Alþjóðleg viðmið um bestu framkvæmd

Meginreglur PFMI hafa verið nánar útfærðar í leiðbeiningum

Í Kjarnareglunum um innviði fjármálamarkaða (PFMI) eru m.a. gerðar kröfur um öryggi í upplýsingakerfum og um ábyrga stýringu áhættu, sjá einkum meginreglur 3 og 17.

Samkvæmt meginreglu 3 skal viðhafa stefnu, ferla og verklag sem auðvelda eiganda og rekstraraðila kerfislega mikilvægs fjármálainnviðar að bera kennsl á, mæla, fylgjast með og stýra hvers kyns mögulegri áhættu. Umgjörð áhættustýringar ber að endurskoða reglulega.[22]

„Nauðsynleg umgjörð skal vera til staðar svo að tryggja megi virka áhættustýringu í rekstri fjármálainnviða að því er varðar lagaáhættu, greiðslufallsáhættu, lausafjáráhættu og aðra áhættuþætti".

(Meginregla 3, PFMI)

Meginregla 17 gerir ítarlegri kröfur til umgjarðar áhættustýringar með sérstöku tilliti til rekstraráhættu. Áhætta tengd net- og upplýsingaöryggi fellur undir rekstraráhættu. Stjórn (e. board of directors) ber ábyrgð á umgjörð og tilhögun rekstraráhættustýringar. Skilgreina ber með skýrum hætti markmið um rekstraröryggi og fyrir hendi skal vera yfirgripsmikil stefna um efnislegt öryggi og upplýsingaöryggi. Viðbúnaðaráætlun skal sniðin þannig að hún tryggi að mikilvæg upplýsingakerfi geti haldið áfram starfsemi innan tveggja klukkustunda frá skaðlegum atburðum og að kleift verði að ljúka uppgjöri samdægurs, jafnvel þegar um ræðir mjög óvenjulegar og alvarlegar aðstæður. Athygli skal veita áhættu sem steðja kann að kerfislega mikilvægum fjármálainnviðum vegna tengsla við aðra innviði, þjónustu- og veitufyrirtæki.[23]

„Fjármálainnviðir skulu skilgreina mögulegar orsakir rekstraráhættu, jafnt innri sem ytri, og leitast við að draga úr áhrifum slíkrar áhættu með því að beita viðeigandi kerfi, stefnu, verklagsreglum og eftirliti. Kerfi skulu sniðin þannig að þau tryggi sem best öryggi og rekstraráreiðanleika. Afkastageta þeirra skal vera fullnægjandi og aukning möguleg samfara auknum umsvifum. Stjórnun rekstrarsamfellu skal miðast við að starfsemi fjármálainnviða verði endurreist og að staðið verði við skuldbindingar þeirra á réttum tíma, þar á meðal ef til víðtækrar eða stórfelldrar röskunar kemur".

(Meginregla 17, PFMI)

Áður tilvitnaðar leiðbeiningar CPMI og IOSCO, *Guidance on cyber resilience for financial market infrastructures* (2016), geyma nánari leiðsögn um eflingu viðnámsþróttar fjármálainnviða gegn netárásum. Fram kemur að leiðbeiningunum sé ekki ætlað að leggja ríkari skyldur á herðar kerfisstjórum kerfislega mikilvægra fjármálainnviða í þessum efnum umfram það sem þegar er kveðið á um í meginreglum PFMI. Fremur beri að líta á þær sem viðbótarleiðsögn um æskilegar ráðstafanir í þeim tilgangi að efla viðnámsþrótt gegn netárásum enn frekar og takmarka þannig möguleg neikvæð áhrif á fjármálastöðugleika.[24] Við beitingu leiðbeininganna er óhjákvæmilegt að styðjast við áhættumiðaða nálgun og skal í því sambandi minnt á að netárásir geta verið ófyrirsjáanlegar og því eðli máls samkvæmt erfitt að verjast þeim.[25]

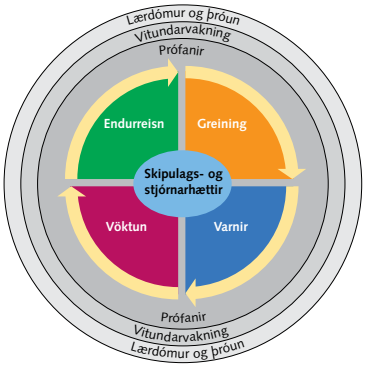
Meginatriði leiðbeininganna – Að hverju þarf að huga?

