TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ohjelmistoturvallisuuden tila 2023

Nykytilaraportti

Timo Kiravuo
Päivi Timlin
Karoliina Kemppainen
Juhani Eronen
Saana Seppänen

Traficomin tutkimuksia ja selvityksiä
Traficoms forskningsrapporter och utredningar
Traficom Research Reports

20/2023

TRAFICOM
Liikenne- ja viestintävirasto

Julkaisupäivämäärä
12.10.2023

Julkaisun nimi Ohjelmistoturvallisuuden tila 2023			
Tekijät Timo Kiravuo, Päivi Timlin, Karoliina Kemppainen, Juhani Eronen, Saana Seppänen			
Toimeksiantaja ja asettamispäivämäärä Huoltovarmuuskeskus			
Julkaisusarjan nimi ja numero Traficomin tutkimuksia ja selvityksiä 20/2023	ISSN (verkkojulkaisu) 2669-8781 ISBN (verkkojulkaisu) 978-952-311-882-9		
Asiasanat ohjelmistoturvallisuus, tietoturvallinen ohjelmistokehitys, DevOps, DevSecOps, Security by Design			
Tiivistelmä Suomessa ollaan tietoisia ohjelmistoturvallisuuden merkityksestä. Ohjelmistoala on jatkuvassa ja nopeassa muutoksessa. Turvallisuuden taso ohjelmistotyössä on noussut, mutta ei samaa vauhtia kuin teknologia- ja toimintatapamuutokset. Ohjelmistoja tuottavilla, hankkivilla ja hyödyntävillä organisaatioilla ei ole yhteistä, jaettua näkemystä siitä, kenelle vastuu tietoturvallisuudesta ohjelmistotyössä kuuluu. Turvallisuuden tarve ymmärretään yleisellä tasolla, mutta toteutustasolla vastuut ja turvallisuuden vaatimukset eivät konkretisoidu tekemiseen. Osalla organisaatioista osaaminen ja toteutuskyky on korkealla tasolla, mutta toisilla on huomattavia haasteita jo perustason turvallisuuden toteuttamisessa. Tarvitaan tietoisuutta ongelmasta ja menetelmiä käytännön ratkaisuiksi. Ratkaisuksi raportti esittää, että ymmärrystä turvallisen ohjelmistokehityksen vaatimuksista ja tavoitteista tulee lisätä laaja-alaisesti organisaatioissa. Tietoturvallisuus on keskeinen osa organisaatioiden riskienhallintaa. Tämän vuoksi tietoisuutta ohjemistokehityksen turvallisuusvaatimuksista tulee tarjoa aina liikkeenjohdosta ohjelmistokehittäjiin. Organisaatioden tulee panostaa uusien ja hyvien käytäntöjen jakamiseen sekä eri tehtävissä työskentelevien asiantuntijoiden osaamisen ylläpitämiseen ja kehittämiseen.		
Yhteyshenkilö Juhani Eronen	Raportin kieli suomi	Luottamuksellisuus Julkinen	Kokonaissivumäärä 45
Jakaja Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus	Kustantaja Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus		

TRAFICOM
Transport- och kommunikationsverket

Utgivningsdatum
12.10.2023

Publikation Läget för programvarusäkerheten 2023			
Författare Timo Kiravuo, Päivi Timlin, Karoliina Kemppainen, Juhani Eronen, Saana Seppänen			
Tillsatt av och datum Försörjningsberedskapscentralen			
Publikationsseriens namn och nummer Traficoms forskningsrapporter och utredningar 20/2023	ISSN (elektronisk publikation) 2669-8781 ISBN (elektronisk publikation) 978-952-311-882-9		
Ämnesord programvarusäkerhet, informationssäker programvaruutveckling, DevOps, DevSecOps, Security by Design			
Sammandrag I Finland är vi medvetna om betydelsen av programsäkerheten. Programvarubranschen genomgår en ständig och snabb förändring. Nivån på säkerheten i programvaruarbetet har stigit, men inte i samma takt som förändringarna i teknologin och verksamhetssätten. Organisationer som producerar, skaffar och utnyttjar programvaror har ingen gemensam, delad syn på vem som ansvarar för informationssäkerheten i programvaruarbetet. Vi förstår behovet av säkerhet på ett allmänt plan, men på genomförandenivå konkretiseras inte ansvaren och kraven på säkerhet i arbetet. En del av organisationerna har en hög kompetens och genomförandeförmåga, men andra har betydande utmaningar redan i att genomföra säkerheten på basnivå. Vi behöver medvetenhet om problemet och metoder för praktiska lösningar. Som en lösning föreslår rapporten att förståelsen för kraven och målen för en säker programvaruutveckling ska ökas på ett övergripande sätt i organisationerna. Informationssäkerhet är en central del av organisationernas riskhantering. Därför ska medvetenheten om säkerhetskraven för programvaruutveckling alltid tillhandahållas från företagsledning till programvaruutvecklare. Organisationerna ska satsa på att dela med sig av ny och god praxis samt på att upprätthålla och utveckla kompetensen hos experter som arbetar inom olika uppgifter.		
Kontaktperson Juhani Eronen	Språk finska	Sekretessgrad Offentlig	Sidoantal 45
Distribution Transport- och kommunikationsverket Traficom, Cybersäkerhetscentret	Förlag Transport- och kommunikationsverket Traficom, Cybersäkerhetscentret		

TRAFICOM
Finnish Transport and Communications Agency

Date of publication
12.10.2023

Title of publication
Status of software security 2023

Author(s)
Timo Kiravuo, Päivi Timlin, Karoliina Kemppainen, Juhani Eronen, Saana Seppänen

Commissioned by, date
National Emergency Supply Agency

Publication series and number
Traficom Research Reports 20/2023

ISSN (e-publication) 2669-8781
ISBN (e-publication) 978-952-311-882-9

Keywords
software security, secure software development, DevOps, DevSecOps, Security by Design

Abstract
The importance of software security is recognised in Finland. The software industry is undergoing constant, rapid change. The level of security in software work has risen, but not at the same speed as the changes in technology and operating methods. The organisations producing, procuring and using software do not have a common and shared view of who is responsible for information security in software work. The need for security is understood on a general level, but on the level of implementation, the responsibilities and security requirements do not become actions in reality. In some of the organisations, the expertise and implementation capabilities are at a high level, but others have considerable challenges already in implementing a basic level of security.

