Systeeminen turvallisuusjohtaminen

Systeemisen turvallisuusjohtamisen päätavoite on turvallisuuden lisääminen erityisesti huomioiden turvallisuustoimenpiteiden keskinäiset vuorovaikutukset ja takaisinkytkennät. Intensiivikurssi näiden käytännönläheisten kysymysten tiimoilta keräsi kymmenen alan perus- ja jatko-opiskelijaa Aalto-yliopistoon syksyllä 2015.

Teksti: Antti Toppila ja Björn Wahlström

ALTO-YLIOPISTON intensiivikurssi ”Systeeminen turvallisuuden suunnittelu ja johtaminen” pidettiin 1.–3.9.2015 Espoon Otaniemessä, entisessä TKK:n päärakennuksessa, joka nykyisin toimii Aalto-yliopiston kandidaattiopintojen keskuksena. Kurssihenkilökunta koostui tämän artikkelin kirjoittajista: luennoista ja opetussisällöistä vastasi Björn Wahlström ja käytännön järjestelyistä vastasi Antti Toppila.

Miksi kurssi systeemisestä turvallisuusjohtamisesta?

Systeemiseen näkökulmaan kuuluu kokonaisuuden hahmottaminen, jotta toimenpiteet osataan suhteuttaa ja ajoittaa oikein. Systeeminen turvallisuusjohtaminen painottaa erityisesti vuorovaikutuksia ja takaisinkytkentöjä, joita eri tekijöistä ja toimenpiteistä seuraa. Takaisinkytkentöihin perustuvia tasapainoja, joita turvallisuusjohtamisessa on huomioitava, ovat mm. huolellisuus-tehokkuus, kilpailu-yhteistyö, prosessi-tuote ja valvonta-luottamus. Liiallinen panostus yhteen toisen kustannuksella aiheuttaa helposti turvallisuuteen negatiivisesti vaikuttavan takaisinkytkennän, joka pahimmillaan saattaa tehdä panostuksen nettovaikutuksen turvallisuutta vähentäväksi.

Esimerkkinä ei-toivotusta takaisinkytkennästä ovat tieliikenteen nopeusrajoitukset. Liian alhaisilla rajoituksilla jotkut kokevat rajoituksen ylityksen pienenä rikkeenä ja tästä johtuen nopeuserot teillä kasvavat. Nopeuserot puolestaan korreloivat vahvasti lisääntyneiden liikenneonnettomuuksien kanssa. Turvallisuusjohtamisessa on siten huomioitava kaikkien tekijöiden systeemiset vaikutukset ja osattava punnita niitä ja niiden merkittävyyttä keskenään.

Riskien aina vain tarkempi mallintaminen ei välttämättä lisää turvallisuutta. Tämä johtuu siitä, että mallinnukseen liittyvät epävarmuudet ovat joka tapauksessa suuret, jolloin paremmalla mallilla saatetaan saada tuotettua vain marginaalisesti turvallisempia ratkaisuja, joiden implementointi voi olla virhealtista ja viedä resursseja tehokkaammilta ratkaisuilta. Kokonaisuuden ymmärtäminen sekä siihen vaikuttamisen mekanismien sisäistäminen ovat keskeisiä teemoja systeemisessä turvallisuusjohtamisessa.

Turvallisuuteen käytettävien resurssien rajallisuudesta johtuen kaikkia turvallisuutta parantavia toimenpiteitä ei voida toteuttaa. Tästä syystä on etsittävä niitä toimenpiteitä, jotka tehokkaasti korjaavat löydettyjä puutteita pidemmän ajanjakson yli. Merkittäviin riskeihin pitää kuitenkin puuttua jo järjestelmien suunnitteluvaiheessa.