Samkvæmt leiðbeiningum CPMI og IOSCO skipta fimm þættir höfuðmáli við stýringu áhættu með tilliti til net- og upplýsingaöryggis, þ.e. *skipulags- og stjórnarhættir* (e. governance), *greining* (e. identification), *varnir* (e. protection), *vöktun* (e. detection) og *endurreisn* (e.

22. Kjarnareglur um innviði fjármálamarkaða (PFMI), CPMI og IOSCO, 2012, bls. 32 (leiðbeinandi eining 1 við meginreglu 3). Kjarnareglurnar eru aðgengilegar á vefsíðu Alþjóðagreiðslubankans (BIS), www.bis.org.
23. Sama heimild, bls. 94 (leiðbeinandi einingar 1-7 við meginreglu 17).
24. Sjá t.d. bls. 1, 4 og 8 í leiðbeiningunum.
25. Sama heimild, bls. 3. Áhættumiðuð nálgun (e. risk based approach) er skilgreind þannig í leiðbeiningunum (viðauki A, hugtakalisti): „An approach whereby FMIs identify, assess and understand the risks to which they are exposed to and take measures commensurate with these risks."

resumption). Jafnframt eru tilgreindir þrír aðrir þættir er máli skipta, þ.e. *prófanir* (e. testing), *vitundarvakning* (e. situational awareness), ásamt *lærdómi og þróun* (e. learning and evolving). Hér verður stuttlega gerð grein fyrir sérhverjum þessara þátta, sjá einnig mynd VI-1.

Mynd VI-1
Lykilþættir áhættustýringar m.t.t. net- og upplýsingaöryggis



Heimild: Leiðbeiningar CPMI/IOSCO 2016, bls. 7.

Skipulags- og stjórnarhættir

Við áhættustýringu er mikilvægt að fyrir liggi skýr og skjalfest ramma-áætlun um varnir gegn netárásum (e. cyber resilience framework), sem samkvæmt viðauka við leiðbeiningarnar (hugtakalisti) „samanstendur af stefnu, ferlum og umgjörð sem komið hefur verið á í rekstri fjármálainnviðar í því skyni að bera kennsl á, vernda gegn, uppgötva, bregðast við og endurreisa starfsemi eftir netárás af þeim toga sem helst má vænta".[26] Í slíkri áætlun skulu endurspeglast sjónarmið um mikilvægi öryggis og skilvirkni í rekstri þess fjármálainnviðar er um ræðir, sem eiga að styðja við fjármálastöðugleika í víðara samhengi.

Samhliða rammaáætluninni skal setja stefnu um aðgerðir gegn netárásum (e. cyber resilience strategy) en bæði áætlun og stefna skulu staðfestar af stjórn viðkomandi stofnunar með undirritun.[27] Í stefnunni skal m.a. kveðið á um alla þá aðila sem hlut eiga að máli og boðleiðir í því sambandi, sem og þá ferla og tækniatriði er málefnið varðar. Skýrlega skal kveðið á um hlutverk og ábyrgð hvers og eins sem ábyrgð ber á áhættustýringu vegna netárása, þ.m.t. hverjir megi taka ákvarðanir ef á viðnámsþrótt gegn þeim reynir.

Vikið er að ábyrgð annars vegar stjórnar (e. board) og hins vegar stjórnenda (e. senior management) í þessu samhengi í leiðbeiningunum. Stjórn ber ábyrgð á áhættustýringu vegna netógna, með vísan til fyrri umfjöllunar um meginreglu 17 í PFMI og er ætlað að ákveða þolmörk innviðar í þessu sambandi og endurmeta þau reglulega. Æðstu stjórnendum skal falin umsjón með framkvæmd ramma-áætlunarinnar, viðeigandi reglna og aðferða og því að viðeigandi eftirlit sé viðhaft. Jafnframt skulu stjórn og æðstu stjórnendur efla meðvitund um netárásir og stuðla að almennum vilja til skuldbindingar í þá veru að berjast gegn þeim. Tilnefna skal sérstakan ábyrgðaraðila um málaflokkinn í rekstrarumgjörð innviðar og skal hann koma úr röðum æðstu stjórnenda.

