktsionaalsuse kirjeldus on toodud välja lisas 2.



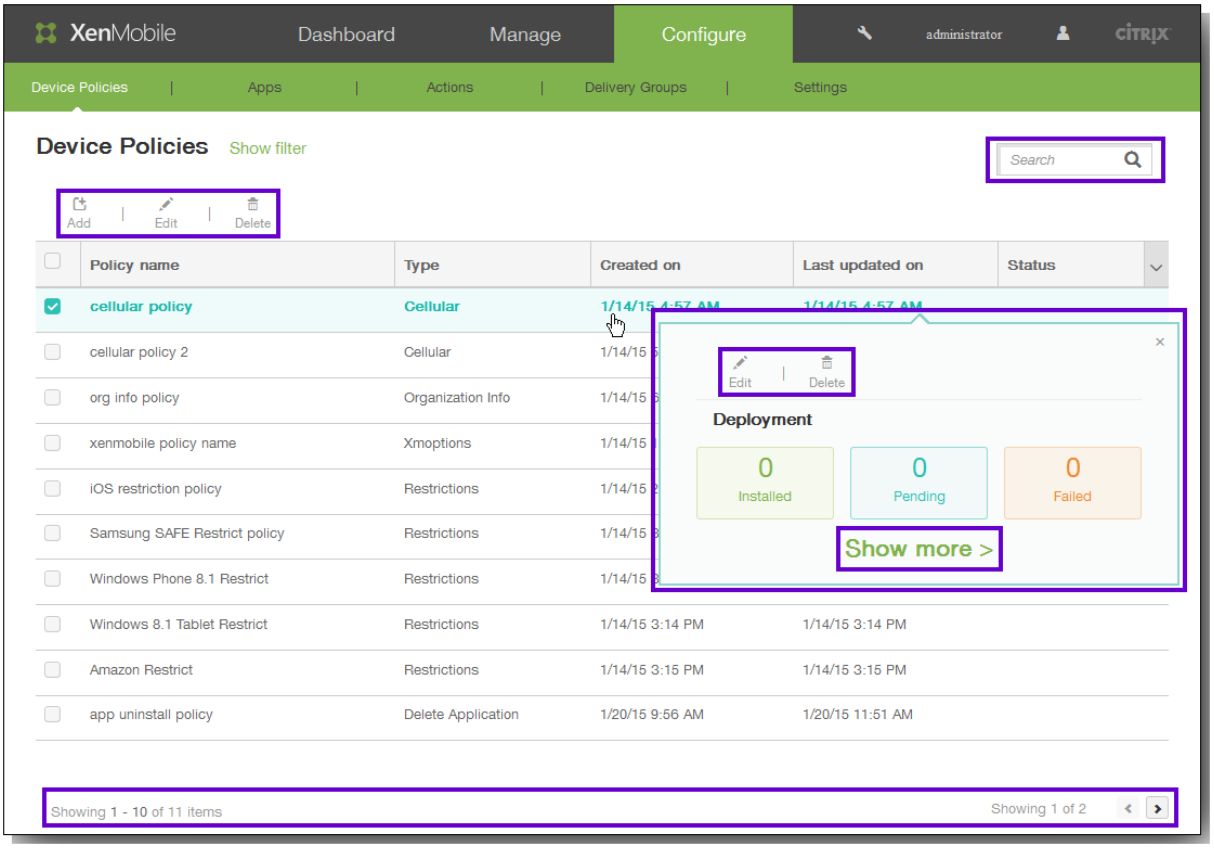
Joonis 5. Cisco AnyConnect kasutajaliides Apple iOS ja Android operatsioonisüsteemidel (Cisco, 2015).

Citrix XenMobile

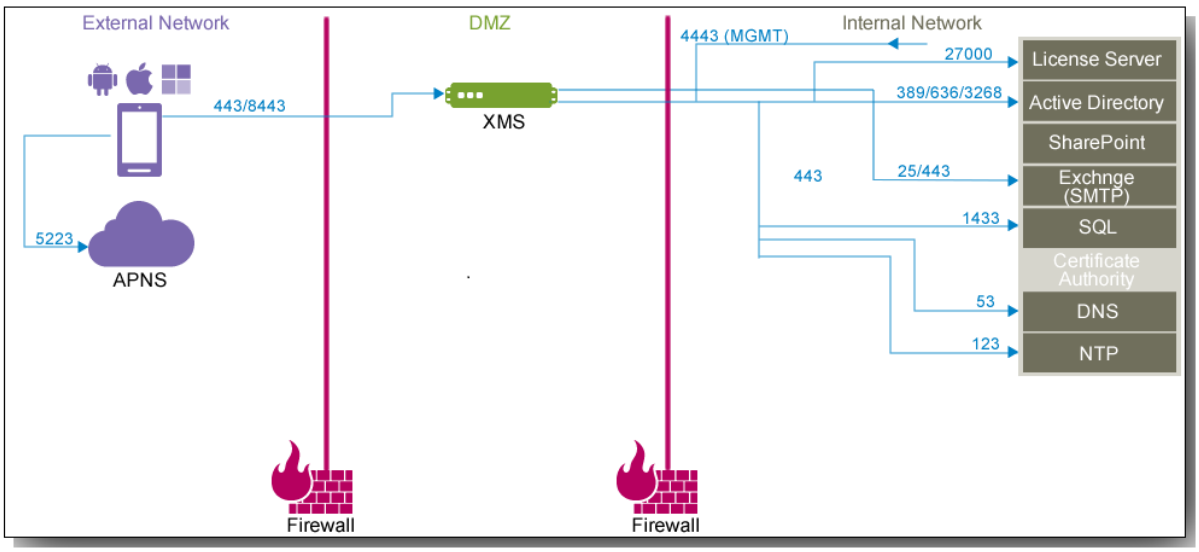
AS Eesti Telekomis kasutusel olev Citrix XenMobile tarkvara on tootja väitel kõik-ühes EMM lahendus, mis sisaldab nii MDM kui ka MAM funktsionaalsusi (Citrix, 2015c). Lihtsalt öeldes tähendab see, et tööriist pakub turvamis- ja haldusvõimekust nii seadmetele kui ka rakendustele. Põhjalikum funktsionaalsuse kirjeldus on esitatud lisas 3. Kui süsteem on paigaldatud ja toimiv, siis on igapäevane haldus lihtsasti tehtav läbi administraatori kasutajaliidese (vt joonis 6). Ka uute turvapoliitikate loomine ja olemasolevate muutmine on üllatavalt käepäraseks suudetud teha (vt joonis 7).

Ettevõtte IT arhitektuuris soovitatakse XenMobile paigaldada demilitaartsooni (DMZ) sise- ja välisvõrgu vahele. Tüüparhitektuuri joonisel (joonis 8) on kujutatud kõige lihtsamat paigalduslahendust, millest on praegu lähtutud ka AS Eesti Telekomis. Sinise värviga on tähistatud avatud portide numbrid; XMS tähistab XenMobile serverit.

Joonis 6. Citrix XenMobile kasutajaliides administraatorile (Citrix, 2015a).



Joonis 7. Citrix XenMobile turvapoliitikate haldamine administraatori kasutajaliideses (Citrix, 2015a).



Joonis 8. Citrix XenMobile tüüparhitektuuri joonis (Citrix, 2015a).

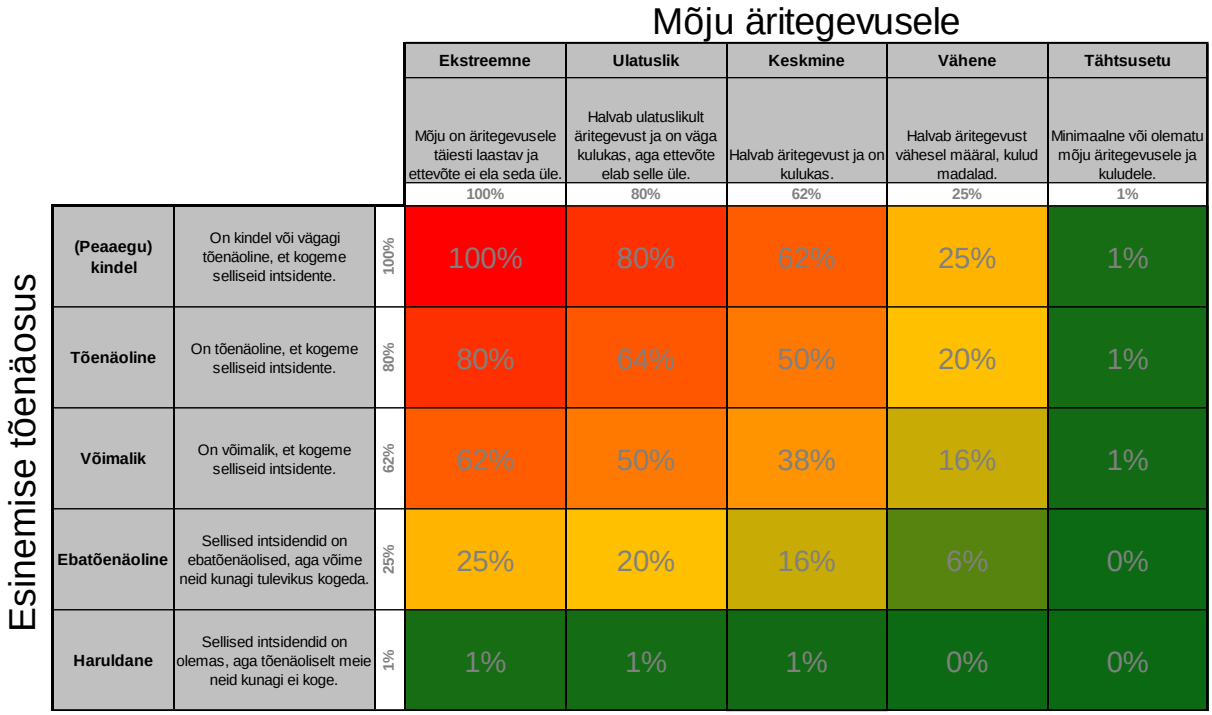
VOSK riskid AS Eesti Telekomis

AS Eesti Telekomis on infoturbe riskide haldamisel kasutusel „ISO27k Toolkit“ riskiregister (Koger, 2015). ISO (*International Organization for Standardization* ehk Rahvusvaheline Standardiorganisatsioon) on väga paljude eri riikide standardimisasutusi ühendav organisatsioon. ISO 27000 (ehk ISO27k) standardipere standardid käsitlevad infoturbe halduse süsteeme ja nendega seonduvat. (Veldre et al., 2015). „ISO27k Toolkit“ riskiregister on antud standardiperes levinud tööriist, mis kujutab endast Microsoft Exceli tabelit, kuhu lisatakse ja uuendatakse tabelis 4 välja toodud infot. Sama tööriista (“ISO27k Toolkit,” 2015) kasutatakse ka antud magistritöös. Kõiki riske hinnatakse teljestik-maatriksil, milles on üheks teljeks riski esinemise tõenäosus (*probability*) ja teiseks teljeks riski realiseerumise mõju äritegevusele (*business impact*). Kahel teljel asuvate väärtuste korrutamisel saadakse riski koondhinnang protsendina ning sellele lisatakse automaatselt ka visuaalne tähistus värvina (roheline, kollane, punane või nende vahepealne toon) – vt. joonis 9.