Turvallisuus – ”näin me tehdään bisnestä”

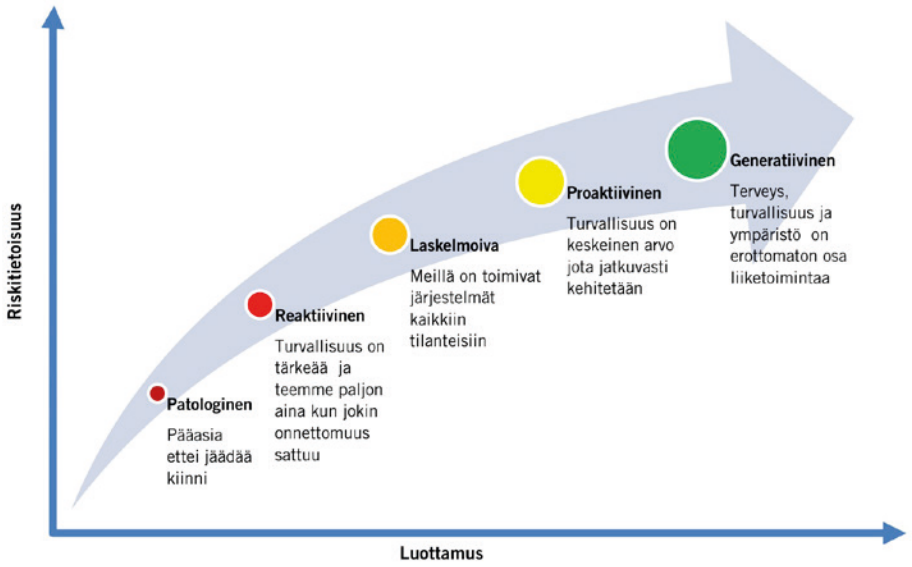
Huomattava esimerkki turvallisuusjohtamisen näkökulmista on kansainvälisen energiayhtiö BP plc:n johdon toiminta 2000-luvun aikana. Tänä ajanjaksona yhtiön surullisen kuuluisaan historiaan kuului mm. Deepwater Horizon lautan palo, räjähdykset Texas Cityn jalostamossa sekä vuodot Alaskan öljykentillä.

BP:n organisaatiossa turvallisuuskysymykset koettiin toimintaa haittaavina tai tehokkuutta vähentävinä. Niihin suhtauduttiin vähättelevästi, huolimattomasti tai jopa vastustavasti. Tämä lähtökohta oli jyrkkä vastakohta sille ideaalille, että turvallisuus 1) on keskeinen osa liiketoimintaa, 2) varmistaa toiminnan ennustettavuuden ja 3) pitkällä aikavälillä myös kustannustehokkuuden, kun onnettomuuksilta vältytään.

BP:n tapauksen pohjalta on helppo ymmärtää, miten turvallisuuskulttuurin puutteita voidaan tunnistaa ja mitä keinoja on käytettävissä niiden parantamiseksi. BP:n tapauksesta nousee esiin lyhytnäköisyys päätöksenteossa ja nopea kasvu hinnalla millä hyvänsä. Merkillepantavaa on myös, että BP:n toimin-

DI Antti Toppila
Tohtorikoulutettava
Aalto-yliopisto
antti.toppila@aalto.fi

TkL Björn Wahlström
Professori emeritus
Aalto-yliopisto
bjorn.wahlstrom@aalto.fi



Kuva 1. Turvallisuuskulttuurin tasoja.

taan ei puututtu viranomaisten toimesta, vaikka mahdollisuuksia olisi ollut. Valtiovalta oli jopa kannustamassa onnettomuuksia kokenutta yhtiötä porauksiin Meksikonlahden syvillä vesillä, jotta Yhdysvaltojen kotimarkkinoille saataisiin edullista öljyä ja työpaikkoja.

Johtopäätöksenä voidaan pitää, että BP organisaationa oli ajautunut tilaan, jossa mikään riskianalyysi ei olisi kyennyt estämään onnettomuuksia, koska yhtiön turvallisuuskulttuuri oli kehittymätön. Kuvan 1 mukaisen turvallisuuskulttuurin kehittyneisyyttä kuvaavan mittariston [1] perusteella BP olisi joutunut alimpaan tai toiseksi alimpaan luokkaan, jossa onnettomuuksista ei välitetä, ellei niistä jäädä kiinni tai toimenpiteisiin ryhdytään vasta kun onnettomuus sattuu. Matkaa parhaimmalle, eli generatiiviselle tasolle, jossa turvallisuus on erottamaton osa organisaation toimintaa, oli todella paljon.

