VEGLEIÐING UM VÁÐAMETING

November 2020

2. útgáva

Dátueftirlitið

Innihaldsyvirlit

1. Innleiðsla

Hendan vegleiðing er skrivað til tín, sum er dátuábyrgdari, og hevur brúk fyri at vita, hvørji trygdarviðurskifti eru viðkomandi, tá persónupplýsingar skulu viðgerast. Í tekstinum verður viðgjørt, hvussu ein váðameting kann gerast í roynd og veru. At enda er eisini ein leistur, sum váðametingin kann gerast eftir.

2. Trygd

Trygd hevur ein serliga týðandi leiklut í lógini um vernd av persónupplýsingum (dátuverndarlógini). Í lógini er trygd ásett sum ein grundleggjandi meginregla, tá tað snýr seg um viðgerð av persónupplýsingum. Góð trygd snýr seg um at tryggja upplýsingar í mun til atkomu, trúnað og integritet samstundis. Váðametingin er grundarlagið fyri at velja røtt og viðkomandi trygdartiltøk og at seta hesi í verk. Yvirskipað eru nógv av tiltøkunum, sum skulu setast í verk í samsvari við kapitli 4 í lógini, partur av góðari trygdaratferð (ISO2700x), so sum stýring av veitarum (dátuviðgerum), útnevning av dátuverndarfólki og eisini í mun til teir standardir sum eru innan vinnugreinina.

3. Váði

Trygd spælir ein týðandi leiklut í dátuverndarlógini, og tí er hugtakið váði, og metingin av hesum váða, eisini blivið alt meiri týðandi. Váði spælir ein leiklut í mun til tey tiltøk, ein dátuábyrgdari ítøkiliga skal seta í verk. Í dátuverndarlógini eru nógvar ásetingar, sum á ymsan hátt sipa til váðan í sambandi við viðgerð av persónupplýsingum:

- § 37: Dátuábyrgdari skal leggja upp fyri váða, tá tiltøk skulu setast í verk
- § 38: Dátuábyrgdarin skal meta um váðan við viðgerðini og síðani gera av hvørji tiltøk eru fyri neyðini, og hvussu hesi kunnu sniðgevast inn í skipanir
- § 45: Váðin er avgerandi fyri um fyritøkur, sum hava færri enn 250 starvsfólk, skulu gera *yvirlit yvir viðgerðir*
- § 46: Váðin er avgerandi fyri hvørji tiltøk verða sett í verk
- § 47: Váðin fyri rættindunum hjá einstaklingum er avgerandi fyri um eitt trygdarbrot skal fráboðast Dátueftirlitinum
- § 48: Váðin fyri rættindunum hjá einstaklingum er avgerandi fyri um eitt trygdarbrot skal fráboðast skrásetta
- § 49: Váðin fyri rættindum hjá einstaklingum er avgerandi fyri um ein avleiðingargreining um dátuvernd skal gerast
- § 50: Ein avleiðingargreining skal hava eina meting av váðunum, sum eru fyri rættindum hjá teimum skrásettu
- § 58: Dátuverndarfólkið skal røkja sínar uppgávur við fyriliti fyri tí váða, sum er knýttur at uppgávuni

Dátuverndarlógin er grundað á eina váðagrundaða tilgongd. Hetta merkir, at dátuábyrgdarin sjálvur kann velja, hvørji trygdartiltøk verða sett í verk útfrá eini meting av tí váða, sum stendst av viðgerðini. Dátuábyrgdarin er sostatt ikki bundin av at seta tiltøk í verk eftir einum givnum lista av tiltøkum, sum ikki hava týdning í mun til teir váðarnar, sum eru við viðgerðini. Ein váðagrundað tilgongd hevur sostatt við sær, at orka og møguleikar verða gagnnýttar á besta hátt. Hinvegin setur hetta eisini krøv til dátuábyrgdaran, sum skal meta um váðarnar fyri tann skrásetta, tá persónupplýsingar vera viðgjørdir.