Pealkiri	**Selgitus**
ID	Unikaalne tähis.
Risk	Riski kirjeldus lühidalt.
Omanik	Isik, kes vastutab riskiga tegelemise ja tagajärgede eest, kui risk peaks realiseeruma.
Mõju	Kirjeldus, milline on mõju riski realiseerumisel?
Esialgne tõenäosus	Esinemise tõenäosus juhul, kui riskiga ei tegeleta (protsent)**.**
Esialgne mõju	Mõju ulatus, kui riskiga ei tegeleta (protsent)**.**
Esialgne riskimäär	Esialgne tõenäosus x esialgne mõju = esialgne riskimäär (kui riskiga ei tegeleta).
Meede	Kuidas riskiga tegeletakse? Milline meede või otsus (eirata/aktsepteerida).
Meetme kulu	Kui suur kulu kaasneb?
Meetme staatus	0% = idee/plaan. 100% = toimiv meede.
Meetmejärgne tõenäosus	Esinemise tõenäosus juhul, kui riskiga on tegeletud (protsent).
Meetmejärgne mõju	Mõju ulatus, kui riskiga on tegeletud (protsent).
Meetmejärgne riskimäär	Meetmejärgne tõenäosus x meetmejärgne mõju = meetmejärgne riskimäär (kui riskiga on tegeletud).
Praegune riskimäär	Praegune riskimäär, mis arvestab meetme staatust.

Kommentaar	Olulised märkmed või kommentaarid.
Viimane muudatus	Kuupäev, millal riskiga on tegeletud (muudetud, üle vaadatud, uuendatud vm).

Tabel 4. ISO27k riskide register – tüüpinfo (“ISO27k Toolkit,” 2015).



Joonis 9. ISO27k riskide register – maatriks (“ISO27k Toolkit,” 2015).

ISO27k registrisse on kantud sisendinfo peatükist “VOSK infoturbe ohud“ – vt. tabel 5.

Riski ID	**Risk**	**Mõju**
VOSK_15/2_1	Konfidentsiaalsete andmete leke	Ärisaladuse leke, kliendiandmete leke, konkurentsieelise kaotus, maine langemine, seaduse rikkumine, finantskaotus.
VOSK_15/2_2	Andmete saaste	Ebaolulised, konfidentsiaalsed või kahjulikud (nt ründetarkvaraga nakatunud) andmed võivad sattuda tagavarakoopiatele või failiserveritesse ning sealt edasi levida. Konfidentsiaalsed andmed võivad töötaja kaudu koos isiklike andmetega lekkida.
VOSK_15/2_3	Ründetarkvaraga nakatumine	Ründetarkvara tulemusel võivad lekkida konfidentsiaalsed andmed, tekkida ligipääs ettevõtte süsteemidele, toimuda andmetega manipuleerimine ja tööprotsesside häirimine.

VOSK_15/2_4	Õngitsemine (*phishing*)	Võidakse seadmesse paigaldada nuhk- ja ründetarkvara, mis saadavad infot ja võimaldavad kavandada suuremaid rünnakuid ettevõtte infosüsteemidele.
VOSK_15/2_5	Tüssamine/spuufimine (*spoofing*)	Pahatahtlikud isikud võivad etendada usaldusväärseid teenuseosutajaid, et käivitada võltssuhtlemist või vastupidiselt etendada usaldusväärset kasutajat teenusepakkujatele. Tõenäoline kasutajakontode ligipääsude leke, ründetarkvaraga nakatumine.
VOSK_15/2_6	Urkimine (*tampering*)	Konfidentsiaalsete andmete leke, andmetega manipuleerimine.
VOSK_15/2_7	Ebaturvaline failijagamine	Konfidentsiaalsete andmete leke, andmetega manipuleerimine, andmete kustumine.
VOSK_15/2_8	Seadme kaotus	Konfidentsiaalsete andmete leke, varaline kahju.
VOSK_15/2_9	Seadme vargus	Konfidentsiaalsete andmete leke, varaline kahju.
VOSK_15/2_10	Puudulik turvapoliitikate jõustamine	Seadmete turvalisus ebapiisav, puudulik kontroll ja haldusvõimekus.
VOSK_15/2_11	MDM süsteemi tungimine	Võimalik kontrollida kõiki ettevõtte mobiilseid seadmeid ja nendes sisalduvaid andmeid (lähtuvalt MDM funktsionaalsusest).
VOSK_15/2_12	Inimtegur	Konfidentsiaalsete andmete leke, ründetarkvaraga nakatumine, andmete manipuleerimine, ligipääs ettevõtte süsteemidele.

Tabel 5. ISO27k riskide register – riskide ja võimalike mõjude kirjeldused.

A. Kogeri ekspertteadmisele tuginedes on hinnatud tabelis 5 välja toodud riskide tõenäosust ja mõju; kirjeldatud olemasolevate meetmed ja vajadusel lisatud kommentaarid. Tulemused on esitatud tabelis 6 reastatuna lähtuvalt praegusest riskimäärast. Peamised VOSK infoturbe riskid AS Eesti Telekomis (praeguse riskimäära järgi) on:

1) ebaturvaline failijagamine;
2) konfidentsiaalsete andmete leke;
3) andmete saaste;
4) ründetarkvaraga nakatumine;
5) inimtegur;
6) puudulik turvapoliitikate jõustamine.

RISKI ID	ESIALGNE TÕENÄOSUS	ESIALGNE MÕJU	ESIALGNE RISKIMÄÄR	MEEDE	MEETME KULU	MEETME STAATUS	MEETMEJÄRGNE TÕENÄOSUS	MEETMEJÄRGNE MÕJU	MEETMEJÄRGNE RISKIMÄÄR	PRAEGUNE RISKIMÄÄR	KOMMENTAAR
VOSK_15/2_7	75%	70%	53%	Ettevõtte sisemise pilve loomine turvaliseks failivahetuseks (DropBox, OneDrive jt).	14000€	50%	**10%**	70%	7%	30%	
VOSK_15/2_1	40%	80%	32%	Mobiilseadme infovahetus ettevõtte infosüsteemidega ainult läbi VPN kanali, iga VPN sessiooni käivitamisel kaheastmeline autentimine ja seadme kaugelt tühjendamise võimalus.	83000€	70%	**20%**	80%	16%	21%	Staatus: VPN ja MDM kaughalduse tugi olemas, kuid hetkel kasutavad ainult osad töötajad.
VOSK_15/2_2	30%	75%	23%	Konfidentsiaalseid andmeid ei hoita seadmes, vaid ettevõtte infosüsteemides.	0	40%	**15%**	75%	11%	18%	
VOSK_15/2_3	25%	50%	13%	Android seadmetele pakutakse välja viirusetõrje.	0	20%	**10%**	50%	5%	11%	
VOSK_15/2_12	25%	50%	13%	Teadlikkuse tõstmine juhendite ja koolituste näol.	0	50%	**10%**	50%	5%	9%	
VOSK_15/2_10	80%	40%	32%	Seadmes ei hoita konfidentsiaalseid andmed ning kõik seadistused saab kaugelt tühjendada MDM abil.	0	100%	**10%**	40%	4%	4%	
VOSK_15/2_4	5%	50%	3%	Android seadmetele pakutakse välja viirusetõrje.	0	20%	**2%**	50%	1%	2%	
VOSK_15/2_6	5%	20%	1%	Manipuleerimise vastu meetmed puuduvad.	0	0%	5%	20%	1%	1%	
VOSK_15/2_11	2%	50%	1%	MDM süsteemi haldusliides ei ole kättesaadav avalikust võrgust ning MDM ei võimalda ligipääsu seadmes olevatele andmetele.	0	100%	**50%**	**0%**	0%	0%	

RISKI ID	ESIALGNE TÕENÄOSUS	ESIALGNE MÕJU	ESIALGNE RISKIMÄÄR	MEEDE	MEETME KULU	MEETME STAATUS	MEETMEJÄRGNE TÕENÄOSUS	MEETMEJÄRGNE MÕJU	MEETMEJÄRGNE RISKIMÄÄR	PRAEGUNE RISKIMÄÄR	KOMMENTAAR
VOSK_ 15/2_9	5%	40%	2%	Seadmes ei hoita konfidentsiaalseid andmed ning kõik seadistused saab kaugelt tühjendada MDM abil.	0	90%	5%	**4%**	0%	0%	Tõenäosus ei muutu, küll aga meede aitab vähendada mõju
VOSK_ 15/2_8	5%	30%	2%	Seadmes ei hoita konfidentsiaalseid andmed ning kõik seadistused saab kaugelt tühjendada MDM abil.	0	90%	5%	**3%**	0%	0%	Tõenäosus ei muutu, küll aga meede aitab vähendada mõju
VOSK_ 15/2_5	5%	10%	1%	Ettevõtte rakendused on kaitstud SSL-iga ja juursertifikaadid on lisatud kaughaldusega mobiilsetesse seadmetesse. MITM ja *spoofing* tüüpi ründeid ei saa täielikult välistada, kuid vigane sertifikaat võiks anda töötajale märku ohust.	0	100%	**2%**	10%	0%	0%	

Tabel 6. ISO27k riskide register – tõenäosused, mõjud, meetmed ja kommentaarid.