Awareness of the problem and methods for practical solutions are needed.

As a solution, the report proposes increasing the understanding of the requirements and objectives of secure software development widely in the organisations. Information security is a key part of the risk management of organisations. Therefore, awareness of the security requirements of software development should be offered to everyone from company management to software developers. Organisations must invest in sharing good new practices as well as maintaining and developing the competence of experts working in different tasks.

Contact person	Language	Confidence status	Pages, total
Päivi Timlin, Juhani Eronen	Finnish	Public	45

Distributed by Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland

Published by
Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland

ALKUSANAT

Tämä selvitysraportti kuvaa ohjelmistoturvallisuuden tilaa Suomessa keväällä 2023. Raportti perustuu haastatteluihin, kyselytutkimukseen ja työpajoihin, joiden avulla on saatu ajantasainen kuva nopeasti kehittyvästä toimialasta.

Huoltovarmuuskeskus ja Liikenne- ja viestintävirasto Traficom käynnistivät Huoltovarmuuskeskuksen rahoittamana selvityksen turvallisen ohjelmistokehityksen nykytilasta. Selvityksen tavoitteena oli myös tunnistaa toimenpiteitä, miten turvallista ohjelmistokehitystä ja ohjelmiston hankintaa voidaan kehittää kansallisella tasolla. Turvallisen ohjelmistokehityksen selvityksen pohjalta on muodostettu toimenpidesuunnitelma, jossa esitetyt ratkaisut perustuvat selvitystyöhön. Suunnitelma toimii pohjana jatkokehitykselle, joka toteutetaan osana Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelmaa.

Tutkimuksen ovat toteuttaneet Timo Kiravuo, Consultor Finland oy, sekä Traficomin Kyberturvallisuuskeskuksen asiantuntijat Päivi Timlin, Karoliina Kemppainen, Juhani Eronen ja Saana Seppänen, Teemu Juujärvi ja Jouni Vaahtera. Projektilla oli ohjausryhmä, johon kuuluivat Jukka Uusitalo, Huoltovarmuuskeskus ja Päivi Timlin, Traficomin Kyberturvallisuuskeskus.

Digipoolin Kyberturvallisuuden nykytila -selvityksessä turvallinen ohjelmistokehitys on nostettu yhdeksi kolmesta tärkeimmästä kehityskohteesta. Ohjelmistoturvallisuus on tärkeää koko yhteiskunnalle ja erityisesti huoltovarmuuskriittisille toimijoille. Raportti on kohdistettu organisaatioille, jotka hyödyntävät ohjelmistotekniikkaa toiminnassaan toteuttamalla tai hankkimalla ohjelmistoja. Raportissa tarkastellaan myös alan koulutustarpeita.

Selvityksen havaintojen perusteella moni asia on jo hyvin, mutta tähän ei pidä tuudittautua. Nopeasti muuttuva toimintaympäristö, teknologinen kehitys ja EU:sta tuleva sääntely haastavat organisaatioita tietoturvallisen palvelun hankinnassa, kehittämisessä ja ylläpidossa. Tarjolla on runsaasti erilaisia ohjeita ja käytäntöjä ohjelmistoturvallisuuden parantamiseksi. Vaikeus on löytää niiden joukosta toimivin ratkaisu omalle organisaatiolle, sillä kansallisten ja kansainvälisten standardien, ohjeiden ja hyvien käytänteiden hyödyntäminen vaatii perehtyneisyyttä ja aktiivisuutta. Ohjausta ja neuvontaa turvalliseen ohjelmistokehitykseen ja tietoturvallisten ohjelmistojen hankintaan ei ole tai sitä ei osata hyödyntää.

Raportin kursiivilla merkityt lainaukset ovat selvitystyöstä poimittuja lausahduksia ja kommentteja.

Helsinki, 11. lokakuuta 2023

Jukka-Pekka Juutinen
vt. ylijohtaja
Liikenne- ja viestintävirasto Traficom

FÖRORD

Den här utredningsrapporten beskriver läget för programsäkerheten i Finland våren 2023. Rapporten baserar sig på intervjuer, enkäter och workshoppar som har gett en aktuell bild av branschen, som utvecklas snabbt.

Försörjningsberedskapscentralen och Transport- och kommunikationsverket Traficom inledde med finansiering av Försörjningsberedskapscentralen en utredning om nuläget för en säker programvaruutveckling. Syftet med utredningen var också att identifiera åtgärder för hur en säker programvaruutveckling och anskaffning av program kan utvecklas på nationell nivå. Utgående från utredningen om en säker programvaruutveckling har vi upprättat en åtgärdsplan, där de lösningar som presenteras baserar sig på utredningsarbetet. Planen utgör grunden för den fortsatta utvecklingen, som genomförs som en del av Försörjningsberedskapscentralens program Digital säkerhet 2030.

Undersökningen har genomförts av Timo Kiravuo, Consultor Finland oy, samt av sakkunniga Päivi Timlin, Karoliina Kemppainen, Juhani Eronen och Saana Seppänen, Teemu Juujärvi och Jouni Vaahtera vid Cybersäkerhetscentret vid Traficom. Projektet hade en styrgrupp som bestod av Jukka Uusitalo vid Försörjningsberedskapscentralen och Päivi Timlin vid Cybersäkerhetscentret vid Traficom.