4. Váðameting úr sjónarhorni skrásetta

At gera váðametingar fyri at kunna velja og íverkseta tey røttu trygdartiltøkini er ikki eitt nýtt fyribrygdi fyri fyritøkur í Føroyum. Tað er tó møguligt, at tær váðametingar, sum eru gjørdur, eru gjørdar í mun til búskapin ella góða umdømi hjá fyritøkuni, um hon er fyri telduálopi. Tað er altavgerandi fyri fyritøkur at gera slíkar váðametingar, men tað eru ikki slíkar váðametingar, sum skulu gerast sambært dátuverndarlógini.

Ein váðameting eftir dátuverndarlógini tekur útgangsstøði í tí skrásetta. Ein dátuábyrgdari, t.d. ein fyritøka, skal tí gera eina meting av, hvørjir váðar ein viðgerð av persónupplýsingum hevur fyri skrásetta. Hetta kann vera t.d. viðskiftafólk, starvsfólk og aðrir samstarvsfelagar.

Dátuábyrgdarin kann sostatt ikki nýta eina váðameting, sum er gjørd í mun til fyritøkuna við støði í t.d. fíggjarstøðu ella umdømi, men má gera eina váðameting, har tey skrásettu eru í miðdeplinum. Hinvegin, so ber til at endurnýta framferðarháttin, tí hann er hin sami.

5. Framferðarháttur at gera váðameting

Dátuábygdarin skal áseta eitt hóskandi trygdarstøði, og hetta skal leggjast í mun til teir váðar, ið eru viðkomandi fyri viðgerðina av persónupplýsingunum, sum skal fara fram. Tí er neyðugt við eini váðameting. Dátuverndarlógin hevur ongar ásetingar um, hvussu ein váðameting skal gerast, ella hvussu nágreinilig ein slík váðameting skal vera.

Áðrenn ein váðameting verður gjørd, er neyðugt at hava eitt yvirlit yvir tær kunningareindir sum verða brúktar. Hetta kann vera ambætarar, KT-skipanir, samskiftislinjur o.a. har persónupplýsingar verða viðgjørdar. Hvør kunningareind eigur at hava ein eigara, og hesin sami persónur kann so eisini vera eigari av váðanum.

Tá arbeitt verður við trygd, er neyðugt at hava greiðu á grundleggjandi hugtøkunum, sum eru: trúnaður, atkoma og integritetur.

Trúnaður merkir, at óviðkomandi ikki fáa atgongd til upplýsingarnar (t.d. vernd móti telduálopi).

Atkoma merkir at upplýsingarnar eru tøkar hjá teimum, sum hava brúk fyri teimum, tá tey hava brúk fyri teimum (t.d. kann ein hending sum hevur elvt at KT-skipanir eru óvirknar forða atkomu).

Integritetur merkir m.a. at upplýsingarnar eru rættar og eftirfarandi og ikki eru broyttar ella strikaðar av óviðkomandi (t.d. haldføri og neyvleikin hjá eini KT-skipan, sum sendir lønarseðlar).

Her verður greitt frá, hvussu tú við fýra stigum kanst fara fram, tá tú skalt gera eina váðameting og harvið staðfesta, meta um og fremja trygdartiltøk, sum skulu til fyri at lúka treytina um viðgerðartrygd.

4.1 Stig 1 - avleiðingameting

Fyri hvørja kunningareind (t.d. ambætarar, KT-skipanir, samskiftislinjur) verður byrjað við at fastleggja avleiðingarnar fyri skrásetta um brot verður á trúnað, atkomu og integritet. Hesar avleiðingar vera ásettar at vera høgar, miðal ella lágar.

Dátuverndarlógin ásetur ikki krav um nágreining av váðametingum, og tí kann dátuábyrgdarin t.d. bólka sínar kunningareindir ella áseta ein felagsváða fyri eindirnar í staðin fyri at uppbýta í atkomu, trúnað og integritet. Tað er dátuábyrgdarin, sum ger av, hvussu nágreinilig ein avleiðingameting skal vera.