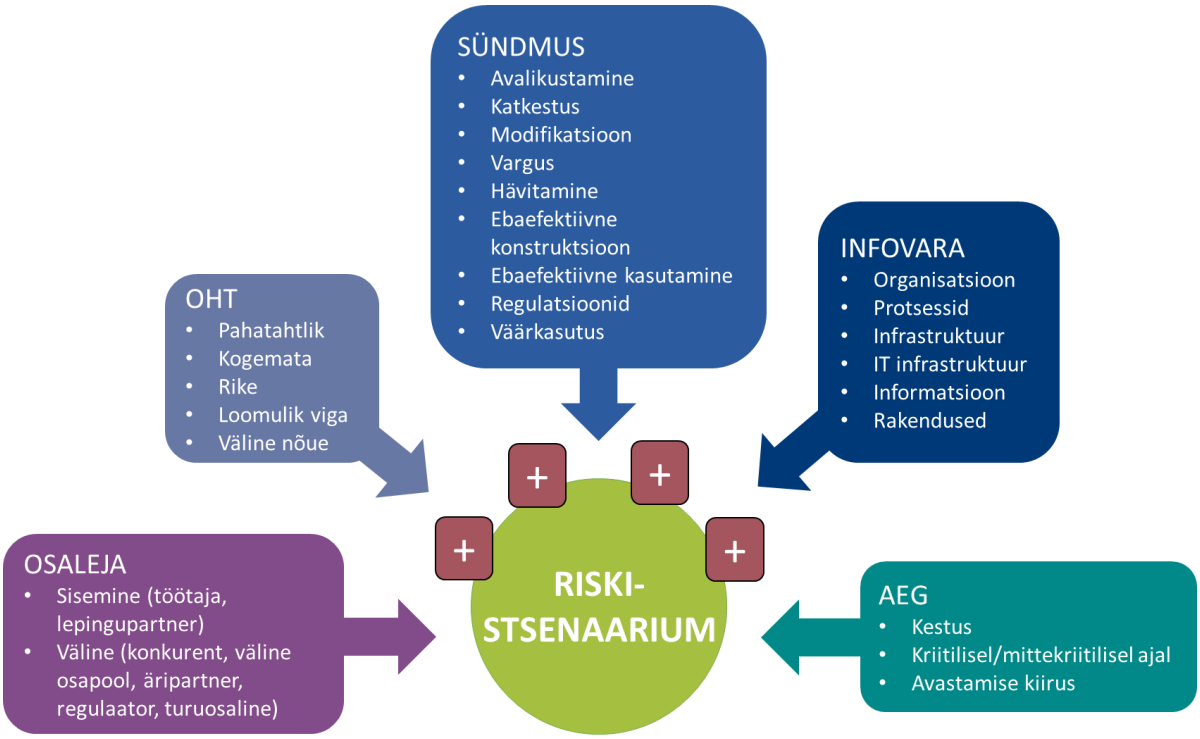
3.4 Analüüs

Alapeatükis esitatakse uuringu tulemuste analüüs.

Kõigepealt esitatakse detailsed riskistsenaariumid kuue riski kohta, mille praegune riskimäär on tabelis 6 kõige kõrgem, seejärel analüüsitakse samu riske kikilipsu meetodil (*bow-tie risk assessment*). Kuna ülejäänud riskide riskimäär on väga madal (vaid 0-2%), siis nende kohta riskistsenaariumeid ja kikilipsu analüüsi ei koostata.

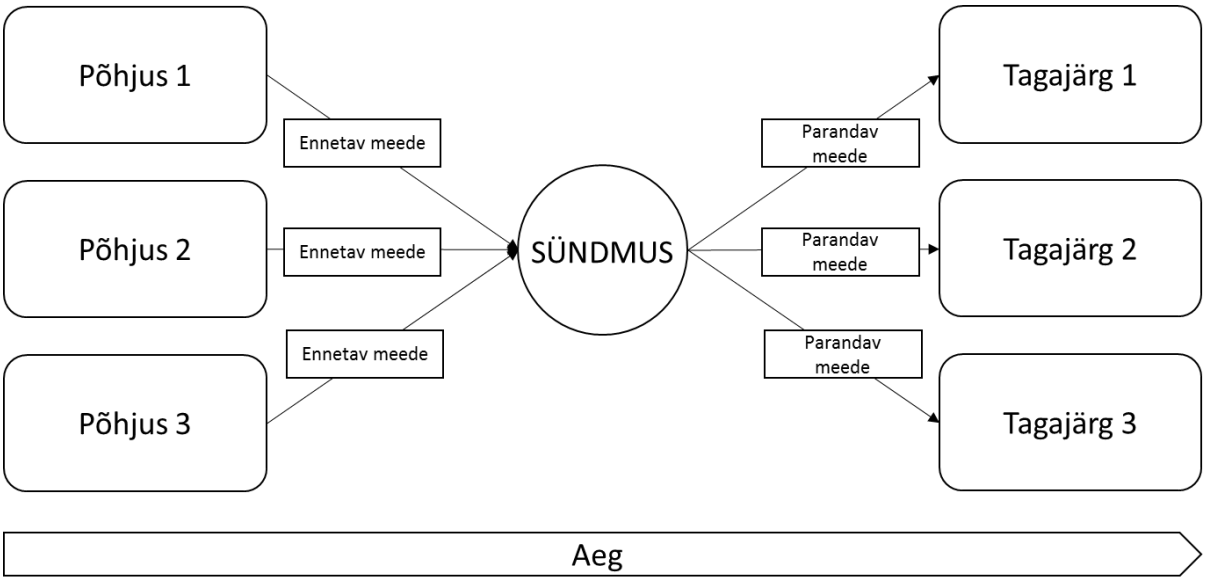
Riskistsenaariumite kirjeldamisel lähtutakse RISK IT raamistikust (ISACA, 2009), mille kohaselt on riskistsenaariumil järgnevad olulised komponendid (vt ka joonis 10):

- osaleja;
- oht;
- sündmus;
- infovara;
- aeg.



Joonis 10. RISK IT raamistiku riskistsenaariumi komponendid (ISACA, 2009).

Kikilipu meetod on küllaltki universaalne (sobib riskide hindamiseks eri valdkondades) praktilise suunitlusega kvalitatiivne riskihindamise tööriist, mille abil visualiseeritakse ohtude, sündmuste, ennetavate ja parandavate meetmete ning tagajärgede omavahelised seosed. Kikilipsu meetodi plussiks on läbipaistvus, sest meetod toob selgelt välja teekonna põhjusest tagajärjeni ehk põhjus-tagajärg seosed. Meetod on lihtsasti kasutatav ja selle kasutegurina nähakse ka ennetavate ja parandavate meetmete selget eristamist, mis võimaldab tähelepanu suunata eelkõige ennetavatele meetmetele ja soovimatute sündmuste ärahoidmisele. Klassikalise kikilips-diagrammi (vt joonis 11) keskel on kriitiline sündmus (nt infoturbe intsident), millest vasakule jäävad põhjused ning paremale tagajärjed. Mõlemale poolele lisatakse riskide haldamise meetmed: vasakule ennetavad ja paremale parandavad. (Aqlan & Mustafa Ali, 2014; Cockshott, 2005; Jacinto & Silva, 2010).



Joonis 11. Tüüpiline kikilips-diagramm (Aqlan & Mustafa Ali, 2014; Jacinto & Silva, 2010).

Riskistsenaarium 1 – ebaturvaline failijagamine (VOSK_15/2_7)

Osaleja on eelkõige sisemine – töötaja, kes soovib kiirelt, lihtsalt ja mugavalt faile jagada. Osaleja võib olla ka väline, nt partner, kellega jagatakse poolelioleva projekti faile välises failijagamise keskkonnas (nt Dropbox, OneDrive Google Drive). Ohu liigid on antud riski puhul pahatahtlik (kolmas osapool, nt konkurent hangib ligipääsu andmetele), kogemata (nt unustatakse märkida, et andmed on privaatsed ja tehakse need kogemata kõigile internetis nähtavaks) või rike (nt oluliste andmete hävimine rikke tõttu või puudulik ligipääs neile). Sündmuseks võib olla avalikustamine, modifikatsioon, vargus, hävitamine, väärkasutamine. Riski kõige tõenäolisem mõju on konfidentsiaalsete andmete leke, andmetega manipuleerimine,

andmete kustumine. Ohustatud infovara ongi eelkõige erinevad andmed (pooleliolevad projektid, ärisaladused, isiku- või kliendiandmed). Ajafaktor ei ole antud riski puhul määrava olulisusega, pigem on risk ajaliselt pidev ja püsiv seni, kuni ebaturvaline failijagamine toimub. Ajastus võib muutuda määravaks oluliste sündmuste eel (nt uue teenuse lansseerimisel).

Riski esialgne mõju äritegevusele on 70% (keskmine kuni ulatuslik) ehk halvab realiseerudes äritegevust ja on ettevõttele kulukas. Esinemise esialgne tõenäosus on 75% s.t pigem tõenäoline. Kokku on esialgne riskimäär (mõju*tõenäosus) 53%. Leevendamata kujul on tegemist kõige ohtlikuma VOSK riskiga AS Eesti Telekomis, mistõttu tuleb riskiga kindlasti tegeleda. Sobiliku meetmena riski leevendamiseks nähakse ettevõtte sisese pilve loomist turvaliseks failivahetuseks. See tähendab, et kõik andmed asuvad ettevõtte valitud serverites ja töötajatele jääb alles mugava ja harjumuspärase pilveteenuse kasutamise võimalus. Meede panustab riski realiseerumise tõenäosuse vähendamisele ja selle rakendamise investeeringu suurus on hinnanguliselt 14 000€. Vastav projekt on ka juba töös, meetme rakendamise staatus on hetkel 50% (0% = idee/plaan, 100% = toimiv meede.). Meetmejärgne (s.t kui meede on 100% rakendunud) riskimäär on 7%, mis tähendab, et mõju äritegevusele on vähene ja esinemine ebatõenäoline. Tulenevalt võib järeldada, et valitud meede on riski leevendamiseks piisav ja sobilik. Kuna hetkel pole meede veel 100% jõustunud, siis on praegune riskimäär 30%, mis tähendab, et riskist tulenevaid intsidente võib esineda ja nende mõju äritegevusele võib olla vähene või keskmine.

