SALASTATUD TEABE KAITSJA PEAB OSKAMA RISKE HINNATA

Eestis on salastatud teabe kaitsemeetmed kehtestatud pigem ühetaoliselt ja vähese paindlikkusega.

Samas aeguvad riskihinnangud kiiresti ning riskijuhtimine peab olema pidev protsess.

Seetõttu tuleks ohtudele reageerimiseks ja rahvusvahelise koostöö toetamiseks määrata kaitsemeetmeid riskipõhiselt teabe loomise ja töötlemise tasandil.

Riigid kaitsevad oma tundlikku teavet salastatud teabena, sest selle jõudmisel võimaliku vastase või avalikkuse kätte võib tekkida oht riigi julgeolekule, välissuhtlusele või muule huvile.

Suurim oht salastatud teabele on vaenulikud riigid, kes on huvitatud nii Eesti kui ka liitlaste tundlikust teabest, et tugevdada ja kaitsta oma sõjalist võimekust, geopoliitilist mõju ja strateegilist positsiooni. Autoritaarsed riigid kasutavad teiste riikide tundlikku teavet ühtlasi poliitiliseks mõjutamiseks nii oma koduriigis kui ka rahvusvahelisel tasandil. Lisaks on üha levinum tööstusspionaaž ehk tundliku tehnoloogia varastamine – see on eriti kasulik rahvusvaheliste sanktsioonide all olevatele riikidele.

Eestile on selles vallas suurimaks ohuks eelkõige suuremad ja meie naabruses paiknevad vaenulikud riigid. Kuid ka kaugemad vaenulikud riigid võivad üritada saada Eesti kaudu ligipääsu meie liitlaste ja nende peamiste huviriikide tundlikule teabele. Niisamuti on ohuks terroristlikud organisatsioonid, kes võivad rünnaku planeerimise eesmärgil tunda huvi Eesti kriitilise taristu ja julgeolekumeetmete vastu.

Tundlikku teavet ei kaitsta ainult välise, vaid ka sisemise ohu eest: asutuste töötajad võivad teavet lekitada kas raha või teenete vastu, aga ka ideoloogilistel põhjustel. Vaenulike riikide luureasutused püüavad selliseid inimesi koostööle värvata ning sihtmärgiks võib olla iga isik, kel on juurdepääs väärtuslikule teabele. Seetõttu piiratakse tundlikule teabele juurdepääsu alati teadmisvajadusega ning isikud läbivad enne juurdepääsu saamist tausta- või julgeolekukontrolli.

KUIDAS SALASTATUD TEABE KAITSEL OHTUDELE REAGEERIDA?

Teave ise ei ole alati ühesuguse tundlikkusega ja seda ei ole kogu aeg võimalik või mõistlik ühetaoliselt kaitsta. Teave on ka strateegiline ressurss, mille puhul tuleb tagada usaldusväärsus, terviklus ja kättesaadavus, sest need määravad riigi võimekuse ohtudele reageerida. Niisamuti on oluline teabe rahvusvaheline vahetamine ja vastastikune usaldus – seetõttu peab teabe kaitse olema esiteks turvaline, aga samaaegselt ka piisavalt paindlik ja ajakohane.

Lääneriikides on salastatud teabe kaitsel valdavalt juurdunud selline riskipõhine teabekaitse, kus teabe kaitsevajadust hinnatakse vahetult teabe looja tasandil ja kaitsemeetmed määratakse vahetult teabe töötleja tasandil, arvestades ka teabe kasutusvajadusega.

See on sarnane erasektoriga, kus ettevõtted otsustavad ise oma tundliku teabe (isikuandmed ja ärisaladus, sh tundlikud tehnoloogiad ja muu intellektuaalomand) kaitsevajaduse ja kaitsemeetmed ohtudest avalduva riski alusel. Rohkem on riskipõhine teabekaitse juurdunud tugevamalt reguleeritud valdkondades, kus teabe lekkimine võib tuua rahalist kahju või riigipoolseid karistusi, näiteks finants, kõrgtehnoloogia, kriitiline taristu, digiteenused ja küberjulgeolek, ravimitööstus, tervishoid ja ka kaitsetööstus.

Eesti on jätnud riskipõhise otsustamise seadusandja ja valitsuse tasandile. See tähendab, et salastatud teavet loovad ja töötlevad asutused saavad salastatuse tasemete ja kaitsemeetmete määramisel kaasa rääkida vaid vähesel määral. Samas on ka meil vaja mõista uuenduslikku riskipõhise kaitse põhimõtet, seda nii koostöö jaoks oma liitlastega ja kaitsetööstusega kui ka Eesti salastatud teabe kaitse põhimõtete väljatöötamisel tulevikus.