4.2 Stig 2 – hóttanarmeting og sannlíkindi

Dátuábyrgdari skal síðani eyðmerkja tær hóttanir, sum eru í mun til kunningareindirnar, og meta um, hvørji sannlíkindini eru fyri, at hóttanin gerst veruleiki. Sannlíkindini kunnu vera høg, miðal, lág. Dømi um hóttanir kunnu vera: hacking, phishing ella ransomeware.

Tá hóttanirnar eru eyðmerktar, kann vera trupult at siga nakað um, hvørji sannlíkindini eru fyri, at ein ávís hóttan sæst aftur í einari hending. Í slíkum førum eiga søgulig dátu at hava stóra vekt – hvørjar hóttanir síggjast aftur í trygdarhendingum hjá dátuábyrgdara? Hevur dátuábyrgdari verið úti fyri hacking, phishing ella ransomeware, stolnum persónupplýsingum, eru persónupplýsingar sendar skeivum móttakara, ella hevur starvsfólk lagt persónupplýsingar í privatar Cloudtænastur. Tá hetta er kannað, ber til at leggja afturat hesum, tey rák og hagtøl sum eru uppi í tíðini, so ein enn betri meting fast av hóttanum.

Arbeiðið við at ávísa hóttanir og at meta um avleiðingarnar av hóttanunum er ikki eitt vísindaligt fak. Dátuábyrgdari skal koma við sínum besta boði og síðani standa við tað.

4.3 Stig 3 – meting av verandi tiltøkum

Á einum ávísum virki kunnu trygdartiltøk longu vera sett í verk, sum verja eitt sindur fyri teimum hóttanum, sum eru eyðmerktar í hóttanarmetingini. Tað er neyðugt at ávísa hvørji verandi trygdartiltøk eru sett í verk, og hvussu hesi eru við til at minka um sannlíkindi og avleiðingar.

4.4 Stig 4 - váðamynd

Út frá undanfarnu stigum ber nú til at lýsa vandamyndina:

(avleiðing x sannlíkindi) – verandi tiltøk = váði

Leiðslan skal síðani taka støðu til, um váðin er góðkendur, ella um eyka tiltøk skulu setast í verk, so váðin minkar enn meiri. Leiðslan skal góðkenna tann eyka váðan, sum altíð er eftir.

Samanumtikið ber til at savna hetta í myndina niðanfyri, har serliga kann leggjast til merkis, um kunningareindirnar ella persónupplýsingar eru í reyða økinum á myndini.

Avleiðing

Sannlíkindi

	Lág	Miðal	Høg
Lág			
Miðal			
Høg			

6. Spurningar í mun til váðameting

Tá ein váðameting skal gerast, eigur støða at takast til ymiskar spurningar. Hesir kunnu vera:

- Hvørjar hóttanir kunnu ávirka trúnað, atkomu ella integritet?
- Hvør eigur váðan?
- Hví er hetta ein váði?
- Hvør er avleiðingin (á stiga frá 1 - 5) um váðin gerst veruleiki?
- Hví er avleiðingin júst hendan?
- Hvørji eru sannlíkindini (á stiga frá 1 -5) fyri at váðin gerst veruleiki?
- Hví eru sannlíkindini júst hesi?

Tá hesir spurningar eru settir og svaraðir, verða avleiðing og sannlíkindi mett samlað til ein váða, sum fellur í antin reytt, gult ella grønt slag, sum víst í myndini undir pkt. 4.4. Tá váðin er staðfestur, kann ein dátuábyrgdari velja at góðtaka váðan, hava eftirlit við honum ella koma sær undan tí eyðmerkta váðanum. Um dátuábyrgdarin ynskir at sleppa undan váðanum, kunnu nýggj bygnaðarlig ella tøknilig tiltøk setast í verk.

Tá møgulig nýggj tiltøk eru sett í verk, eigur dátuábyrgdarin av nýggjum at meta um hvør avleiðingin, sannlíkindini og (rest)váðin er, og sum dátuábyrgdarin so uppaftur skal taka støðu til.

Ein fyrimunur við einum slíkum skjalfestum framferðarhátti er, at tað ber til á skipaðan hátt at leggja fram allar grundgevingar, sum valini hjá dátuábyrgdaranum byggja á. Slík skjalfesting kann leggjast fram fyri myndugleikum og øðrum áhugaðum, sum vilja hava innlit í váðametingina hjá dátuábyrgdara.