Riskistsenaarium 2 - konfidentsiaalsete andmete leke (VOSK_15/2_1)

Osaleja on sisemine ja/või väline. Konfidentsiaalset infot võib lekitada töötaja, hankida väline huvitatud osapool või toimuda nende kahe omavaheline koostöö. Ohu liigid on pahatahtlik (info lekitamine, varastamine), kogemata (nt teadmatusest või lohakusest) või rike (nt mõni turvasüsteem ei toimi). Sündmuseks on eelkõige avalikustamine, vargus, väärkasutus. Infovarana on otseselt ohus informatsioon, kaudselt ka teised komponendid. Mõjuks võib olla ärisaladuse leke, kliendiandmete leke, konkurentsieelise kaotus, maine langemine, seaduse rikkumine, finantskaotus. Konfidentsiaalsete andmete lekke puhul on äärmisel oluline avastamise kiirus, et oleks võimalik reageerida (nt kasutajakontode andmete lekkimisel saab muuta paroolid; kliendiandmete lekkel saab kliente teavitada jne).

Riski esialgne mõju äritegevusele on 80% (ulatuslik) ehk halvab ulatuslikult äritegevust ja on väga kulukas, aga ettevõte elab selle üle. Esinemise esialgne tõenäosus on 40% s.t pigem

ebatõenäoline. Kokku on esialgne riskimäär (mõju*tõenäosus) 32%. Leevendamata kujul ei tundu esialgu tegemist olevat väga tõsise riskiga, aga tulenevalt väga suurest potentsiaalsest mõjust äritegevusele peab riskiga kindlasti tegelema. Sobiliku meetmena riski leevendamiseks nähakse, et mobiilseadme infovahetus ettevõtte infosüsteemidega toimub ainult läbi VPN kanali. Seejuures rakendub iga VPN-sessiooni käivitamisel kaheastmeline autentimine ja seadme kaugelt tühjendamise võimalus. Meede panustab riski realiseerumise tõenäosuse vähendamisele. Meetme rakendamise investeeringu suurus on hinnanguliselt 83 000€ ja meetme rakendamise staatus on hetkel 70%. Tegemist on kõige kulukama VOSK infoturbe tagamise meetmega AS Eesti Telekomis, aga arvestades mobiilsete seadmete ulatuslikku kasutamist on investeeringu vajadus mõistetav. Meetmejärgne (s.t kui meede on 100% rakendunud) riskimäär on 16%, mis tähendab, et mõju äritegevusele on vähene ja esinemine ebatõenäoline. Valitud meede on küll kulukas, aga riski leevendamiseks vajalik ja piisav. Kuna hetkel pole meede veel 100% jõustunud, siis on praegune riskimäär 21%.

Riskistsenaarium 3 - andmete saaste (VOSK_15/2_2)

Osaleja võib olla nii sisemine kui ka väline. Oht tuleneb pahatahtlikkusest või kogemata. Ebaolulised, konfidentsiaalsed või kahjulikud (nt ründetarkvaraga nakatunud) andmed võivad sattuda tagavarakoopiatele või failiserveritesse ning sealt edasi levida. Konfidentsiaalsed andmed võivad töötaja kaudu koos isiklike andmetega lekkida. Seega sündmuseks võib olla avalikustamine, modifikatsioon, vargus, hävitamine, ebaefektiivne kasutamine, väärkasutus. Ohustatud infovara on eelkõige informatsioon, kaudsemalt ka erinevad rakendused. Andmete saaste võib toimuda pika aja jooksul ja märkamatult.

Riski esialgne mõju äritegevusele on 75% (keskmine kuni ulatuslik) ehk halvab realiseerudes äritegevust ja on ettevõttele kulukas. Esinemise esialgne tõenäosus on 30% s.t pigem ebatõenäoline. Kokku on esialgne riskimäär (mõju*tõenäosus) 23%. Sobiliku meetmena riski leevendamiseks nähakse reeglit ja töökorraldust, et konfidentsiaalseid andmeid ei hoita seadmetes, vaid ettevõtte infosüsteemides. Meede panustab riski realiseerumise tõenäosuse vähendamisele ja meetme rakendamisega täiendavat investeeringut VOSK kontekstis ei kaasne, sest infosüsteemide turvalisusega tagamisega on juba tegeletud ja tegeletakse jätkuvalt ka VOSK konteksti väliselt. Meetme rakendamise staatus on hetkel 40%, tulenevalt on praegune riskimäär 18%. Meetmejärgne riskimäär on 11%, mis tähendab, et mõju äritegevusele on vähene ja esinemine ebatõenäoline.

Riskistsenaarium 4 - ründetarkvaraga nakatumine (VOSK_15/2_3)

Osaleja võib olla väline (ründetarkvara autor, huvitatud kasutaja) ja sisemine (töötaja, kes enda teadmata või tahtlikult ründetarkvaraga nakatab). Oht tuleneb pahatahtlikkusest või kogemata. Sündmuseks võib olla avalikustamine, katkestus, modifikatsioon, vargus, hävitamine, väärkasutus. Ründetarkvara tulemusel võivad lekkida konfidentsiaalsed andmed, tekkida ligipääs ettevõtte süsteemidele, toimuda andmetega manipuleerimine ja tööprotsesside häirimine. Ründetarkvara puhul on väga oluline avastamise kiirus, et oleks võimalik reageerida.

Riski esialgne mõju äritegevusele on 50% (keskmine) ehk halvab realiseerudes äritegevust ja on ettevõttele kulukas. Esinemise esialgne tõenäosus on 25% s.t ebatõenäoline. Kokku on esialgne riskimäär (mõju*tõenäosus) võrdlemisi madal: 13%. Sobiliku meetmena riski leevendamiseks nähakse Android seadmetel viirusetõrje tarkvara kasutamist. Vastav tarkvara peaks olema suuteline ründetarkvara tuvastama ja kahjutuks tegema. Meede panustab riski realiseerumise tõenäosuse vähendamisele. Kuna rahalist investeeringut ei planeerita teha, siis mõeldakse tõenäoliselt vabavara kasutamisele, jäetakse vastavad kulud töötajate kanda või omatakse juba ostetud litsentsidega ka mobiilsete seadmete tuge. Meetme rakendamise staatus on hetkel 20%, tulenevalt on praegune riskimäär 11%. Meetmejärgne riskimäär on 5%, mis tähendab, et risk on sellisel juhul väga hästi leevendatud.

Riskistsenaarium 5 - inimtegur (VOSK_15/2_12)

Riski puhul on osaleja sisemine ja oht tekib pahatahtlikkusest, teadmatusest või ettevaatamatusest (kogemata). Sündmuseks võib olla avalikustamine, katkestus, modifikatsioon, vargus, hävitamine, ebaefektiivne konstruktsioon, ebaefektiivne kasutamine, väärkasutus. Infovaradena on ohus eelkõige informatsioon, rakendused ja protsessid. Avastamise kiirus võib olla aeglane, sest inimene võib üritada oma eksimust või pahatahtlikku tegu varjata; sellist tegevust võib olla keeruline tuvastada enne, kui eksisteerivad selged tagajärjed.

Riski esialgne mõju äritegevusele on 50% (keskmine) ehk halvab realiseerudes äritegevust ja on ettevõttele kulukas. Esinemise esialgne tõenäosus on 25% s.t ebatõenäoline. Kokku on esialgne riskimäär (mõju*tõenäosus) võrdlemisi madal: 13%. Sobiliku meetmena riski leevendamiseks nähakse ennetavaid tegevusi juhendite ja koolituste näol töötajate teadlikkuse tõstmiseks. Meede panustab riski realiseerumise tõenäosuse vähendamisele. Kuna otsest rahalist investeeringut ei planeerita teha, siis mõeldakse tõenäoliselt sisekoolitustele (kulud

eksisteerivad, aga on kaudsed, nt palgakulu, ruumirent). Meetme rakendamise staatus on hetkel 50%, tulenevalt on praegune riskimäär 9%. Meetmejärgne riskimäär on 5%, mis tähendab, et risk on sellisel juhul väga hästi leevendatud.

Riskistsenaarium 6 - puudulik turvapoliitikate jõustamine (VOSK_15/2_10)