BP:n vastakohtana voitaneen pitää pohjoismaista ydinvoimateollisuuden turvallisuuskulttuuria, jossa uhkiin varaudutaan ennakoiden ja vakavuudella. Laitoksia operoivat tahot osallistuvat aktiivisesti turvallisuutta kehittävään tutkimukseen ja varmistavat laitosten turvallisen hyödyntämisen sekä tietotaidon säilymisen pitkällä aikavälillä. Toiminta on kansainvälistä ja avointa, eikä voimayhtiöiden välinen kilpailu ole johtanut yhteistyökyvyttömyyteen turvallisuustutkimuksen tai käyttökokemusten jakamisen osalta. Myös valvovan viranomaisen toiminta ja lainsäädäntö on asianmukaisella tasolla.

Organisaation kokonaisvaltainen turvallisuustarkastelu

Kokonaisuuden hahmottamisen sovelluksia voidaan havainnollistaa perussyysanalyysin kautta. Tässä analyysimenetelmässä onnettomuuteen johtaneita tapahtumaketjuja seurataan syy-seurausketjujen avulla ajassa taaksepäin, kunnes löydetään ne syyt, joita korjaamalla voidaan olettaa, että vastaavantyyppinen onnettomuus ei enää voisi tapahtua.

Kokonaisuuden kannalta perussyitä kannatta kartoittaa niin kauas kun 1) kartoittamisen voidaan järkevästi olettaa synnyttävän turvallisuutta parantavia toimenpiteitä ja 2) kartoittaminen tuottaa ymmärrystä ja oppeja joita viedään osaksi organisaation käytäntöjä. Tällöin voidaan saada organisaation kanssa vaikuttavat tahot, niin tuotantohenkilökunta, taloushenkilöstö kuin asiakkaatkin, sitoutetuksi yhteiseen turvallisuuden parantamiseen. Organisaation turvallisuusajattelua ja -kulttuuria voidaan tällä tavalla kehittää samalla kun varaudutaan yksittäisiin riskeihin.

Tarkastellaan esimerkinomaista onnettomuustilannetta, jossa huoltomies on kivunnut tikkaita pitkin tarkastelemaan ilmastointilaitetta, pudonnut lattialle, ja joutunut viikonlopun yli odottamaan apua. Syitä tapahtumaketjuun ovat mm. ilmastoinnin suunnittelu (miksi huollettava laite asennettu katonrajaan?), toimintatavat (miksi korjaajaa toimi yksin? miksi vartiointi ei havainnut loukkaantunutta huoltomiestä?), ja hankintatoimen käytänteet (miksi hankintavaiheessa riskiä ei havaittu?). Yksittäisen onnettomuuden analysoinnin kautta voidaan siis löytää organisaation toiminnassa olevia puutteita, joiden korjaaminen voisi estää samantapaisten onnettomuuksien syntymisen jatkossa.

Vuorovaikutusmalli kokonaisuuden hallintaan

Kuten edeltävästä esimerkistä ilmenee, organisaation kokonaisvaltainen turvallisuusanalyysi edellyttää monipuolista näkemystä turvallisuutta luovista ratkaisuista. Käsitteellinen MTOI-malli (MTOI = Man Technology Organization Information [2]) luo perustan vuorovaikutusten jaottelemiseksi, kuten havainnollistetaan kuvassa 2. Mallin mukaan organisaation toiminnan voidaan ajatella koostuvan teknisestä järjestelmästä, sitä käyttävästä henkilökunnasta, henkilöiden keskinäisestä vuorovaikutuksesta organisaation toimintatapojen mukaisesti ja tiedon kulusta sitä tarvitsevien tahojen välillä.

MTOI-mallia voidaan käyttää käsitteellisenä mallina keskeisten organisaation vuorovaikutusmekanismien luokitteluun ja ymmärtämi-

Näkemyksiä kurssin

KURSSIN PUITTEISSA opiskelijat kirjoittivat noin 10 sivun mittaisen esseen valitsemastaan kurssin piirissä olevasta aiheesta. Aiheita olivat mm. Challenger sukkulan vikaantumisen tai pienen IT-asiantuntijaorganisaation riskikartoitus sekä kaupunginosan kyberturvallisuus. Alla on pari lyhyttä tiivistelmää esseissä esiintyneistä opiskelijoiden omiin pohdintoihin perustuvista ajatuksenkuluista.