KUIDAS OTSUSTATAKSE RISKIPÕHISELT TEABE SALASTATUSE TASE?

Salastatud teabe tasemed on läänemaailmas enamasti defineeritud võimaliku kahju ulatuse järgi, kui teave saab teatavaks juurdepääsuõiguseta isikule. Tavaline salastatud teabe tasemete määratlus on järgmine:

TÄIESTI SALAJANE	avalikustamine võib põhjustada **riigi huvidele väga olulist kahju**
SALAJANE	avalikustamine võib põhjustada **riigi huvidele olulist kahju**
KONFIDENTSIAALNE	avalikustamine võib põhjustada **riigi huvidele kahju**
PIIRATUD	avalikustamine võib olla **riigi huvidega vastuolus**

Üldiselt on salastamine volitatud teabe loonud asutusele, kus osatakse riskianalüüsi põhjal paremini tuvastada valdkonna teabega seotud riske. Tuvastatud riskide põhjal tehakse riskihinnang, millega teabe eest vastutav asutus määrab igale teabeliigile salastatuse taseme ja ajalise kestuse. Riigi tasandil kehtestatud salastamise juhised on valdavalt kas juhendava eesmärgiga või ei tehta selliseid juhiseid avalikult kättesaadavaks, sest ka ohu- ja riskihinnangud võivad sisaldada tundlikku teavet.

TÕENÄOSUS \ MÕJU	Väga suur	Suur	Keskmine	Väike	Väga väike
Väga suur	Kõrge	Kõrge	Kõrge	Keskmisest kõrgem	Keskmine
Suur	Kõrge	Kõrge	Keskmisest kõrgem	Keskmine	Keskmisest madalam
Keskmine	Kõrge	Keskmisest kõrgem	Keskmine	Keskmisest madalam	Madal
Väike	Keskmisest kõrgem	Keskmine	Keskmisest madalam	Madal	Madal
Väga väike	Keskmine	Keskmisest madalam	Madal	Madal	Madal

Riskianalüüsis võib ühe meetodina kasutada ka riskimaatriksit, mis aitab riske hinnata ohu avaldumise tõenäosuse ja teabe lekkimise mõju järgi. Erinevates kontekstides võib tõenäosuse ja mõju suuruse määrata kas täpse arvutuse tulemusel või muusuguse hinnangu põhjal.

Ka Eesti riigisaladuse tasemed sõltuvad teabe kaitsevajadusest ning mõne üksiku salastamisaluse puhul on lubatud teatav paindlikkus salastatuse taseme või ajalise kestuse osas. Veel on elektroonilise teabeturbe (küberjulgeoleku) puhul teatud tingimustel lubatud täiendavad erandid teabe madalamal tasemel salastamiseks.

Valdavalt on kaitstava teabe liigid, nende tase ja ajaline kestus siiski õigusaktides ette ära määratud. Nii näiteks saab riigisaladusena kaitsta ainult välissuhete, riigikaitse, korrakaitse, julgeolekuasutuste ning infrastruktuuriga seotud tundlikku teavet, mis on kitsam kui lääneriikides valdavalt. Salastamisalused on enamjaolt väga detailselt sõnastatud, mille tõttu ei pruugi sõnastus kogu tundlikku teavet ära katta ja nii ei saa seda riigisaladusena kaitsta.

Sellise lahendusega saavutatakse salastamisaluste puhul küll teatav selgus, kuid teabe loonud asutus ei saa enamasti ise oma muutuva vajaduse põhjal paindlikult otsustada, milline tema tundlik teave kaitset vajab või kas seda tuleks kaitsta kas madalamal või kõrgemal tasemel või lühema tähtajaga. Seadusandja ja valitsuse tasandil õigusaktide muutmine on ajakulukas ning vajab üleriigilist kooskõlastust – kiiresti muutuva vajaduse jaoks võib see protsess jääda liiga aeglaseks ja piiravaks.

MILLEST TULEVAD RISKIPÕHISED KAITSEMEETMED?