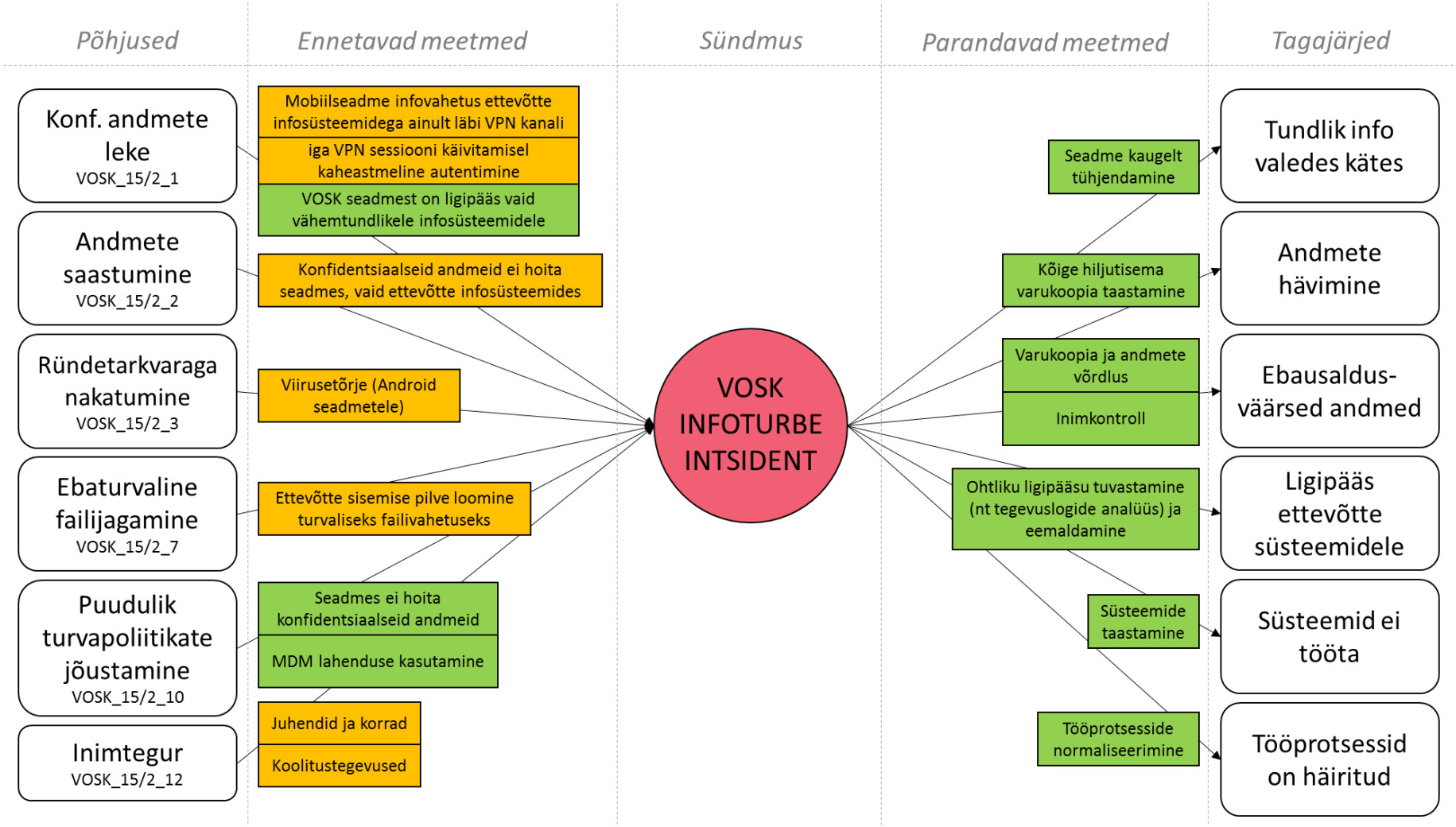
Riski puhul on osaleja sisemine. Oht võib tuleneda pahatahtlikkusest (nt töötaja ei soovi turvapoliitikate jõustamist), rikkest (turvapoliitikate automaatne jõustamine ei toimi), välisest nõudest (töötaja õigus privaatsusele). Sündmuseks võib olla avalikustamine, vargus, väärkasutus. Seadmete turvalisus on ebapiisav, kontroll ja haldusvõimekus puudulikud. Infovaradena on ohus eelkõige informatsioon ja rakendused. Ajalise faktori puhul võiks arvestada, et jõutamine toimuks automaatselt (võimalikult kiirelt ja mugavalt) ja kõrvalekallete avastamine toimuks võimalikult kiiresti (nt automaatne teavitus).

Riski esialgne mõju äritegevusele on 40% (vähene, aga keskmisele lähenev). Esinemise esialgne tõenäosus on 80% s.t tõenäoline. Kokku on esialgne riskimäär (mõju*tõenäosus): 32%. Sobiliku meetmena riski leevendamiseks nähakse, et seadmetes ei hoita konfidentsiaalseid andmeid ning kõiki seadistusi saab distantsilt juhtida kasutusel oleva MDM süsteemi abil. Meede panustab riski realiseerumise tõenäosuse vähendamisele ja rakendamise staatus on 100%. Tulenevalt on praegune ja meetmejärgne riskimäär mõlemad 4%, mis tähendab, et risk on piisavalt leevendatud.

Kikilipsu analüüs

Joonisel 12 on esitatud läbiviidud kikilips-analüüsi tulemused kikilips-diagrammil, mille keskmes on VOSK infoturbe intsident kui sündmus ning sellest vasakul põhjused koos ennetavate meetmetega ja paremal tagajärjed koos parandavate meetmetega. Meetmete rakendamise staatus AS Eesti Telekomis on joonisel edasi antud järgnevalt:

- roheline – rakendamise staatus on üle 80%;
- kollane – rakendamise staatus on 20-80%;
- punane – rakendamise staatus on alla 20% (joonisel puuduvad, sest sellise rakendamise staatusega meetmeid pole).



Joonis 12. Kikilips-diagramm VOSK infoturbe intsidendi kohta.

Kikilips-analüüsist selgub, et iga põhjuse ja tagajärje jaoks eksisteerivad nii ennetavad kui ka parandavad meetmed, mis näitab, et teemaga on adekvaatselt tegeletud ning mis muudab VOSKist tuleneva infoturbe intsidendi mõju ja/või tõenäosuse madalaks. Ennetavate meetmete rakendamise staatus varieerub „kollase“ ja „rohelise“ vahel, aga „kollaseid“ meetmed on hetkel ülekaalus. Tulenevalt saab siin turvalisuse astet tulevikus märgatavalt tõsta, viies ka nende meetmete rakendamise staatuse „roheliseks“. Parandavate meetmete rakendamise staatus on kõigil üle 80% ja siin tasub tulevikus jätkata meetmete aktiivsest kasutamist ja regulaarset kontrollimist-testimist.

Läbiviidud uuringu tulemusena on olemas ülevaade, milliseid lahendusi AS Eesti Telekomis VOSK põhimõtte võimaldamiseks ja turvamiseks kasutatakse. Samuti on tehtud kindlaks, millised on aktuaalsed VOSK infoturbe riskid, analüüsitud nende riskide võimalikku mõju ja esinemise tõenäosust ning esitatud meetmed riskide leevendamiseks. Lisaks on oluliste riskide kohta esitatud detailsed riskistsenaariumid ja kikilipsu analüüs. Järgnevalt arutletakse saadud tulemuste üle.

4 ARUTELU

Peatükis analüüsitakse kirjaliku aruteluna magistritöö tulemusi.

Tulemustest selgub, et kõige kõrgema praeguse riskimääraga (30%) VOSK risk on ebaturvaline failijagamine. Avalike failijagamiskeskkondade (DropBox, OneDrive, Google Drive jt) populaarsust töötajate hulgas on lihtne mõista, sest need on mugavad, kiired, lihtsasti kasutatavad ja hõlpsasti ligipääsetavad eri seadmetest. Ometi on selliste keskkondade kasutamine ilmselgeks turvariskiks, sest andmed võivad väga kergesti lekkida ja pole välistatud nendega manipuleerimine või andmete hävimine. Sobiva meetmena riski leevendamiseks nähakse ettevõtte sisese pilve loomist – hinnanguliselt ollakse selle tegevusega 50% staatuses valmis. Kui ettevõtte sisene turvaline pilv on loodud ja ka aktiivselt kasutuses, siis on antud risk suure tõenäosusega piisavalt leevendatud.

Praeguse riskimäära järgi teisel kohal (21%) on konfidentsiaalsete andmete leke, mille mõjuks võib olla ärisaladuse leke, kliendiandmete leke, konkurentsieelise kaotus, maine langemine, seaduse rikkumine, finantskaotus. Nagu ka antud töö teoreetilises osas kirjutati, siis võimalusi andmete lekkeks on VOSK nähtuse puhul rohkelt. Riski leevendamiseks on jõustamisel meede (meetme staatus hetkel 70%), mille tulemusena toimub mobiilseadme infovahetus ettevõtte infosüsteemidega ainult läbi VPN kanali, seejuures iga VPN sessiooni käivitamisel toimub kaheastmeline autentimine ja eksisteerib seadme kaugelt tühjendamise (*remote wipe*) võimalus. Tehniliselt on VPN ja MDM kaughalduse tugi olemas, kuid hetkel kasutavad seda siiski ainult osad töötajad, mitte kõik. Tulenevalt on aktuaalseks väljakutseks ka ülejäänud töötajate, kes VOSKi hüve kasutada soovivad, kaasamine nimetatud lahenduste kasutamisesse.

Kolmandal kohal (praegune riskimäär 18%) on andmete saaste risk, mille realiseerudes võivad ebaolulised, konfidentsiaalsed või kahjulikud (nt ründetarkvaraga nakatunud) andmed sattuda tagavarakoopiatele või failiserveritesse ning sealt edasi levida; samuti võivad konfidentsiaalsed andmed töötajate kaudu koos isiklike andmetega lekkida. Andmete „saaste“ on VOSK nähtuse puhul kerge tekkima tulenevalt seadmete paljususest ja era- ning tööandmete pidevast segunemisest. Riski leevendava meetmena kasutatakse AS Eesti Telekomis reeglit, et konfidentsiaalseid andmeid ei hoita seadmes, vaid ettevõtte infosüsteemides. Meetme

rakendamise staatus on hetkel 40%, millest võib järeldada, et tõenäoliselt eksisteerib hetkel siiski päris palju konfidentsiaalseid andmeid ka töötajate kasutatavates seadmetes.

Neljandal kohal (praegune riskimäär 11%) on ründetarkvaraga nakatumise risk, mille realiseerumise tulemusel võivad lekkida konfidentsiaalsed andmed, tekkida ligipääs ettevõtte süsteemidele, toimuda andmetega manipuleerimine ja tööprotsesside häirimine. Leevendava meetmena on astutud AS Eesti Telekomis esimesi samme (rakendamise staatus 20%), pakkudes Android seadmetele välja viirusetõrje tarkvara. Töö teoreetilises osas selgus, et mobiilsetele seadmetele mõeldud ründetarkvara osas on täheldatav kasvutrend, mistõttu ei tasu antud riski alahinnata ning see võib tulevikus üha aktuaalsemaks ja ohtlikumaks muutuda. Tulenevalt tasub mõelda täiendavate turvameetmete rakendamisele.

Praeguse riskimäära (9%) järgi viiendal kohal on inimtegurist tulenev risk. Riski realiseerumise korral võivad lekkida konfidentsiaalsed andmed, toimuda ründetarkvaraga nakatumine/nakatamine, andmete manipuleerimine, tekkida ligipääs ettevõtte süsteemidele jm. Inimtegurist tulenevad riskid võivad olla põhjustatud töötajate pahatahtlikkusest, hoolimatusest või teadmatusest. Riski leevendamiseks on AS Eesti Telekomis asutud inimeste teadlikkust tõstma juhendite ja koolituste näol – meetme rakendamise hinnanguline staatus on 50%, millest järeldub, et sellega tegeletakse, aga tõenäoliselt leidub veel palju töötajaid, kes on antud teemal puudulikult informeeritud.