Greining

Komi til þjónusturofs í rekstri kerfislega mikilvægs fjármálainnviðar kann það að hafa neikvæð áhrif á fjármálastöðugleika. Ófullnægjandi öryggi og skilvirkni í rekstri slíks innviðar getur enda valdið keðjuverkun milli þátttakenda og markaða. Í þessu samhengi má minna á að staðgengnimöguleikar og tengsl við aðra fjármálainnviði eru á meðal skilgreindra viðmiða sem liggja til grundvallar við ákvörðun um kerfis-

26. Sama heimild, viðauki A (hugtakalisti). E. Cyber resilience framework „consists of the policies, procedures, and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces."

27. Sama heimild, bls. 9-10. Það athugast að í leiðbeiningunum er gert ráð fyrir því að skipulags- og stjórnarhættir fjármálainnviðar geti verið með þeim hætti að ekki sé fyrir að fara eiginlegri eða hefðbundinni stjórn og er þá vísað til „sambærilegs fyrirkomulags" (e. equivalent to [a] board). Þetta ber að hafa í huga þegar í umfjöllun þessari er vísað til stjórnar fjármálainnviðar.

legt mikilvægi einstakra innviða.[28] Mikilvægt er að fyrir liggi greining á því hvaða viðskiptaaðgerðir teljast mikilvægastar í viðkomandi kerfi og á tengdum ferlum, hvaða eignir (þ.m.t. gögn) og kerfisstillingar (þ.m.t. tengingar við önnur innri og ytri kerfi) er mikilvægast að standa vörð um o.s.frv. Skal greiningin m.a. notuð sem viðmið við skjalfesta forgangsröðun í tengslum við áhættustýringu vegna netárása. Fylgjast skal með aðgangsréttindum aðila að kerfum og gögnum, einkum til að koma auga á háttsemi sem kann að teljast óeðlileg. Að því er tengsl innviða varðar skal samhæfa aðgerðir með hlutaðeigandi aðilum.[29]

Varnir

Gæta þarf viðeigandi öryggisráðstafana og haga hönnun upplýsingatæknikerfa og ferla á þann hátt er miði að því að tryggja aðgengi að þjónustu, heilleika og trúnað um gögn/upplýsingar. Varnarráðstafanir skulu ná til tenginga við aðra innviði í samstarfi við hlutaðeigandi. Þá er sérstaklega vikið að mannlega þættinum en áhætta getur steðjað að net- og upplýsingaöryggi frá innherjum. Fylgjast þarf með og bera kennsl á óeðlilega eða óvenjulega starfsemi kerfis, sinna eftirliti með bakgrunni starfsmanna og beita strangri nálgun við aðgangsstýringu. Loks er rík áhersla lögð á að tryggja viðhlítandi þjálfun starfsmanna og að þeir séu ávallt meðvitaðir um hættuna sem stafar af netárásum.[30]

Vöktun

Í rekstrarumgjörð kerfislega mikilvægs fjármálainnviðar skal gera nauðsynlegar ráðstafanir svo að uppgötva megi óeðlilega virkni tímanlega. Mælt er t.d. með því að stöðugt eftirlit sé viðhaft með notkun, framkvæmd ferla og tæknilegum þáttum. Markmiðið er að koma auga á atriði eða aðstæður sem bent geta til yfirvofandi netárásar og að borin séu kennsl á alvarleg rekstrarfrávik þegar í stað, ef til kemur, svo að bregðast megi skjótt við á grundvelli ferla um viðbúnað og samfelldan rekstur.[31]

Endurreisn

Endurreisn eftir alvarlega netárás getur verið flókið viðfangsefni og ólíkt ferli endurreisnar eftir hefðbundið rekstrarrof eins og t.d. við rafmagnsleysi eða bilun í tölvubúnaði. Endurreisn millibankakerfa eftir náttúruhamfarir er enn önnur möguleg sviðsmynd.