7. Leistur til váðameting

Her verður greitt nærri frá, hvat ein váðameting er, hvussu hon kann vera gjørd og hvussu hon kann brúkast. Teksturin skal lesast saman við rokniarkinum (vadameting.xsl) og vendir sær til smærri virkir, sum brúka 3-5 KT-skipanir, ið eru neyðugar fyri virksemið. Hesar KT-skipanir kann virkið sjálvt umsita, men tað kann eisini vera talan um at uttanhýsis veitari umsitur tær.

7.1 Um váðametingar

Váðastýring er ein týðandi partur av arbeiðinum við KT-trygd og trygd av upplýsingum. Við váðastýring er gjørligt hjá leiðslum at raðfesta neyðugar íløgur og tiltøk í mun til váðan, sum ein fyritøka vil góðtaka. Hetta byggir alt á eina váðameting.

Málið við eini váðameting er at gera váðar sambærligar, og hetta kann gerast t.d. við at ein váði fær eitt talvirði.

Váðin verður máldur við at áseta, hvussu stór *sannlíkindini* eru fyri, at ein hóttan brúkar ein veikleika, og hvussu stórar *avleiðingar* hetta kann fáa fyri virkið. Eitt dømi er, at virkið missur burtur eina farteldu (hóttan), sum ikki er bronglað (veikleiki), soleiðis at tað er gjørligt fyri óviðkomandi at fáa atgongd til teldupost og líknandi á telduni.

Grundað á váðametingarnar skal virkið meta um tørvin og velja møgulig eyka trygdartiltøk, sum tryggja neyðugu atgongdina, trúnaðin og integritetin. Í døminum kundi tað verði tørvurin á at brongla farteldu na. Hendan meting skal takast við í ætlanina fyri váðahandfaring.

8. Handfaring av váðum

Yvirskipað kunnu váðar handfarast á fýra hættir:

- Váðin verður góðtikin
- Váðin verður stýrdur
- Váðin verður sundurbýttur (t.d. við trygging)
- Sloppið verður undan váðanum

Ein máti at handfara váðan uppá er, at váðin verður býttur upp í trý og har hvørt býti fær ein lit (grønt, gult og reytt). Eitt tríbýti kundi verið at

- lágur váði fær ein grønan lit
- miðal váði fær ein gulan lit
- høgur váði fær ein fær reyðan lit

Tað er dátuábyrgdarin (t.d. leiðslan), sum ásetur býtið útfrá váðafýsni, og hetta váðafýsnið vísir hvørjir váðar kunnu góðtakast.

Eru nógvir váðar, sum ikki kunnu góðtakast, uttan at tiltøk verða sett í verk, er talan um sokallað lágt váðafýsni. Tá eru nógvir váðar merktir við reyðum. Her kann talan vera um serliga týdningarmiklar upplýsingarnar.

Er býtið millum váðar, sum kunnu góðtakast, og váðar, sum ikki kunnu góðtakast meira javnt, er sokallaða váðafýsni miðal. Tá er býtið millum grønt, gult og reytt meiri javnt.

Eru nógvir váðar, sum kunnu góðtakast, er sokallaða váðafýsni høgt, og tí eru nógvir váðar, merktir við grønum. Tað ber væl til at hava høgt váðafýsni, um tað ber til at arbeiða, t.d. uttan at egnu ambætarar eru virknir, ella at tað bert í lítlan mun verður arbeitt við persónupplýsingum.

Um ein stórur váði (reyður litur) ikki kann minkast, so kann verða neyðugt at sleppa undan váðanum. Hetta kann viðføra, at virkið t.d. ikki kann loysa eina uppgávu.