I Digipoolis utredning om nuläget i cybersäkerheten har säker programutveckling lyfts fram som ett av de tre viktigaste utvecklingsobjekten. Programvarusäkerheten är viktig för hela samhället och i synnerhet för de aktörer som är kritiska för försörjningsberedskapen. Rapporten riktar sig till organisationer som utnyttjar programvaruteknik i sin verksamhet genom att förverkliga eller skaffa programvaror. I rapporten granskas också utbildningsbehoven inom branschen.

Utifrån observationerna i utredningen finns det mycket som redan är bra, men vi får inte invagga oss i detta. Den snabbt föränderliga verksamhetsmiljön, den tekniska utvecklingen och EU:s reglering utmanar organisationerna i upphandlingen, utvecklingen och underhållet av informationssäkra tjänster. Det finns en mängd olika riktlinjer och metoder för att förbättra programvarusäkerheten. Svårigheten är att bland dessa hitta den mest fungerande lösningen för den egna organisationen, eftersom det krävs kännedom och aktivitet för att kunna utnyttja nationella och internationella standarder, anvisningar och god praxis. Det finns ingen handledning och rådgivning för informationssäker programvaruutveckling och anskaffning av informationssäkra programvaror eller så kan man inte utnyttja detta.

Citaten som anges i rapporten med kursiv stil är kommentarer och yttranden som hämtats från utredningsarbetet.

Helsingfors, den 11 oktober 2023

Jukka-Pekka Juutinen
Överdirektör
Transport- och kommunikationsverket Traficom

FOREWORD

This report describes the status of software security in Finland in the spring of 2023. The report is based on a survey, interviews and workshops that have been used to obtain an up-to-date picture of the rapidly developing industry.

The National Emergency Supply Agency and the Finnish Transport and Communications Agency Traficom started a study of the current status of secure software development, funded by the National Emergency Supply Agency. The goals of the study also included identifying measures for developing secure software development and software procurement at the national level. An action plan has been drawn up based on the study of secure software development; the solutions presented in it are based on the work done for the study. The plan acts as a basis of further development to be implemented as a part of the Digital Security 2030 programme of the National Emergency Supply Agency.

The study has been implemented by Timo Kiravuo, Consultor Finland oy, as well as the experts Päivi Timlin, Karoliina Kemppainen, Juhani Eronen and Saana Seppänen, Teemu Juujärvi and Jouni Vaahtera of the National Cyber Security Centre Finland (NCSC-FI) of Traficom. The project had a steering group that included Jukka Uusitalo, the National Emergency Supply Agency and Päivi Timlin, NCSC-FI, Traficom.

In the Current State of Cybersecurity survey by the Digital Pool, secure software development has been highlighted as one of the three most important development targets. Software security is important for society as a whole, and especially for the operators critical to the security of supply. The report is targeted at organisations that use software technology in their operations by implementing or procuring software. The report also reviews the need for training and education in the field.

Based on the observations in the study, many things are already going well, but this should not create a false sense of security. The rapidly changing operating environment, the technological development and the regulations from the EU challenge organisations in procuring, developing and maintaining services in an information secure manner. There are plenty of different kinds of instructions and practices available for improving software security. The difficulty lies in finding the solution that works best with one’s own organisation, because the use of national and international standards, instructions and good practices requires study and proactivity. Either there is no guidance and advice for secure software development and the procurement of information secure software, or people do not know how to take advantage of it.

The quotes in the report in italics are statements and comments selected from the work done in the study.

Helsinki, 12 October 2023

Jukka-Pekka Juutinen
Deputy Director-General
Finnish Transport and Communications Agency Traficom

Sisällysluettelo

1 Raportin termejä

Agile	Ohjelmistokehitysmetodi, joka olettaa vaatimusten muuttuvan jatkuvasti kehitystyön aikana
CI/CD-putki	Continuous Integration / Continuous Delivery, ohjelmistokehitysmenetelmä, jolle on tyypillistä pienten muutosten jatkuva tuotantoonvienti ja etenkin tähän liittyvä automaattinen testaus
CRA	Cyber Resilience Act, Kyberkestävyyssäädös, EU:n valmistelussa oleva lainsäädäntö ohjelmistojen elinkaaren kattavasta tuotevastuusta
DevOps	Ohjelmistokehityksen ja tuotannon yhdistävä toimintatapa
DevSecOps	Kehitystiimin vastuuta ohjelmistoturvallisuudesta sekä kehityksessä että tuotannossa korostava toimintatapa
DVV	Digi- ja väestötietovirasto
ISO 27001	International Organization for Standardizationin yleisesti käytössä oleva tietoturvallisuuden hallintajärjestelmän määrittävä standardi
IT	Information Technology, tietotekniikka
Kyberturvallisuus	Digitaalisen ja verkottuneen yhteiskunnan tai organisaation ja niiden toimintojen turvallisuus
NIS2	Network and Information Security -direktiivi II, yhteiskunnan kriittisten tietojärjestelmien turvallisuutta edellyttävä lainsäädäntö EU:sta
NIST CSF	USA:n National Institute of Standards and Technologyn laatima Cybersecurity Framework, kyberturvallisuuden hallintamalli
Ohjelmistoturvallisuus	Kyberturvallisuuden osa-alue, joka kattaa ohjelmistojen suunnittelun, toteutuksen ja käytön turvallisuuden
OT	Operational Technology, fyysisiä järjestelmiä (esim. tehtaat, lentokoneet) ohjaava tietotekniikka
OWASP	Open Worldwide Application Security Project, ohjelmistoturvallisuutta edistävä vapaaehtoisyhteisö
PCI-DSS	Payment Card Industry Data Security Standard, maksukorttien tietojen käsittelyä määrittävä toimialaohjeisto
SBOM	Software Bill of Materials, lista ohjelmiston toteuttamiseen käytetyistä ohjelmistokirjastoista ja komponenteista
SDLC	Software Development Life Cycle, ohjelmistokehityksen vaiheita kuvaava elinkaarimalli
Tietoturvallisuus	Organisaation tietoja eri uhilta suojaava toiminta
VAHTI	Digi- ja väestötietoviraston johtama julkisen ja valtionhallinnon digitaalista turvallisuutta kehittävä toiminto.