Salastatud teabe kaitseks vajalikud meetmed peavad arvestama vaenulike isikute huviorbiidi ja nende võimalustega teabele ligi pääseda, näiteks suure teabekoguse puhul või kui salastatud teavet töödeldakse väljaspool turvalist keskkonda. Eriti rangelt tuleb riske hinnata salastatud teabe elektroonilisel töötlemisel, sest vaenulikud riigid korraldavad Eesti tundlikule teabele ligipääsemiseks küberrünneid ning küberluuretegevus on raskesti avastatav.

Läänemaailmas on salastatud teabe kaitseks riigi tasandil enamjaolt kehtestatud miinimumnõuded ning asutus peaks riskihinnangu alusel ise otsustama, milliste kaitsemeetmetega ta konkreetsel juhul teavet kaitseb. Riskide hindamist ja nende kaitsemeetmetega maandamist nimetatakse riskijuhtimiseks ehk riskihalduseks.

Mingi risk jääb salastatud teabe kaitsel alati alles ning teabe looja peab otsustama, kas selline tuvastatud jääkrisk on tema jaoks aktsepteeritav ehk kas ta on nõus sellist riski taluma. Seejuures tuleb arvestada, et asutuse riskitaluvus võib kriisiolukorras olla hoopis teistsugune ning õiguskord peaks toetama asutuse õigust sellises olukorras teisiti otsustada. Riskihalduse viimases etapis tuleb ette valmistada täiendavad kaitsemeetmed tulevikus kasvava riski maandamiseks, näiteks tehnoloogilise arengu vaatest. Ühtlasi tuleb paika panna kahju vähendamise meetmed juhuks, kui teavet ei ole enam võimalik kaitsta.

Eestis on salastatud teabe kaitsemeetmed kehtestatud pigem ühetaoliselt ja vähese paindlikkusega. Rohkem arvestatakse madalama taseme riskipõhiste kaitsemeetmetega elektroonilise teabeturbe puhul, kus salastatud teavet sisaldava süsteemi puhul tuleb rakendada katkematut riskijuhtimist. Valdavalt siiski ei arvestata sellega, et asutused on väga erineva kasutusvajadusega või et nad peavad oma salastatud teavet kaitsma erinevate ohtude eest.

Sellega saavutatakse kaitsemeetmete puhul küll üleriigiline selgus, kuid paindlikkuse puudumine võib takistada uute tehnoloogiliste lahenduste kasutuselevõtmist, sest seda oleks kergem alguses juurutada asutuse tasandil. Uusi lahendusi on ka keeruline riigi tasandil reguleerida, kui ühelgi asutusel ei ole uue lahenduse kasutuspraktikat.

Niisamuti takistab üleriigiline vähepaindlik lahendus koostööd liitlasriikidega, kelle salastatud teabe kaitsemeetmetes juba lubatakse teatud riskipõhist paindlikkust, kuid Eesti peab teavet kaitsma ühetaoliste meetmetega. Suuremaks probleemiks on see näiteks ühisõppustel ja -operatsioonidel, ühiste süsteemide kasutuselevõtmisel ning välishangete puhul.

RISKIHALDUSE ETAPP	TEGEVUS
Ohuhinnang	Millised ohud riigile avalduvad? Kelle eest tuleb teavet kaitsta?
Riskihinnang	Millist kahju teabe avalikustamine riigile põhjustaks? Millisel salastatuse tasemel tuleks teavet kaitsta?
Kaitsemeetmed	Millised peavad olema kaitsemeetmed üldiselt? Millised peavad olema kaitsemeetmed konkreetsel kasutusjuhul?
Jääkrisk	Millised riskid jäävad pärast meetmete rakendamist alles? Kas maandamata risk on vastuvõetav?
Täiendavad meetmed	Kuidas tulevikus tekkida võivaid riske maandada? Milliseid kahju vähendamise meetmeid ette valmistada?
Protsessi kordamine	Kas ohu- või riskihinnang on muutunud või muutub tulevikus? Milliseid uusi kaitsemeetmeid kasutada?

Riskihinnang hakkab aeguma kohe pärast selle koostamist, mistõttu peab riskijuhtimine olema pidev protsess. Selle eelis on, et teabe looja ja kaitsja peavad regulaarselt uuesti läbi mõtlema, milliste ohtude eest, millisel tasemel ja milliste kaitsemeetmetega tuleb teavet kaitsta. Riskipõhisuse juurutamine teabe looja ja töötleja tasandil võib esmalt tunduda suure ja seniseid alusväärtusi muutva sammuna. Tegelikult oleks salastatud teave vajadusel paindlikumalt kasutatav, aga samas kaitstud kõige ajakohasemate meetmetega.