7.2 Váðastýring

Tilgongdin til váðastýring er hendan:

a) Dátuábyrgdarin (t.d. starvsfólkið, sum hevur ábyrgd av trygdini) skal gera av nær ein váðameting skal gerast, hvussu avleiðingarnar skulu metast, hvør váði kann góðtakast, og hvørjar váðar hond skal takast um (váðafýsni)

b) Dátuábyrgdarin (t.d. starvsfólkið, sum hevur ábyrgd av trygdini) skal meta um hvørjar upplýsingar, mannagongdir og KT-skipanir hava týdning, og tí skulu váðametast. Her ber til at hyggja at, hvørjar tilgongdir eru avgerandi fyri at kunna veita eina ávísa tænastu ella vøru, og hvørjar upplýsingar og KT-skipanir eru fortreyt fyri hesum tilgongdum.

c) Tá týðandi skipanir, dátur og tilgongdir eru ávístar, skal ein eigari av hvørjum váða sær veljast. Eigarin av váðanum skal taka støðu til, um ein ávísur váði verður góðtikin, ella váðin skal minkast.

d) Dátuábyrgdarin (t.d. starvsfólkið, sum hevur ábyrgd av trygdini) skal saman við váðaeigara og øðrum viðkomandi eyðmerkja tær hóttanir, sum kunnu brúka verandi veikleikar og viðføra eitt brot á atkomu, trúnað og integritet í mun til tilgongdir, dátu og KT-skipanir, og soleiðis vera ein váði.

e) Dátuábyrgdarin (t.d. starvsfólkið, sum hevur ábyrgd av trygdini) skal áseta avleiðingarnar av hesum váðum og metir, um hetta hevur týdning fyri virkið. Avleiðingarnar vera síðani bólkað í ymisk stig:

    1- Sera lítil avleiðing – sum í royndu veru ikki hevur týdning
    2- Lítil avleiðing – sum kann handfarast sum partur av rakstrinum
    3- Nakað av avleiðing – her skulu eyka tiltøk umhugsast
    4- Stór avleiðing – sum hevur ávirkan á ársúrslitið
    5- Sera stóra avleiðing – virkið er hótt

f) Dátuábyrgdarin (t.d. starvsfólkið, sum hevur ábyrgd av trygdini) skal meta um sannlíkindini fyri, at ávísi váðin er ein veruligur váði. Sannlíkindini verða síðani løgd í ymisk stig:

    1- Sjáldan ella ósannlíkt

2- Kemur neyvan fyri

3- Er møguligt

4- Kann henda

5- Fer at henda

Tað er týdningarmikið at ávísa og lýsa teir viðkomandi váðar og grundgeva fyri bæði avleiðingum og sannlíkindunum í teigunum: "Hví er talan um avleiðing, og hví eru sannlíkindini mett soleiðis?" í skjalinum til váðameting. Váðametingin kann leggjast fyri leiðsluna, og váðametingin kann eisini eftirmetast, um váðamyndin broytist.

7.3 Úrslitið

Tá váðin er útroknaður, og trygdartiltøk sett í verk, vil tað ofta vera so, at tað framhaldandi er ein váði eftir (ein nýggjur váði). Um ein fyritøka kann liva við nýggja váðanum, er treytað av, hvussu váðafús fyritøkan er. Antin kann nýggi váðin góðtakast, ella er neyðugt at fremja fleiri tiltøk sum viga upp ímóti.