2 Yhteenveto: ohjelmistotuotannon turvallisuuden tila Suomessa 2023

"Tilanne on hyvin hallinnassa, mutta tähän ei pidä tuudittautua. Ala on jatkuvassa murroksessa ja kehityksessä"

- Suomessa ollaan tietoisia ohjelmistoturvallisuuden merkityksestä.
- Osaamisen ja hyvien käytänteiden jalkauttamisessa on kuitenkin vajetta: osalla organisaatioista on osaamista, toisilla ei.
- Asiakkaat ja yritysjohto ovat alkaneet vaatia ohjelmistoturvallisuutta.

Tässä raportissa ohjelmistoturvallisuus on jaettu useaan osa-alueeseen. Aihetta on arvioitu organisaation johdon, keskijohdon ja varsinaisen ohjelmatyön tekijöiden näkökulmasta. Lisäksi on tarkasteltu ohjelmistohankintojen näkökulmaa ja alan koulutusta. Lukijan on syytä pitää mielessä, että ohjelmiston toteuttajien tai hankkijoiden toimintamahdollisuudet riippuvat organisaation toimintatavoista ja resursseista, jotka puolestaan riippuvat organisaation johdon päätöksistä. Raportin perusteella tullaan myös laatimaan toimenpideohjelma, jolla pyritään nostamaan ohjelmistoturvallisuuden osaamistasoa Suomessa.

"Täällä saat juosta kaikin voimin, jos haluat pysyä paikoillasi. Ja jos haluat päästä eteenpäin toiseen paikkaan, saat juosta kaksin verroin niin kovasti." (Lewis Carroll: Liisan seikkailut peilimaailmassa)

Keskeinen havainto ohjelmistotyöstä on jatkuva muutos. Ohjelmistotyötä ohjaavien menetelmien ja prosessimallien kehitykset ovat muuttaneet työn luonnetta. Kehitystyön automaattitestaus ja jatkuva tuotantoonvienti (*continuous delivery*), ketterät (*agile*) menetelmät vaatimustenhallintajärjestelmineen ja mikropalveluarkkitehtuuria tukevat kontit ja pilvipalvelut ovat suuri ero vuosikymmenen tai kahden takaiseen maailmaan. Muutos tulee jatkumaan, uusimmat muutosvaikuttajat ovat tekoäly ja suuret kielimallit, joiden vaikutusten merkittävyydestä ollaan varmoja, vaikka vielä ei osata ennustaa minkälaisia ne tulevat olemaan.

IT-teknologian merkitys yritysten toiminnalle ja sen jatkuvuudelle on kasvanut, ja tämä on huomioitava myös liikkeenjohdon tasolla. Ohjelmistoturvallisuus voidaan leipoa johdon tuella organisaation toimintatapoihin. Silloin se on toiminnan ohessa toteutuva ominaisuus, joka ei edellytä suuria resursseja, kun kaikki osallistuvat omalta osaltansa sen toteutumiseen.

Turvallisuuden taso ohjelmistotyössä on noussut, mutta tämä muutos ei ole yhtä selkeä eikä ole lyönyt läpi alan samalla vauhdilla kuin muut teknologia- ja toimintatapamuutokset. Viime vuosina on kuitenkin ollut havaittavissa kehityspainetta yritysten johdon taholta, minkä myötä kyberturvallisuuteen kiinnitetään enemmän huomiota. Tämä heijastuu luonnollisesti myös ohjelmistotyöhön ja hankintoihin. Osaamisessa ja toimintamalleissa on edelleen kehittämisen varaa: aiemmin turvallisuus on ollut usein yksittäisten toimijoiden oman aktiivisuuden varassa, jatkossa systemaattisempi ja johdosta lähtevä toimintatapa on tarpeen. Selvitystyössä nousi esille positiivisia muutoksia, kuten ns. "shift left", eli turvatyön lisääminen kehityshankkeen alkuvaiheeseen, esimerkiksi uhkamallinnuksen toteuttamisessa osana palvelusuunnittelua.

3 Ohjelmistoturvallisuuden ulkoiset vaikuttimet

"Kaikki yritykset ovat ATK-yrityksiä."

Ohjelmistojen ja tietojärjestelmien kyberturvallisuus riippuu itse ohjelmistotyön ulkopuolisista tekijöistä. Tyypillisesti organisaation johto ja kulttuuri mahdollistavat tai estävät turvallisuutta. Muitakin vaikuttavia tekijöitä on, esimerkiksi lainsäädäntö ja eri toimialojen kansainvälinen ohjeistus asettavat kasvavissa määrin vaateita ohjelmistoturvallisuuteen.

3.1. Johdon panostus kyberturvallisuuteen

"Tietoturva on johdon strategiassa, miksi se ei toteudu tuotteessa?"

Yhä useamman yrityksen ja organisaation johto tiedostaa IT-palveluiden merkityksen toiminnalle ja etenkin toiminnan jatkuvuudelle. Kyberturvallisuuden perään kysellään johtoryhmätasolta ja jopa yritysten hallituksista. Viime vuosina julkisuudessa esiintyneet kiristysohjelmahyökkäykset ja muut tapahtumat ovat osoittaneet turvallisuuden merkityksen toiminnan jatkuvuudelle ja siten strategisen tason asiaksi. Osa haastatelluista tietoturvallisuushenkilöistä mainitsi toimenkuvaansa kuuluvan "eksistentiaalisten riskien" seuraamisen, tarkoittaen ohjelmistotyöhön liittyviä liiketoimintariskejä, jotka uhkaavat itse yrityksen olemassaoloa (huomattakoon, että kyberturvallisuuspoikkeamat aiheuttavat harvoin yrityksen toiminnan päättymistä, mutta ne ovat usein aiheuttaneet merkittäviä taloudellisia vahinkoja).