Kuuendal kohal (praegune riskimäär 4%) paiknev risk on puudlik turvapoliitikate jõustamine, mille tüüpiline mõju on seadmete ebapiisav turvalisus, puudulik kontroll ja haldusvõimekus. Risk on VOSK kontekstis aktuaalne, sest reeglina on ettevõtte turvapoliitikaid just töötajate isiklikes seadmetes keeruline jõustada ning olukorda ei tee lihtsamaks ka kasutusel oleva riist- ja tarkvara lai variatiivsus. AS Eesti Telekomis on aga õnnestunud antud riski oluliselt leevendada (esialgne riskimäär 32% ja praegune 4%!) võimeka MDM lahenduse kasutamise abil.

Ülejäänud teoorias esile kerkinud VOSK tüüpriskide (õngitsemine, urkimine, MDM süsteemi tungimine, seadme vargus/kaotus, tüssamine) riskimäärad on AS Eesti Telekomis hinnanguliselt väga madalad. Nende esialgne riskimäär on vahemikus 1-3% ja praegune riskimäär vahemikus 0-2%. Kuigi antud riskide mõju äritegevusele võib olla keskmine (10-50%), siis peetakse äärmiselt vähetõenäoliseks nende esinemist (esinemise tõenäosus vaid 2-

5%). Siit järeldub, et vastavaid intsidente on seni ettevõttes kas väga vähe või siis üldse mitte esinenud, mistõttu neis tänasel päeval reaalset ohtu ei tajuta. Sellegipoolest on ka nende riskide jaoks kehtestatud leevendavad meetmed; ainsaks erandiks on manipuleerimine (*tampering*), mille jaoks eraldi kehtestatud meede puudub.

Koondpilti vaadates ei ole VOSK infoturbe riskid antud ettevõttes ülikriitilised, sest leevendamata kujul on riskimääraks 1-53%, mis 12 kaardistatud riski keskmiseks esialgseks riskimääraks annab 14%. Kuna on otsustatud VOSKi töötajatele võimaldada, siis on riskide leevendamiseks sobilikud meetmed valitud ning läbi nende viidud riskimäär 0-30%-ni, mis annab 12 riski keskmiseks praeguseks riskimääraks 8%. Kui kõik meetmed on 100% rakendatud, siis on riskimääraks 0-16%, mis annab 12 riski keskmiseks meetmejärgseks riskimääraks 4%. Kikilips-analüüsist tuli hästi välja, et kõikide oluliste riskide ning võimalike tagajärgede jaoks eksisteerivad nii ennetavad kui ka parandavad meetmed. Seejuures on parandavate meetmete rakendamise staatus väga hea, aga ennetavate meetmete rakendamisega tuleb veel üksjagu tööd teha. Tasub mõelda, kas viirusetõrje kasutamine Android seadmetele on piisav ennetav meede ründetarkvarast tulenevaks riskiks või tasuks siin mõelda veel täiendavaid meetmeid (nt virtualiseerimisest tulenevad lahendused, viirusetõrje võimaldamine ka teistele levinud OSidele vm). Tervikule mõeldes on riskide võimalik mõju äritegevusele viidud väheseks ning nende esinemine ebatõenäoline.

Võrreldes AS Eesti Telekomi lähenemist teoorias välja toodud soovitustega, kuidas VOSKi turvaliselt võimaldada, ei kerkinud esile olulisi ebakõlasid. VOSK nähtuse osas on uuritud ettevõttes võetud selgeks suunaks n-ö ajaga kaasas käia ja selmet tekitada töötajatele piiranguid, üritatakse luua võimalusi, kuidas uusi tehnoloogiaid, sh isiklikke seadmeid, turvaliselt ja otstarbekalt töö kontekstis kasutada. AS Eesti Telekomis puudub eraldiseisev VOSK turvapoliitika dokument, mille olulisust teoreetilises osas rõhutati. Samas on ootused ja reeglid käitumise osas töötajateni viidud erinevate juhendite, reeglite ja koolitustegevuse kaudu. Tulevikku vaadates võib mõelda, kas eraldiseisva VOSK poliitika dokumendi loomine annab ettevõttele täiendavat väärtust või mitte. MDM süsteemi kasutamine on justkui „usalda, aga kontrolli lähenemine“, mis on tõenäoliselt mõistlik kompromiss mõlema osapoole jaoks: ettevõtte jaoks on tagatud selge ülevaade töötajate poolt tööks kasutatavate isiklike seadmete üle ja seeläbi ka teatav kindlustunne ning töötaja loovutab küll osa privaatsusest, aga saab vastu võimaluse isiklikke seadmeid töö tegemiseks kasutada. Kasutamiseks valitud MDM lahendus

Citrix XenMobile koos Cisco AnyConnect VPN tarkvaraga tundub olevat toimiv, turvaline ja ülejäänud IT taristuga hästi ühilduv lahendus, mida on ka piisavalt lihtne hallata.

Magistritöö sisu pakub tõenäoliselt huvi neile, kes tahavad täpsemalt mõista, mis üldse on VOSK nähtus ning millised on nähtusega seonduvad tüüpilised kasutegurid, tehnoloogiad, infoturbe väljakutsed ja tagamise võimalused. Läbiviidud uuringu tulemusi ei saa küll üldistada, sest tegemist oli ühe äriettevõtte põhise juhtumiuuringuga, aga need võivad siiski aidata mõista teisi sarnaseid situatsioone ning olla abiks. Teiste organisatsioonide töötajad võivad magistritöös esitatud infost ning kasutatud meetoditest eeskuju võtta või inspiratsiooni saada, kuidas VOSK infoturvet praktikas korraldada ja erinevaid riske konkreetsete magistritöös välja toodud meetmete kaudu leevendada. Seejuures tasub kindlasti pidada silmas mööndust, et AS Eesti Telekomi ei saa antud momendil käsitleda etalonina, sest VOSK võimaldamise protsess on seal alles käsil ja väljakujundamise järgus, tulenevalt ka vastav infoturbe korraldus; lisaks on iga organisatsiooni olukord ja täpsed väljakutsed unikaalsed.

AS Eesti Telekomis nähakse VOSK nähtusest tulenevaid võimalikke kasutegureid nagu suurem produktiivsus, töötajate rahulolu, paindlikkus, mugavus, mobiilsus jm. Samuti teadvustatakse VOSKi võimaldamisega kaasnevaid infoturbe riske nagu ebaturvaline failijagamine, konfidentsiaalsete andmete leke, andmete saaste, ründetarkvaraga nakatumine jm. Riskide leevendamiseks on ettevõtte praktikas kasutusele võetud hulk meetmeid, mis on kooskõlas teoorias esitatud infoga, sh MDM süsteem ja VPN lahendus mobiilsete seadmete turvamiseks ning töötajate teadlikkuse tõstmisega tegelemine. Kõik püstitatud uurimisküsimused on saanud vastuse ning magistritööle seatud eesmärk on edukalt täidetud.

KOKKUVÕTE

Magistritöös uuriti infoturvet VOSK põhimõtte rakendamisel AS Eesti Telekomi näitel. Eesmärgi täitmiseks koostati kõigepealt teemakohane kirjanduse ülevaade ja loodi teoreetiline alus, mis võimaldas uuritavat VOSK nähtust ning sellega seotud infoturbe riske paremini mõista. Seejärel viidi läbi kvalitatiivne juhtumiuuring valitud ettevõttes, esitati tulemused, analüüs ja arutelu. Uurimisküsimusi oli kolm:

1) Millised on VOSK võimaldamisega kaasnevad infoturbe riskid AS Eesti Telekomis?
2) Millised on kaardistatud VOSK riskide võimalikud mõjud ja esinemise tõenäosused?
3) Millised on võimalused kaardistatud VOSK riskide leevendamiseks?

Kõik uurimisküsimused said töös vastused. Selgus, et peamised VOSK infoturbe riskid AS Eesti Telekomis (praeguse riskimäära järgi) on:

1) ebaturvaline failijagamine;
2) konfidentsiaalsete andmete leke;
3) andmete saaste;
4) ründetarkvaraga nakatumine;
5) inimtegur;
6) puudulik turvapoliitikate jõustamine.

VOSKi võimaldamiseks kasutatakse Cisco Anyconnect VPN ja Citrix XenMobile MDM lahendusi. Tänu erinevatele turvameetmetele (infovahetus läbi VPN kanali, kaheastmeline autentimine, MDM, piiratud ligipääsud, viirusetõrje, ettevõtte sisene pilv, juhendid ja korrad, koolitustegevused, seadme kaugelt tühjendamine jt) on VOSKiga seotud riskimäär 1-53% (esialgne keskmine riskimäär) viidud 0-30% (praegune keskmine riskimäär) tasemele. Kui kõik olemasolevad meetmed oleks 100% rakendatud (praegune keskmine meetmete rakendamise staatus on 65%), siis oleks keskmine riskimäär taandatud 0-16% tasemele.

Kokkuvõtvalt saab öelda, et VOSK infoturbe riskide võimalik mõju äritegevusele on AS Eesti Telekomis viidud väheseks ning nende esinemine ebatõenäoline, mistõttu võib ettevõtte praktikat käsitleda positiivse eeskujuna ning magistritöö tulemustest võib olla kasu ka teistele organisatsioonidele. Täiendavalt tasub tulevikus uurida inimtegurist tulenevaid riske töötajate hulgas, sest Emori poolt läbiviidud Nutiseadmete kasutajate turvateadlikkuse ja turvalise

käitumise uuring Eesti elanike seas (EMOR, 2014) annab põhjust muretsemiseks. Lisaks saab seeläbi täiendavat sisendit vastavate juhendite ja koolituste läbiviimiseks, millega AS Eesti Telekomis juba tegeletakse. On alust arvata, et lähitulevikus muutub üha aktuaalsemaks temaatikaks spetsiaalselt nutiseadmetele suunatud ründetarkvara ja pahatahtlikud rünnakud, mistõttu tasub ka sellega tegeleda. Samuti soovitan uurida erinevate virtualiseerimisel põhinevate tehnoloogiate võimalikku kasutamist VOSK võimaldamise ja infoturbe kontekstis. Tehnoloogiliste arengutrendide tõttu tundub aktuaalne ja VOSK nähtusega haakuv oluline uurimisvaldkond ka ettevõtte mobiilsuse haldus ehk EMM (*Enterprise Mobility Management*) ning nn virtuaalsete ettevõtete kujunemine üldisemalt, seda nii infoturbe kui ka IT-juhtimise kontekstis.