Ef á reynir skal samkvæmt leiðbeiningunum vera mögulegt að endurreisa kerfi hratt og örugglega og þannig að hægt sé þá að treysta á áreiðanleika upplýsinganna í kerfinu.[32] Í tilvikum þar sem full endurræsing kerfis er ómöguleg skal áhersla lögð á að endurheimta

28. Þannig má t.d. nefna að seðlabankar einir reka stórgreiðslukerfi á hlutaðeigandi gjaldmiðilssvæði og að peningahluti verðbréfaviðskipta er einatt gerður upp í gegnum stórgreiðslukerfi, með vísan til meginreglu 8 í PFMI. Um kerfislega mikilvæga fjármálainnviði á Íslandi og þau viðmið sem liggja til grundvallar ákvörðun um kerfislegt mikilvægi var fjallað í rammagrein IV-1, bls. 27-28 í riti Seðlabankans, *Fjármálainnviðum*, 2015.
29. Leiðbeiningar CPMI og IOSCO, bls. 11.
30. Sama heimild, bls. 12-14.
31. Sama heimild, bls. 15.
32. Í þessu sambandi er nefnt að árangursríkar endurheimtur gagna kunni að krefjast aðkomu þriðja aðila. Huga skuli að þessu og lagt á það mat hvort gera þurfi upplýsingaskiptasamninga vegna þessa (e. data-sharing agreements).

fyrst mikilvæga þætti; þá mikilvægustu innan tveggja klukkustunda og þannig að uppgjör geti átt sér stað samdægurs.[33] Þetta er óneitanlega háleitt tímamarkmið og byggist á að ferlar hafi verið kortlagðir fyrirfram, s.s. með tilliti til ákvarðanatöku á ögurstundu, og að útbúin hafi verið raunhæf þrepaskipt áætlun um viðbúnað og samfelldan rekstur til notkunar við slíkar aðstæður.[34] Allar áætlanir skulu prófaðar og uppfærðar reglubundið. Ef fyrir liggja upplýsingar um, eða sterkar grunsemdir eru um, að átt hafi verið við gögn eða upplýsingar þarf að bregðast við með viðeigandi hætti áður en starfsemi innviðar er hafin að nýju eftir netárás. Afleiðinga netárása getur gætt í bæði aðal- og varasetrum. Ef tengsl eru fyrir hendi við aðra fjármálainnviði skal sérstaklega hugað að mögulegri smithættu í samstarfi við hlutaðeigandi, svo fljótt sem verða má.

Mælst er til að samskiptaáætlanir liggi fyrir vegna nauðsynlegrar upplýsingamiðlunar og samráðs við alvarleg rekstrarfrávik/þjónusturof eftir því sem við kann að eiga; gagnvart þátttakendum, tengdum innviðum og viðeigandi stjórnvöldum.[35]

Prófanir

Prófanir eru afar mikilvægar fyrir gangsetningu hugbúnaðarlausna en jafnframt sem hluti af reglubundnum öryggisráðstöfunum. Prófanir skulu m.a. fela í sér mat á öryggisveikleikum (e. penetration tests) og svokölluð „*red team tests*" þar sem líkt er eftir raunverulegum netárásum. Prófanirnar skulu miðast við öfgafullar en raunhæfar aðstæður. Mælst er til þess að starfsmenn og hlutaðeigandi ytri aðilar taki þátt í prófunum, t.d. þátttakendur, mikilvægir þjónustuveitendur og tengdir innviðir. Sé það viðeigandi eru þeir aðilar sem reka kerfislega mikilvæga fjármálainnviði hvattir til að taka þátt í viðlagaæfingum sem stjórnvöld kunna að standa fyrir.[36]

Vitundarvakning

Lélegt viðnámsþol með tilliti til net- og upplýsingaöryggis er óásættanlegt í rekstri kerfislega mikilvægra innviða. Af leiðbeiningum CPMI og IOSCO um bestu framkvæmd sem hér hafa verið reifaðar má þó ljóst vera að það er viðamikið verkefni og kostnaðarsamt að bregðast við og verjast netárásum. Brýnt er að tryggja að vitund um netárásir sé almenn í rekstrarumgjörðinni, þ.e. jafnt meðal starfsmanna, stjórnenda og æðstu stjórnar.