Kyselyssä 72 % johtotehtävissä olevista luokitteli kyberturvallisuuden keskeiseksi seurattavaksi toiminnoksi. Kuitenkin, asetettaessa organisaation toimintoja tärkeysjärjestykseen, liikevaihto, kassavirta ja henkilöstön tyytyväisyys ohittivat kyselyn kyberturvallisuuselementit. Tämän voi katsoa kuvaavan yritystoiminnan realiteetteja.

Keskijohdosta 59 % kuvasi puolestaan ohjelmistoturvallisuuden olevan asia, jota johto edellyttää, mutta jonka toteumista ei valvota. Noin neljännes vastaajista raportoi turvallisuuden vaatimusten olevan määritelty, kun taas 26 % haastatelluista raportoi päinvastaista. 22 % vastaajista kertoi, että uhat ja jäännösriskit on esiteltävä johdolle.

Tulevaisuuden tarve

Yritysjohdon ymmärrys kyberturvallisuuden arvosta yrityksen arvon suojaajana edistää myös ohjelmistotyön turvallisuutta. Kyberturvallisuus ja ohjelmistotyön investoinnit, etenkin ylläpitoinvestoinnit, kilpailevat resursseista muiden toimintojen kanssa. Ohjelmistotyön turvallisuuden merkitystä organisaatioiden johdolle voidaan edistää tiedotuskampanjalla, joka korostaa turvallisuuden merkitystä arvon säilyttäjänä ja jatkuvuuden turvaajana.

3.2. Kyberriskien merkityksen tiedostaminen ja ohjaava vaikutus

"Meillä on puhelin ja lapioita. Mutta kaikki suunnitelmat ovat koneella."

Tietoisuus kyberriskeistä ja niiden mahdollisuuksista aiheuttaa taloudellista vahinkoa ohjaavat yritysten johtoa kehittämään ja resursoimaan turvallisuutta. Tämä ei välttämättä koske kaikkia yrityksiä, mutta haastattelujen ja kyselyn mukaan yrityksissä panostetaan tietoturvaan entistä enemmän ja ennen kaikkea kyberriskejä kohdellaan liiketoimintapäätöksinä. Käytännön työssä tämä näkyy selkeämpänä riskitietoisuutena ja esimerkiksi liiketoimintajohdon valmiutena hyväksyä ohjelmiston turvallisuutta ylläpitävä tai teknistä velkaa poistava kehitystyö, joka ei tuota välitöntä hyötyä tai uutta toiminnallisuutta.

Tulevaisuuden tarve

Viestitään riskien ymmärtämisestä ja hallitsemisestä lähtevää lähestymistapaa kyberturvallisuuteen.

3.3. Tulevat lainsäädännölliset paineet

Sääntely tulee jatkossa pakottamaan alan toimijoita kiinnittämään huomiota kyberturvallisuuteen. EU on tässä merkittävä vaikuttaja. Hiljattain päivitettyä yhteiskunnan kriittisiä (laveasti tulkiten) toimintoja suojaavaa kyberturvallisuusdirektiiviä (NIS2-direktiivi) ja tietoturvallisuutta tuotteille vaativaa kyberkestävyyssäädöstä (CRA, Cyber Resilience Act) tunnetaan vielä huonosti, mutta niistä aletaan olla tietoisia ja niiden vaikutuksesta toimintaan aletaan miettiä. Viisi vuotta voimassa ollut EU:n yleinen tietosuoja-asetus GDPR on jo herättänyt huomaamaan säätelyn olemassaolon ja vaikutuksen toimintaan. Tuleva kyberturvallisuussääntely tulee edellyttämään ohjelmistotoimialalta haavoittuvuusseurantaa, poikkeamien raportointia ja turvallisuusaukkojen korjaamista ohjelmiston koko elinkaaren ajan.

NIS2 velvoittaa organisaatioita sisällyttämään kyberturvallisuusriskit osaksi organisaation riskienhallintaa ja kohdistamaan kattavasti kyberturvallisuuden riskienhallintatoimenpiteitä eri uhkiin ja niistä aiheutuviin riskeihin. Osana riskienhallintaa organisaation tulisi huomioida myös hallussaan olevien viestintäverkkojen ja tietojärjestelmien häiriöiden kokonaisvaikutus. NIS2 tulee edellyttämään kaikki vaaratekijät huomioivaa lähestymistapaa. Esimerkiksi fyysisten riskien ulottuminen tietojärjestelmään tai alihankintaketjujen vaikutukset kyberturvallisuuteen on arvioitava.

CRA tulee koskemaan kaikkia tuotteita, joissa on digitaalinen toiminto ja jotka ovat yhdistettävissä Internetiin joko suoraan tai toisen laitteen välityksellä. Käytännössä tämä kattaa liki kaikki ohjelmistot, pois lukien selainpohjaiset palvelut, joihin kohdistuu NIS2-sääntely. CRA asettaa tietoturvavaatimusten lisäksi velvoitteen hallita haavoittuvuuksia tuotteen koko elinkaaren ajan.

Tulevaisuuden tarve

Lainsäädäntö voi toimia kyberturvallisuutta edistävänä pakotteena, mutta myös yhteiset pelisäännöt asettavana positiivisena vaikutuksena. Haastatteluissa ei ilmennyt vastarintaa itse lainsäädäntöä kohtaan, mutta toivottiin käytännönläheistä ohjeistusta sen toteuttamiseen.

3.4. Toimialojen itsesääntely ja vakuutusten vaikutus

"Vakuutus auttaa hinnoittelemaan tietoturvan."