SUMMARY

"Information Security by Applying BYOD Principles on the Example of AS Eesti Telekom"

Nowadays, many organizations are facing the security challenges of the growing global phenomenon known as BYOD (Bring Your Own Device). BYOD refers to the trend in which employers allow employees to use their personal electronic devices (such as laptops, smartphones, tablets etc.) to engage in work tasks. Allowing and encouraging BYOD has the potential to bring about many benefits (increased productivity, employee satisfaction, mobility, cost-efficiency etc.). Among the possible downsides is the added security risk associated with allowing employees to use their personal devices and easily access company data outside the workplace. Common risks associated with BYOD (such as malware, insecure file-sharing, loss of device, human factors, data disclosure etc.) all need sufficient security measures. Recommended essential security measures are BYOD policy, MDM (Mobile Device Management) system and employee training.

This paper analyzes BYOD information security on the example of AS Eesti Telekom, a well-known telecommunication company in Estonia. Firstly, a literature review is introduced. Secondly, a theoretical framework is created. Thirdly, an empirical study is conducted and fourthly, the results are presented, analyzed and discussed. There are three research questions:

1) Which BYOD information security risks does AS Eesti Telekom face?
2) What are the possible impacts and probabilities of these risks?
3) How can these risks be mitigated?

The results of the study answer these research questions and show that the main BYOD risks for AS Eesti Telekom (according to the current risk rating) are the following:

1) Unsecure file-sharing
2) Data disclosure
3) Data contamination
4) Malware
5) Human factors
6) Insufficient enforcement of BYOD security policies

In terms of BYOD related technology, Cisco Anyconnect VPN and Citrix XenMobile MDM solutions are being used. As a result of using appropriate security measures (such as VPN, 2-factor authentication, MDM, limited access, antivirus, private cloud, guides and procedures, employee training, remote wipe etc.) the overall BYOD raw risk rating of 1-53% has been mitigated to current risk rating of 0-30%. However, currently not all of the security measures are currently 100% active (average status is 65%). If the status of these security measures was to be taken up to 100%, the current risk rating would decrease to 0-16%.

In conclusion it can be said that BYOD information security risks are acknowledged and mitigated well and because of that AS Eesti Telekom can be regarded as a positive example for others. The main suggestion for the company is to continue implementing current security measures further and also to come up with additional preventive measures for malware related risks, which are believed to be of more concern in the near future regarding mobile devices. Further research perspective would be going deeper into the malware related security risks and measures, human factors, possible use of BYOD technologies based on virtualization and looking beyond “devices” to explore EMM (Enterprise Mobility Management) and possible perspectives of becoming a virtual enterprise.

Keywords: BYOD (Bring Your Own Device); MDM (Mobile Device Management); Information Security; Risk Assessment; Risk Management; AS Eesti Telekom.

KASUTATUD KIRJANDUS

Ansaldi, H. (2013). Addressing the Challenges of the “Bring Your Own Device” Opportunity. *CPA Journal*, 63–65.

Aqlan, F., & Mustafa Ali, E. (2014). Integrating lean principles and fuzzy bow-tie analysis for risk assessment in chemical industry. *Journal of Loss Prevention in the Process Industries*, *29(0)*, 39–48.

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Formal modeling and automatic enforcement of Bring Your Own Device policies. *International Journal of Information Security*.

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the “bring your own device” paradigm. *Computer VO - 47*, (6), 48.

Beckett, P. (2014). BYOD – popular and problematic. *Network Security*, *2014*, 7–9.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2008). From desktop to mobile: Examining the security experience. *Computers & Security*, *28*, 130–137.

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD (Bring Your Own Device). *Competition Forum*, *10*(2), 117.

Chang, J. M., Ho, P. C., & Chang, T. C. (2014). Securing BYOD. *IT Professional*, *16*(5), 9–11.

Cisco. (2015). Cisco AnyConnect Secure Mobility Client for Mobile Platforms datasheet, 1–4.

Citrix. (2015a). Citrix Product Documentation. Kasutamise aeg: 10. märts 2015. Allikas: http://support.citrix.com/proddocs/topic/xenmobile/xenmobile-overview-10.html

Citrix. (2015b). Citrix XenMobile Data Sheet, 1–3. Kasutamise aeg: 10. märts 2015. Allikas: http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-xenmobile-the-revolutionary-way-to-mobilize-your-business.pdf

Citrix. (2015c). Citrix XenMobile Product Overview. Kasutamise aeg: 10. märts 2015. Allikas: http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/xenmobile-product-overview.pdf

Coates, S. (2014). BYOD Business Issues. *Internal Auditor*, *71*(1), 21–23.

Cockshott, J. E. (2005). Probability Bow-Ties: A Transparent Risk Management Tool. *Process Safety and Environmental Protection*, *83*(4), 307–316.

Crossler, R. E., Trinkle, B. S., Long, J. H., & Loraas, T. M. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209–226.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security, 48,* 281–297.

Ding, J.-H., Lin, Y.-L., Kuo, C.-Y., Chung, Y.-C., Chien, R., Hung, S.-H., & Hsu, C.-H. (2014). A framework of cloud-based virtual phones for secure intelligent information management. *International Journal of Information Management, 34*(3), 329–335.

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *Procedia Technology, 9,* 43–53.

EMOR. (2014). Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuringuaruanne 2014. *Tellija: Riigi Infosüsteemi Amet, täitja: TNS Emor; 05.12.2014.* AS Emor. Kasutamise aeg: 4. märts 2015. Allikas: http://www.vaatamaailma.ee/nutikaitse/veeb-nutiseadmete-kasutajate-turvateadlikkuse-ja-turvalise-kaitumise-uuring_aruanne-2014

ENISA Threat Landscape 2014. (2014). Overview of current and emerging cyber-threats. Kasutamise aeg: 31. märts 2015. Allikas: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

Free, J. (2014). Real-world BYOD security. BYOD security strategies from two distinct healthcare organizations. *Health Management Technology, 35*(3), 14–17.

Gartner. (2013). Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. Kasutamise aeg: 23. veebruar 2015. Allikas: http://www.gartner.com/newsroom/id/2466615

Ghauri, P., & Grønhaug, K. (2004). *Äriuuringute meetodid: praktilisi näpunäiteid.* Tallinn: Külim.

Gupta, M. V., Sangroha, D., & Dhiman, L. (2013). An Approach to Implement Bring Your Own Device (BYOD) Securely. *International Journal of Engineering Innovations and Research VO - 2,* (2), 154.

ISACA. (2009). The Risk IT Framework. Kasutamise aeg: 14. märts 2015. Allikas: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf

ISACA. (2015). State of Cybersecurity: Implications for 2015 Perspectives on Cybersecurity. Kasutamise aeg: 17. aprill 2015. Allikas: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

ISKE rakendusjuhend versioon 7.00. (2014). Riigi Infosüsteemi Amet; BSI. Kasutamise aeg: 10. jaanuar 2015. Allikas: https://www.ria.ee/public/ISKE/ISKE_kataloogid/ISKE_rakendusjuhend_7.00.pdf

ISO27k Toolkit. (2015). www.iso27001security.com. Kasutamise aeg: 21. veebruar 2015. Allikas: http://www.iso27001security.com/html/iso27k_toolkit.html

Jacinto, C., & Silva, C. (2010). A semi-quantitative assessment of occupational risks using bow-tie representation. *Safety Science*, *48*(8), 973–979.

Keyes, J. (2013). *Bring Your Own Devices (BYOD) Survival Guide.* Boca Raton: CRC Press.

Koger, A. (2015). Intervjuud perioodil 2014-2015, Aivo Koger, AS Eesti Telekom.

Leung, A. (2008). A mobile device management framework for secure service delivery. *Information Security Technical Report*, *13*(3), 118–126.

Levandi, K. (2014). Jälgimine töökohal: kust algab ebaseaduslik jälitustegevus? Kasutamise aeg: 21. veebruar 2015. Allikas: http://www.aripaev.ee/uudised/2014/05/22/jalgimine-tookohal-kust-algab-ebaseaduslik-jalitustegevus

Longo, B. (2013). Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime. *Legal Information Management*, *13*(2), 119.

Miller, K. W., Hurlburt, G. F., & Voas, J. (2012). BYOD: Security and privacy considerations. *IT Professional*, *14*(5), 53–55.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security VO - 2012*, (12), 5.

Moyer, J. E. (2013). Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. *Journal of Hospital Librarianship*, *13*(3), 197–208.

Ng, V. (2013, September). BYOD, open source and security - business as usual? *NetworkWorld Asia*.

Rhee, K., Won, D., Jang, S. W., Chae, S., & Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. *ELECTRONIC COMMERCE RESEARCH*.

RIA. (2014). *RIA küberturvalisuse teenistuse 2014. aasta kokkuvõte*. Kasutamise aeg: 31. märts 2015. Allikas: https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014.pdf

Ríos-Aguilar, S. (1), & Lloréns-Montes, F.-J. (2). (2015). A mobile business information system for the control of local and remote workforce through reactive and behavior-based monitoring. *Expert Systems with Applications*, *42*(7), 3462–3469.

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security VO - 2014*, (1), 13.

Semer, L. (2013). AUDITING THE BYOD PROGRAM. *Internal Auditor*, *70*(1), 23–27.

Smith, K. J., & Forman, S. (2014). Bring Your Own Device - Challenges and Solutions for the Mobile Workplace. *Employment Relations Today (Wiley)*, *40*(4), 67.

Stevenson, K. (2013). 2012-2013 *Intel IT Performance Report*. Kasutamise aeg: 15. veebruar 2015 Allikas: http://www.intel.com/content/dam/www/public/us/en/documents/reports/2012-2013-intel-it-performance-report.pdf

Symantec Corporation. (2014). Internet Security Threat Report. *2013 Trends, 19 (April), 97*. Kasutamise aeg: 23. veebruar 2015. Allikas: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

The State of IT Security in Germany. (2014). Kasutamise aeg: 31. märts 2015. Allikas: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf

Thomson, G. (2012). BYOD: enabling the chaos. *Network Security VO - 2012*, (2), 5.