Í leiðbeiningunum er áhersla lögð á skipulega söfnun og greiningu upplýsinga um netárásir, sem byggja má á við mótun stefnu og útfærslu viðeigandi ráðstafana í rekstri hlutaðeigandi innviðar. Ennfremur er sérstaklega vikið að miðlun upplýsinga í þessu sambandi gagnvart utanaðkomandi aðilum. Að áliti skýrsluhöfunda er upplýsingamiðlun að einhverju marki nauðsynleg þvert á fjármálakerfi, á viðeigandi grundvelli, í því skyni að stuðla að fumlausum viðbrögðum og

33. Um þetta atriði segir m.a. í leiðbeiningunum: „FMIs should, […] within 12 months of the publication of this Guidance [June 2016], have developed concrete plans to improve their capabilities in order to meet the two-hour RTO, (…)."

34. Sjá tengsl við stutta umfjöllun um greiningu (e. identification).

35. Leiðbeiningarnar, bls. 16-17.

36. Sama heimild, bls. 18-19.

viðbúnaði komi til stórfelldra áfalla vegna netárása.[37] Það að tryggja öryggi mikilvægra innviða samfélagsins er samstarfsverkefni ólíkra stjórnsýslustofnana hér á landi. Umgjörðina þarf eftir því sem við kann að eiga að móta í samræmi við samkeppnislög, reglur um meðferð trúnaðarupplýsinga o.fl.

Lærdómur og þróun

Aðferðir við netárásir eru í stöðugri þróun. Því til samræmis þarf sífellt að aðlaga fyrirliggjandi rammaáætlanir um varnir gegn netárásum. Mikilvægt er að draga lærdóm af árásum sem upp koma og greina markvisst. Tækniþróun ber stöðugt að vakta í því skyni að bera kennsl á nýja mögulega ógn og útfæra frekar varnir og viðbrögð.[38]

Að hverjum beinast leiðbeiningarnar?

Af framansögðu má ljóst vera að leiðbeiningum CPMI og IOSCO, *Guidance on cyber resilience in financial market infrastructures*, er fyrst og fremst beint til þeirra sem falla undir skilgreiningu PFMI á hugtakinu kerfislega mikilvægir fjármálainnviðir, þ.e. greiðslukerfa sem geta hrundið af stað og/eða breitt út kerfislega röskun, verðbréfauppgjörskerfa, verðbréfamiðstöðva, miðlægra mótaðila og afleiðuviðskiptaskráa.

Í leiðbeiningunum er hins vegar vakin athygli á að viðeigandi stjórnvöld geta jafnframt ákveðið að beita þeim gagnvart öðrum innviðum.[39] Til dæmis megi horfa til viðmiða þeirra við mat eftirlitsaðila á ráðstöfunum kerfislega mikilvægra greiðsluþjónustuveitenda í því skyni að tryggja net- og upplýsingaöryggi og vægi þeirra í rekstraráhættu.

Viðeigandi og virk framkvæmd áhættustýringar með tilliti til rekstraráhættu og varna gegn netárásum, stöðugt endurmat og prófanir eru nauðsynlegar. En hvenær er nóg að gert? Það er vitaskuld háð mati og aðstæðum en í tilviki millibankakerfa hlýtur markið að verða sett nokkuð hátt.

37. Sama heimild, bls. 20-21. Af áhugaverðum fyrirmyndum erlendis má nefna FS-ISAC (e. Financial Services Information Sharing and Analysis Center). Til þess samstarfsvettvangs var stofnað á grundvelli bandarískrar löggjafar, en samkvæmt sérstakri ákvörðun er hann ekki lengur bundinn við Bandaríkin heldur alþjóðlegur. Á heimasíðu FS-ISAC segir um samstarfsvettvanginn: „The FS-ISAC gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector around the world. Sources of information include commercial companies who gather this type of information, government agencies, CERTs, academic sources, and other trusted sources. After analysis by industry experts, alerts are delivered to participants based on their level of service."

38. Leiðbeiningarnar, bls. 22.

39. Sama heimild, bls. 7-8.