Osa turvallisuusohjeistuksesta ja -standardeista on syntynyt toimialakohtaisesta tarpeesta. Tunnetuin esimerkki itsesääntelystä lienee maksukorttialan PCI-DSS-standardi, joka ohjeistaa yksityiskohtaisesti maksukorttitietojen käsittelyn tietojärjestelmissä. Myös energia-ala ja merenkulku ovat luoneet ja luomassa omia tietoturvaohjeistojaan.

Myös vakuutusala on aikojen saatossa ohjannut eri alojen turvallisuuden parantamista. Klassisin esimerkki lienee laivanvarustus, jolle vakuutusyhtiöt alkoivat asettaa turvallisuusvaatimuksia vakuutuksen saannin edellytykseksi jo 1800-luvulla. Kybervakuutuksia on olemassa, mutta niiden tarjonta on hajanaista. Selvitystyössä ei tutkittu vakuutusalaa tarkemmin, mutta haastatteluissa nousi esille, että vakuutusalan yrityksillä on erilaisia vaatimuslistoja, jotka vaikuttavat kybervakuutusten hinnoitteluun. Alalle ei ole kuitenkaan vielä syntynyt yhtenäistä kriteeristöä.

Tulevaisuuden tarve

Eri toimialojen jo käynnissä olevia hankkeita voidaan tukea. Toimialoja tulisi myös kannustaa yhteistyöhön, tarpeet ja ratkaisut ovat useimmilla toimialoilla samankaltaisia, jolloin kaikki hyötyisivät parhaiden käytäntöjen keräämisestä ja yhtenäistämisestä. Eri toimialojen erityispiirteet voidaan huomioida esimerkiksi toimialakohtaisilla ohjeilla. Mikäli eri alojen säännöksiä saataisiin harmonisoitua, helpottaisi se ohjelmisto- ja kyberturvallisuustoimittajien mahdollisuuksia tarjota palveluita eri toimialoille.

Vakuutustoiminnalla on potentiaalia asettaa lainsäädäntöä vastaavia mutta sitä joustavampia vaatimuksia ja vaikuttaa siten kyberturvallisuuteen myös ohjelmistotyössä.

3.5. Asiakkaiden vaikutus

"Me ei haluta olla se, jonka kautta mennään muiden järjestelmiin."

Haastatteluissa nousi esille vastaajien tietoisuus omasta asemastaan alihankintaketjussa ja tarve nostaa oman turvallisuutensa tasoa hankinnoissa ja kehityksessä muiden suojaamiseksi.

Tulevaisuuden tarve

"Heikoin lenkki" on viestinnässä käyttökelpoinen metafora korostamaan kollektiivista vastuuta kyberturvallisuudesta. Tämä voidaan myös kääntää muotoon "ole vahva lenkki".

3.6. Turvallisuustoiminnon asema organisaatiossa ja rooli ohjelmistotyössä

"Turvatiimi on department of yes. Tarjoaa ratkaisuja."

Turvallisuus tai tietoturvallisuus on usein sijoitettu organisaation esikuntatoiminnoksi, jolla ei ole suoraa määräysvaltaa itse toimintaan. Tämä ei ole välttämättä ongelma, mutta vaikuttaa kuitenkin turvallisuuden asemaan ohjelmistotuotannossa. Muutama haastateltava reflektoi aiempia kokemuksiaan ohjelmistokehityksestä, jossa turvallisuus tulee mukaan kuvioon esimerkiksi hyväksymistestauksessa tai auditoinnissa, josta käydään hakemassa "korjauslista". Kaikille ohjelmistotyötä tunteville on sangen selvää, että tällaisella toimintatavalla ohjelmiston turvallisuus jää pinnalliseksi eikä ohjelmistolle synny turvallisuutta tukevaa arkkitehtuuria.

Mahdollistava tietoturva tuntui olevan tietoturvaa tekevien tavoitteena, ja useampikin vastaaja korosti tietoturvasta vastaavan yksikön pyrkivän aktiivisesti olemaan positiivinen kokemus muulle organisaatiolle. Ehdottomien kieltojen ja rajoitusten sijaan tavoitteena oli jakaa osaamista ja auttaa muita näkemään turvallisuuden merkitys organisaation toiminnalle, ja siten saada turvallisuuden tasoa nostettua omaehtoisesti. Tietoturvan vaatimuksia lähestytään ratkaisukeskeisesti ja turva-asiantuntijat pyrkivät löytämään tapoja täyttää liiketoiminnan tarpeet turvallisesti.

Johtoryhmätasolta kysyttiin kyberriskien arvioinnista liiketoiminnassa. Vastaajista 40 % näki niiden olevan pakollinen osa prosessia ja 45 % totesi niitä arvioitavan tarvittaessa. Kysely ei luodannut johdon kykyä arvioida riskejä, mutta osoittaa, että niistä ollaan tietoisia ja niihin kiinnitetään huomiota.

Keskijohdon kyselyvastauksissa puolestaan 59 % ilmoitti, että turvallisuutta odotetaan, mutta ei valvota ja 26 %, että vaatimuksia ei ole määritelty. Lisäksi yli 90 % keskijohdon vastaajista ilmoitti, ettei kyberturvallisuus ole mukana tulostavoitteissa tai palkitsemismallissa. Tämä saattaa johtua kyberturvallisuuden mittaamisen vaikeudesta, mutta myös kertoa sen alhaisesta prioriteetista. Kyselyssä osa vastaajista toi esille tuen ja osaamisen puutetta organisaatiossa ja olevansa omillansa asian kanssa. Myös haastatteluissa muutama kehittäjä toivoi jonkinlaista oman organisaation ylittävää foorumia kokemusten vaihtoon ja osaamisen kehittämiseen.

Tulevaisuuden tarve

Organisaation turvallisuuden johtaminen ja hallinta ovat tietenkin olennainen asia, mutta selvitystyö ei löytänyt mitään yksittäistä parasta toteutustapaa. Viestinnässä on syytä tuoda esille, että tämän voi järjestää usealla tavalla ja organisaation on löydettävä itsellensä sopivin ratkaisu.