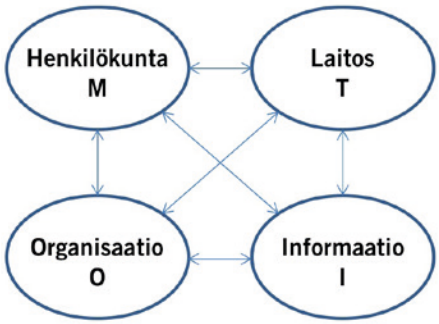
1. **Kuntayhtymän kyberturvallisuus** on monen toimijan vastuulla. Kun toimijoita on useampia, voidaan avoimella tietojen vaihdolla estää hakkeria toistamasta hyökkäystään useampaa toimijaa kohtaan, elleivät hyökkäykset kohdistu niin lyhyelle aikavälille, että niihin reagoiminen ei onnistu. Avoin tietojen vaihto on kuitenkin myös uhka, sillä se edellyttää myös turvallisuustoimintojen yksityiskohtien jakamisen suuremmalle määrällä toimijoita. Tällöin hakkeri voi saada useammalta taholta käsiinsä

seen. Kurssilla keskusteltiin myös mallin käyttämistä parametrisena mallina, jonka pohjalta laadittavan mittariston avulla voidaan tarkkailla organisaation turvallisuutta riittävän monipuolisesti.

Mittaristo voisi perustua seuraavaan jaotteluun: laitoksen teknistä turvallisuutta voidaan seurata todennäköisyyspohjaisen riskianalyysin (probabilistic risk assessment, PRA), nykyisten ja tulevien parannusinvestointien sekä kunnossapitotoimien pohjalta. Henkilökunnan osaamistasoa mittaa mm. heidän koulutustasonsa ja kokemusvuotensa. Organisaation kyvykkyyttä tarkkaillaan auditointien ja kansainvälisten suorituskykyvertailuiden avulla.

Informaation osalta mittaristo voi perustua dokumentaation ajantasaisuuteen (milloin päivitetty/tarkastettu viimeksi?) ja dokumentaatiojärjestelmän kattavuuteen, helppokäyttöisyyteen ja toimintavarmuuteen. Myös vikatilanteiden harjoituksista tai auditoinneista saaduista kokemuksista voidaan tehdä päätelmiä informaatiojärjestelmän kehitystarpeista.

Mittarit voidaan MTOI mallin mukaisen jaotuksen lisäksi jaotella tulevaisuutta ja menneisyyttä kuvaaviin mittareihin (ns. leading and lagging indicators). Tämä jaottelu auttaa hahmottamaan suuntaa johon organisaation turvallisuustilanne on kehittymässä ja arvioimaan kehityksen riittävyyttä.



Kuva 2. MTOI malli.

Turvallisuuden parantaminen tulevaisuudessa

Turvallisuusjohtamisen perusdilemma on samanaikaisesti todistaa että järjestelmä on riittävän turvallinen ja silti kyseenalaistaa järjestelmän turvallisuus uskottavalla tavalla. Erityisen haasteen niin turvallisuuden todistamiselle kuin turvallisuuden järkevälle kyseenalaistamiselle muodostavat nk. mustat joutsenet, eli merkittävät riskitapahtumat, joista ei ole kokemusperäistä tietoa, joten niiden tapahtumista ei ole osattu edes kuvitella mahdollisiksi. Resilienssi, jota voidaan luonnehtia järjestelmän kykynä palautua vikatilanteista, on eräs tapa hallita tällaisia tapahtumia.

Teknologian kehittyessä järjestelmät ovat muuttuneet monimutkaisimmiksi. Niiden ohjaamiseen tarvitaan nykyään huomattava määrä prosessiautomaatiota. Digitaaliset automaatiojärjestelmät ovatkin tuoneet ohjelmistojen virheiden ja haavoittuvuuksien analysoinnin turvallisuustutkimuksen ytimeen. Nykyaikaiset järjestelmät ovat tietojärjestelmien yleistymisen ja verkottumisen myötä myös alttiimpia älykkään toimijan häirinnälle ja sabotaasille.