Váðameting							
ID	Váði - Hvat kann ávirka trúnað, atgeingi ella integritet?	Eigari av váða	Hví er hetta ein hóttan/váði?	Mett avleiðing	Hví er avleiðing metta soleiðis?	Mett sannlíkindi	Hví eru sannlíkindini mett soleiðis?
1	Trúnaðarbrot - Avrit av upplýsingum um keyp hjá viðskiftafólkum er komið á skeivar hendur.	KT-leiðarin	Óviðkomandi kunnu síggja upplýsingar um viðskiftafólk, og fáa innlit í keyp av tænastum og vørum. Upplýsingar um keypssøguna hjá skrásetta kunnu brúkast til at fremja málsøkna marknðarførðslu í móti skrásetta.	3	Upplýsingarnar um keypini hjá skrásetta hava stóran áhuga hjá seljarum á internetinum.	2	Upplýsingar um kundar liggur bert í tveimum skipanum. Báðar skipanirnar hava avmarkaða atgongd og eru vardar av Ajax firewall og trygdarskipanum.
2	Brot á atkomu - heilsuskipan er óvirkin. Eitt telduvirus (ransomeware) hevur læst KT-skipanina har sjúklingar eru skrásettir.	KT-leiðarin	Um tað ikki slepst framat upplýsingum um sjúklingar, so er ikki gjørligt at gera týdningarmiklar skurðviðgerðir.	5	Fleiri viðgerðir skulu fremjast skjótast gjørligt og eru lívsneyðugar fyri sjúklingarnar.	1	Tað finst avrit av upplýsingunum um sjúklingarnar, og tí kunnu hesar upplýsingar endurskapast á øðrum servara. Hartil eru starvsfólkini roynd í at brúka KT-skipanirnar.
3	Brot á integritet - stempliskipan. Skrásetingar, ið eru grundarlag undir tímalønini hjá starvsfólki, reingjast (korrumperast).	Starvsfólkaleiðarin	Um tíðarstemplingarnar reingjast í mun til veruligu tíðirnar, so er grundarlagið undir t.d. lønarútgjaldingum skeivt. Hetta hevur við sær at starvsfólk ikki fáa røttu lønina.	3	Fyri løntakaran er umráðandi at arbeiðstíðin er rætt skrásett, soleiðis at t.d. lønin er røtt og í samsvari við galdandi sáttmála.	1	Skipanin verður kannað og eftirmett regluliga fyri rættleika. Allar stemplingar hjá einum starvsfólki verða sendar starvsfólkinum saman við vikulønini. Á henda hátt kunnu starvsfólk eftirkanna egnar stemplingar og boða frá um skeivleikar eru.

Í rokniarkinum er váðafýsni ásett við litum, grundað á bólkarnar lágt, miðal og høgt. Hesi eri ásett í teigi Q. Grønt hevur lágan váða og hevur talvirðið 1-5. Gult hevur miðal váða og hevur talvirðið 6-9 og reytt hevur hægsta váða og hevur talvirði frá 10-25.

Q	R
Váðafýsni	**Frágreiðing**
Grønt	
1	Leiðslunar meting av lagsta váða í grønum
Gult	
6	Leiðslunar meting av lagsta váða í gulum
Reytt	
10	Leiðslunar meting av hægsta váða í reyðum

7.4 Ætlan fyri váðahandfaring

Grundað á váðametingina skal metast, um trygdin er á einum støði, sum kann góðtakast, ella um neyðugt er at seta í verk fleiri trygdartiltøk, fyri at minka um sannlíkindini fyri at hóttarnirnar gerast veruleiki. Hetta er m.a. treytað av, hvat er fíggjarliga burðardygt. Til ber eisini at umhugsa at enda virksemi, sum hevur váða við sær, um tað er gjørligt. Eisini ber til at umhugsa møguleikan, at býta nýggja váðan sundur við veitara ella tryggja seg frá tí.

7.5 Viðlíkahald

Váðameting og ætlan fyri váðahandfaring eru ikki óbroytilig skjøl. Tað er umráðandi, at fyritøkur o.o. leypandi halda eyga við váðum, hóttanum o.s.fr.

Út yvir ætlanina fyri váðahandfaring og dagføringum av tilbúgvingarætlan, skal mann fylgja við í broytingunum av váðamyndini (hóttanir, veikleikar og/ella nýggj evni sum metast skal um). Er tað so, skal tilgongdin endurtakast fyri tær nýggju broytingarnar.

Hetta eigur í fyrimyndarligu støðuni at henda áhaldandi, t.d. størri broytingar í mun til KT ella tilgongdum, og tá mann gerst varugur við nýggjar hóttanir. Mann eigur at tryggja sær, at hetta hendur regluliga t.d. minst einaferð um árið, við einum títtleika, sum er grundaður á broytiliga heimin, har virkið er virkið.

Vegleiðing

Givið út:

Dátueftirlitið

Reyngøta 33

100 Tórshavn

Tlf: 309100

dat@dat.fo

dat.fo

Dátueftirlitið