Vertaistukea ja tiedonvaihtoa edistävä viestintäkanava olisi hyödyllinen.

3.7. Vastuu ja valta toteuttaa

"Tietoturvatiimillä ei pidä olla käskyvaltaa – miksi ottaa vastuuta, jota ei voi resursoida?"

"Vastuu on toteuttajalla."

Vastuu tieto- ja kyberturvallisuuden toteutumisesta on ollut perinteisesti jonkin verran kuuma peruna, jonka lopullinen pitelijä on usein jäänyt määrittelemättä. Organisaation esikuntaan sijoittuvalla turvallisuustoimella on ollut nimellinen vastuu, mutta liiketoiminta on pystynyt tästä huolimatta tekemään itsenäisesti turvallisuuteen vaikuttavia päätöksiä. Vastuu edellyttää myös toimivaltaa, joka ohjelmistoturvallisuuden kohdalla ilmenee etenkin veto-oikeutena hankintoihin ja ohjelmistototeutuksiin.

Valta voi olla muodolliseen asemaan perustuvaa käskyvaltaa, pehmeämpää vaikutusvaltaa tai monimuotoisempi kokonaisuus.

Keskeisin teema ohjelmistoturvallisuudessa on riskien omistajuus. Jos erillinen turvallisuustoimi vastaa riskeistä, sillä on oltava määräysvaltaa riskien rajaamiseen. Jos liiketoiminta vastaa riskeistä, sillä on oltava ymmärrys riskien vaikutuksesta. Lopullinen vastuu riskeistä on aina organisaation johdolla ja yrityksen omistajilla.

Jos organisaatiossa on turvallisuudesta vastaava yksikkö, se voi toimia määräävässä tai tukevassa roolissa riippuen siitä, miten turvallisuuden hallinta ja riskien omistajuus on määritelty. Mikäli hankinnoista ja ohjelmistotyöstä vastaavat tahot ymmärtävät omistavansa myös riskit ja ottavat konkreettisen vastuun niistä, turvallisuustoimi voi ottaa tukevan asiantuntijaroolin. Koska oletettavasti kaikilla organisaatiossa on melko yhteisenä tavoitteena organisaation tehtävän toteuttaminen, tämä itsessään ei sisällä ristiriitaa.

Mikäli vastuu turvallisuudesta hajautuu organisaation osille ja esimerkiksi autonomisille ohjelmistotiimeille, on jonkinasteinen koordinointi tarpeen. Eräs esille tullut mahdollisuus on sijoittaa tiimiin toimijoita, jotka raportoivat turvallisuustoiminnolle ja ovat turvallisuustoiminnon ohjauksessa oleva resurssi.

Selvitystyössä tuli selväksi, että vastuut ja turvallisuuden organisointi ovat muutoksessa oleva osa-alue, josta ei ole yhtenäistä käytäntöä. Erityisesti ohjelmistotyön siirtymä kohti DevOps-ajattelua ja itsenäisiä tiimejä vaikuttaa muutokseen tilanteessa.

Tulevaisuuden tarve

Toimivalta ja vastuu toiminnan seurauksista ovat välttämättömiä edellytyksiä kaikkien organisaatioiden toimintakyvylle. Ohjelmistoturvallisuutta edistävässä viestinnässä voidaan tuoda esille, että valta ja vastuu kyberturvallisuudesta on

määriteltävä yksiselitteisesti, ellei haluta purjehtia karikkoisilla vesillä vailla merikorttia. Ratkaisuja voi olla useita, mutta niiden niiden kaikkien lähtökohdat ovat seuraavat:

- Yrityksen tai organisaation omistaja vastaa kaikesta.
- Turvallisuuspäätökset ovat liiketoimintapäätöksiä ja liiketoiminnan omistajalla on vastuu niistä.
- Tekemistä voi ulkoistaa, vastuuta ei
- Ohjelmistoturvallisuuden yhteydessä olennainen osa valtaa on kyky sanoa ”Ei”: jos toimija ei voi estää turvatonta toteutusta, hänellä ei ole valtaa.

3.8. Organisaatiorakenteen merkitys turvallisuudelle

Haastatteluissa useampikin tietoturvasta vastaava pohti ohjelmistotekniikan merkitystä organisaatiolle ja sen liiketoiminnalle sekä itse organisaation rakenteen muokkaamista tietotekniikan tarpeiden mukaisesti, esimerkiksi perinteisen IT-osaston hajauttamisena tai jopa organisaation rakenteen muokkaamisen vastaamaan IP-palvelurakennetta, jossa alijärjestelmiä toteuttavat tiimit olisivat liiketoimintayksikköjä. IT-keskeiset liiketoimintayksiköt toisivat ohjelmistotyön lähemmäksi liiketoimintaa ja tämä tarjoaisi mahdollisuuksia turvallisuuden jalkauttamiselle yksiköihin.

Tulevaisuuden tarve

Organisaatiorakenteen mukauttaminen IT-palvelurakenteen mukaiseksi on radikaali idea, jota tuskin kannattaa edistää sellaisenaan. Aihe on syytä tuoda esille ajatuksia herättävänä mahdollisuutena, yhdistettynä muuhun viestintään, jossa korostetaan tarvetta arvioida IT:n ja sen turvallisuuden merkitystä muuttuvassa maailmankuvassa.

4 Ohjelmistotyötä ohjaavat prosessit ja viitekehykset

Kyberturvallisuus on osa ohjelmistotyötä, ei itsenäinen kokonaisuus. Siksi turvallisuuden toteutuminen riippuu erittäin paljon ohjelmistotyön muusta toiminnasta ja siitä, miten organisaatio organisoi ohjelmistotyön.

4.1. Ohjelmistotyön metodiikat: vesiputous, ketterä vai jotain muuta?

"Tilaajat eivät tiedä mitä halutaan. Kun ei osata kuvailla tarpeita, lopputulosta on mahdotonta ennustaa."