Turvallisuuskriittistä teknologiaa, kuten salasanatunnistautumista, sähköpostia, verkkopankkitunnuksia ja USB-tikkuja käytetään niin yksityis- kuin työelämässäkin. Erinäisten järjestelmien verkostumisen myötä hakkerit voivatkin hyödyntää turvallisuusaukkoja heikoimmassa järjestelmässä vahvempien järjestelmien hakkeroimiseksi. Yksittäinen ihminen ei välttämättä osaa tai huomaa käyttää tarvittavia suojakeinoja kaikissa järjestelmissä. Tunkeutumisen tunnistaminen ja siltä suojautuminen erilaisilla puolustusmekanismeilla onkin tärkeä tutkimussuuntaus kyberturvallisuuden parantamiseksi.

Riskienhallinnassa käytetyt menetelmät ja mallit ovat kehittyneet paljon viimeisten vuosikymmenien aikana. Tämän kehitystyön täysimittainen hyödyntäminen edellyttää suuria tietomääriä ja useiden mallien ja menetelmien kehittämistä ja käyttämistä.

Kurssin sanoma

Turvallisuutta kehittäessä keskeinen kysymys onkin, kykenevätkö ihmiset hallitsemaan monimutkaisia järjestelmiä, joiden turvallisuus rakentuu syvyyssuuntaiseen puolustukseen. Järjestelmien turvallisuussuunnitteluun pitää panostaa riittävästi ja niiden käyttämiseen liittyvät riskit pitää saattaa niin pieniksi, että niitä voidaan pitää hyväksyttävinä. Mikäli järjestelmään liittyy liian suuria riskejä, sitä ei pidä ottaa käyttöön tai sen käyttö on hallitusti keskeytettävä.

Järjestelmän käyttöönotto edellyttää myös, että sitä käyttävälle organisaatiolle on kehittynyt riittävän hyvät tekniset apuvälineet ja keinot, sekä turvallisuustoiminnot ja -käytännöt riskien hallitsemiseksi. Tämä kehitys edellyttää kriittistä suhtautumista riskien esiintymiseen, halua kehittää, oppia ja ymmärtää eri teknologioihin liittyviä riskejä sekä kykyä luoda ymmärtämistä tukevia oppimisprosesseja. Lisäksi riskienhallinnan kattavuuden ja riittävyyden osoittaminen on tehtävä riippumattomasti, avoimesti ja ennen kaikkea kriittisesti.

Kurssin verkkosivut: http://sal.aalto.fi/en/gradschool/courses/turvallisuus

opiskelijoilta

tietoja järjestelmän rakenteesta, joita käyttäen hyökkäyksen suunnittelu ja toteuttaminen mahdollistuu.

2. **Syvyyssuuntainen puolustus** on tehokas tapa suojautua riskeiltä, mutta inhimilliset toimijat voivat aiheuttaa uhkia tämän periaatteen toimivuuteen, etenkin jos turvallisuuskulttuurissa on puutteita. Esimerkiksi laitteiden ja rakenteiden testaamisen yhteydessä ihmiset saattavat tiedostamattaan etsiä vain vahvistusta olettamukselle, että komponentti omaa siltä vaadittavat ominaisuudet sen sijaan, että tehokkaasti pyrittäisiin kumoamaan tämä oletus. Esimerkiksi BP:n Meksikonlahden onnettomuutta analysoidessa, muiden virheiden lisäksi testaajat etsivät aktiivisesti syitä hylkäävälle testitulokselle omasta toiminnastaan, jolloin he jättivät huomiotta mahdollisuuden, että testattava komponentti todellakin olisi viallinen.

Viitteet:

[1] D. Parker, M. Lawrie, P. Hudson. 2006. A framework for understanding the development of organisational safety culture, Safety Science 44 551–562.

[2] B. Wahlström, C. Rollenhagen 2014. Safety management – a multi-level control problem. Safety Science, 69, pp. 3–17.