TÖÖTAJATE ARVUTIKASUTUSE PRIVAATSUS. (2013). Andmekaitse Inspektsioon. Kasutamise aeg: 16. detsember 2014. Allikas: https://wwwaki.rik.ee/sites/www.aki.ee/files/elfinder/article_files/Töötajate arvutikasutuse privaatsus_.pdf

Vallaste, H. (2015). Vallaste e-teatmik. Kasutamise aeg: 20. aprill 2015. Allikas: http://www.vallaste.ee/

Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the Employee and the Enterprise Intersect. *Employee Relations Law Journal*, *40*(2), 26–36.

Webster, J., & Watson, R. T. (2002, June). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, pp. xiii–xxiii. MIS Quarterly.

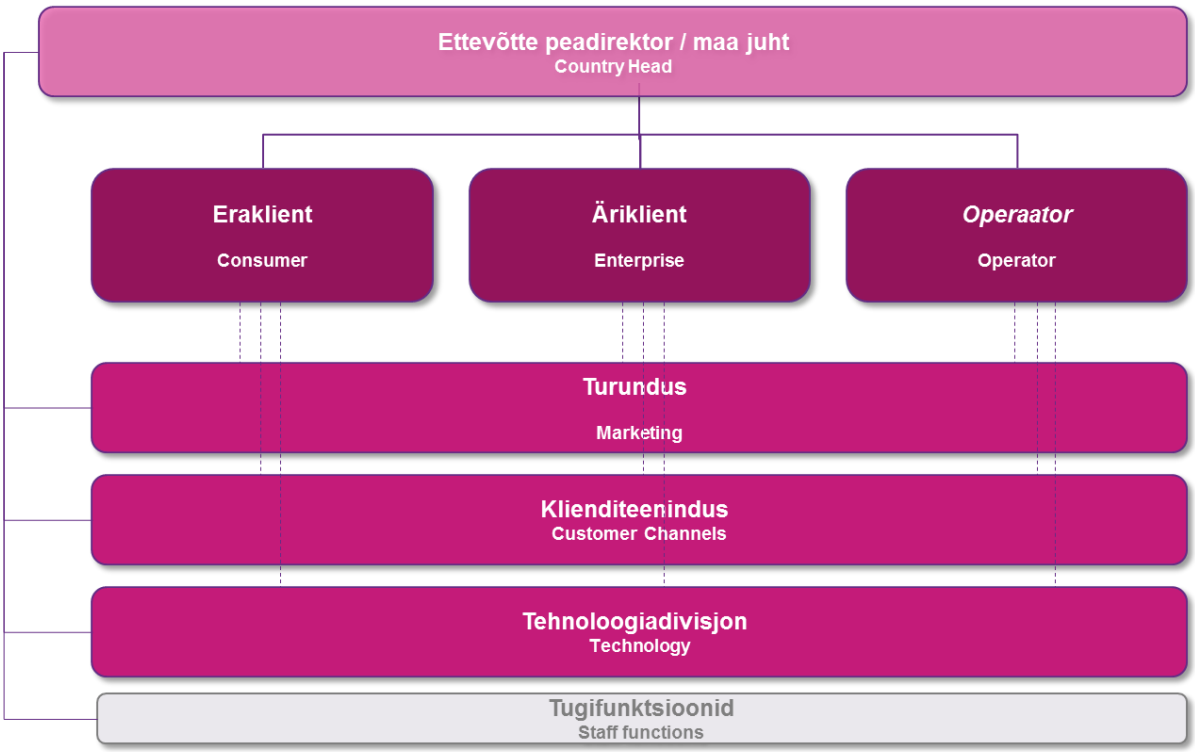
Veldre, A., Hanson, V., Laur, M., Buldas, A., & Krasnosjolov, J. (2015). AKIT - Andmekaitse ja infoturbe seletussõnastik. Cybernetica AS. Kasutamise aeg: 25. aprill 2015. Allikas: http://akit.cyber.ee/

Wong, K. (2008). The rise of Mobile Device Management. *NetworkWorld Asia*, *4*(6), 33.

www.telekom.ee. (2015). AS Eesti Telekomi veebileht. Kasutamise aeg: 21. veebruar 2015. Allikas: https://www.telekom.ee/

Yun, H., Kettinger, W. J., & Lee, C. C. (2012). A New Open Door: The Smartphone's Impact on Work-to-Life Conflict, Stress, and Resistance. *INTERNATIONAL JOURNAL OF ELECTRONIC COMMERCE*.

LISA 1: AS EESTI TELEKOMI STRUKTUUR



Joonis 13. AS Eesti Telekomi struktuur (allikas: Valdo Kalm – ettekanne uue töötaja koolitusel 2014. a lõpus).

LISA 2: CISCO ANYCONNECT MOBIILSETELE SEADMETELE FUNKTSIONAALSUSE KIRJELDUS

Funktsioon	**Kasutegur**
Ligipääs ja ühilduvus	Saadaval rakenduste poodides: ● Apple App Store: Apple iOS 6.0+ seadmed ● Google Play: Android 4.0+ seadmed ● Amazon Appstore: valitud Kindle ja Fire Phone seadmed
Optimeeritud ligipääs võrgus	● Automaatne efektiivseima võimaliku meetodi tuvastamine lähtuvalt võrgu piirangutest ● Kasutab TCP-põhiste rakenduste ja latentsustundliku liikluse (nt VoIP liiklus) jaoks DTLSi ● Kasutab TLSi (*HTTP over TLS/SSL*) ● IPsec/IKEv2 ● Ühildub Cisco ASA VPN koormuse tasakaalustamisega
Mobiilsus	● Taastub nähtamatult pärast IP aadressi muutust, ühenduse katkemist või seadme ooteolekut ● *Trusted Network Detection* (TND) peatab VPN sessiooni, kui ühendutakse usaldusväärsesse sisevõrku
Aku	● Apple iOS seadmete *stand-by* ühilduvus
Krüpteerimine	● AES-256 ja 3DES-168 tugi ● Järgmise-generatsioon krüpteerimine, sh: NSA Suite B algoritmid, ESPv3 koos IKEv2, 4096-bit RSA võtmed, Diffie-Hellman group 24, SHA2 (SHA-256 ja SHA-384)
Autentimine	● RADIUS ● RADIUS koos parooli aegumisega (MSCHAPv2) NT LAN *Manager* (NTLM) ● RADIUS *onetime password* (OTP) tugi ● RSA *SecurID* ● *Active Directory/Kerberos* ● Digitaalne sertifikaat ● *Generic Lightweight Directory Access Protocol* (LDAP) tugi ● LDAP parooli aegumine ja vananemine ● Multifaktor autentimine *(Combined certificate and username/password multifactor authentication)*
Kasutajakogemus	● *Full-tunnel client mode supports remote-access users requiring a consistent LAN-like user experience*
Tsentraliseeritud turvapoliitikate haldus	● Turvapoliitikaid saab eelseadistada ja automaatselt värskendada ● *Universal Resource Indicator (URI) handler* Cisco AnyConnecti jaoks lihtsustab paigaldamist

	● Sertifikaate saab vaadata ja hallata lokaalselt
IP võrguühenduvus	● *Administrator-controlled split- or all-tunneling network access policy* ● *Per-app VPN policy for Google Android (Lollipop) and Samsung KNOX (New in Cisco AnyConnect 4.0: Requires Cisco ASA 5500-X with OS 9.3+ and AnyConnect 4.0 licenses)* ● *Access control policy* IP aadressi määramine: ● *Static* ● *Internal pool* ● *Dynamic Host Configuration Protocol (DHCP)* ● *RADIUS/LDAP*
Keeled	Lisaks inglise keelele: ● *Canadian French (fr-ca)* ● *Czech (cs-cz)* ● *German (de-de)* ● *Japanese (ja-jp)* ● *Korean (ko-kr)* ● *Latin American Spanish (es-co)* ● *Polish (pl-pl)* ● *Simplified Chinese (zh-cn)*
Diagnostika	● Seadmepõhine statistika ja logid ● Logide edastamine administraatorile

Allikas: (Cisco, 2015).

LISA 3: CITRIX XENMOBILE FUNKTSIONAALSUSE KIRJELDUS

Funktsioon	**XenMobile MDM**	**XenMobile Advanced**	**XenMobile Enterprise**
Mobiilsete seadmete haldus (MDM)			
Seadmete haldus	x	x	x
Active Directory integratsioon reaalajas	x	x	x
Turvapoliitikate seadistamine	x	x	x
Turvalisus ja vastavus	x	x	x
Skaleeritavus	x	x	x
Lihtne haldamine	x	x	x
Kasutajate haldus	x	x	x
Integratsioon ettevõtte teiste süsteemidega	x	x	x
Monitoorimine ja kasutajatugi	x	x	x
Seadme keelamine	x	x	x
Jagatud seadmete tugi	x	x	x
Iseteeninduse veebiportaal	x	x	x
Mobiilsete rakenduste haldus (MAM)			
Rakenduste haldus		x	x
Rakenduste turvamine		x	x
Rakenduste interaktsioonide kontroll		x	x
Rakenduste turvapoliitikad		x	x
Worx App SDK		x	x
Aedikus e-maili, veebilehitseja ja failivahetuse rakendused			
Citrix WorxMail		x	x
Konverentsteenuste integratsioon (GoToMeeting, Webex, Lync jt)		x	x
Manusta ja saada e-kirjaga pilte WorxMaili kaudu		x	x

Edasijõudnud e-maili võimekus (HTML e-kirjad jmt)		x	x
Infoõiguste haldus (nt lõikamise funktsiooni keelamine jmt)		x	x
Citrix WorxWeb (turvaline mobiililehitseja)		x	x
Citrix WorxNotes (märkmete tegemise rakendus)			x
Citrix WorxEdit (dokumendiredaktor)	x	x	x
Citrix WorxDesktop (kaugligipääs töölauale)			x
ShareFile Enterprise			x
E-kirja manuse krüpteerimine			x
Ettevõtte rakenduste pood			
Ettevõtte rakenduste pood	x	x	x
Mobiilirakendused	x	x	x
Veebi/SaaS rakendused		x	x
Windows-rakendused		x	x
Multi-faktor autentimine			
Turvaline autentimine		x	x
Ühekordne sisselogimine		x	x
PIN-põhine autentimine		x	x
Kerberos autentimise protokolli tugi		x	x

Allikas: (Citrix, 2015b).