Ohjelmistoala itsessään on jatkuvan muutoksen tilassa. Toteutusteknologioiden lisäksi murroksessa ovat myös tekemisen tavat ja menetelmät. Eriytetty kehitys–hyväksymistestaus–tuotanto -kehitysprosessi on muuttumassa ketterämmäksi ja integroidummaksi DevOps-tyyliseksi toimintamalliksi, jossa testaus ja tuotantoonvienti automatisoidaan pitkälle ja kehityssyklit nopeutuvat. Ketterä kehitys on ollut jo pidempään muotitermi ja se toteutuu eri tavoin, mutta sen lisäksi useampi haastateltava kertoi organisaationsa siirtyneen itsenäisiin ja moniosaajatiimeihin, joilla on kokonaisvastuu omasta osa-alueestaan. Nämä osa-alueet saattavat olla yksittäisen asiakkaan ohjelmistotarpeita tai rajapintojen määrittämiä kokonaisen järjestelmän alijärjestelmiä.

Tulevaisuuden tarve

Viestinnässä on syytä huomioida, että organisaatioiden tai jopa organisaation osien erilaiset toimintatavat vaikeuttavat kaikille sopivien ohjeistusten laatimista. Ohjeistusta voidaan kohdistaa tai esittää hyväksi havaittujen käytäntöjäen muodossa, tuoden myös toimintaympäristön esille.

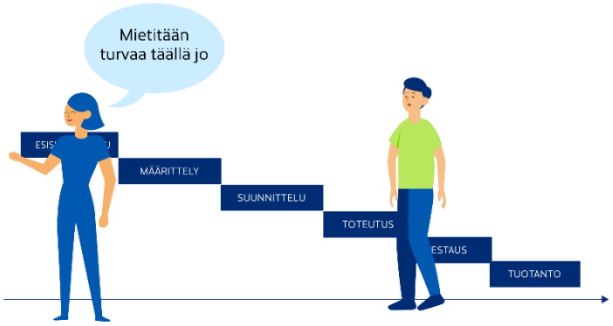
4.2. Kyberturvallisuus ohjelmistosuunnittelussa ja "shift left"

"Shift left on jo historiaa – Shift everywhere""

Vaikka ohjelmistoja kehitetään usein ketterästi lisäten ominaisuuksia asiakastarpeen mukaan, ohjelmiston rakenteen määrittää sen arkkitehtuuri – ja arkkitehtuuripäätökset tehdään kehityksen alkuvaiheessa. Arkkitehtuurin muuttaminen jälkikäteen on mahdollista, mutta yleensä työlästä. Erityisesti iteratiivisen tai ketterän kehityksen ongelma on usein siinä, että kehitys aloitetaan keskeisen toiminnallisuuden toteuttamisesta pohtimatta turvallisuuden tarpeita. Kehitystyö alkaa usein toteuttamiskelpoisuuden osoittamisesta (*Proof of Concept*), tai vähimmät tavoitteet täyttävästä myytävästä tuotteesta (*Minimum Viable Product*). Tällöin jatkokehityksessä esimerkiksi käyttäjien tietosuojan hallinta ohjelmiston sisällä saattaa osoittautua vaikeaksi lisätä valmiiseen arkkitehtuuriin.

Jotta arkkitehtuuri tukisi kyberturvallisuutta ohjelmiston koko elinkaaren ajan, olisi turvallisuuden tarpeet huomioitava jo suunnittelun alkuvaiheessa ohjelmiston

vaatimusmäärittelyssä. Tällöin ohjelmistoon voidaan alusta alkaen suunnitella esimerkiksi tehtävien tai tietoaineiston eriyttämistä, kerroksisuutta, sekä edellisiä tukeva oikeuksien hallintajärjestelmä. Tällaisten perustavanlaatuisten toiminnallisuuksien toteuttaminen myöhemmin on vaikeaa tai jopa mahdotonta.



Selvitystyössä ilmeni, että turvallisuuden huomiointi ohjelmistotyössä on siirtymässä entistä aikaisempaan kehitysvaiheeseen, ns. "shift left" projektimallissa, mutta ei läheskään aina.

Kyselyssä 24 % tuoteomistajista ja projektipäälliköistä ilmoitti turvan huomioimisen kehityshankkeessa alkavan jo esiselvitysvaiheessa, 36 % määrittelyvaiheessa ja 16 % jokaisessa kohdassa kehitystä. Vain 4 % raportoi, että turvallisuutta ei huomioida ja toiset 4 % turvallisuuden tapahtuvan kehityksen loppuvaiheessa.

Kehittäjistä 24 % raportoi myös tietoturvan alkavan esiselvityksessä ja toiset 24 % määrittelyvaiheessa. Alkuvaiheessa toteutusta tietoturvan huomioi 19 %, mutta 14% loppuhyväksynnässä ja 5% toteutuksen loppuvaiheessa. Vastaajista 5% raportoi, ettei turvallisuutta huomioida kehityksessä. Tämä ei kuitenkaan vielä kerro, kuinka syvällisesti turvallisuuden tarpeita otetaan huomioon eri vaiheissa.

Tulevaisuuden tarve

Ohjelmistoturvallisuuden tasoa voitaisiin parantaa huomattavasti suhteellisen vähällä vaivalla, jos tietoturvallisuus otettaisiin huomioon nykyistä aikaisemmassa kehitysvaiheessa, yleensä jo esisuunnittelussa. Tavoitetta voidaan edistää esimerkiksi kohdistamalla eri toimialoille käytännön esimerkkeihin perustuvaa viestintää, turvallisuus saamisesta jo alkuvaiheessa mukaan ohjelmistoarkkitehtuuriin tai hankinnan vaatimuksiin. Varsinainen IT-alan lisäksi on syytä huomioida perinteisemmät toimialat, joille kyberturvallisuus on uudempi osaamisalue.

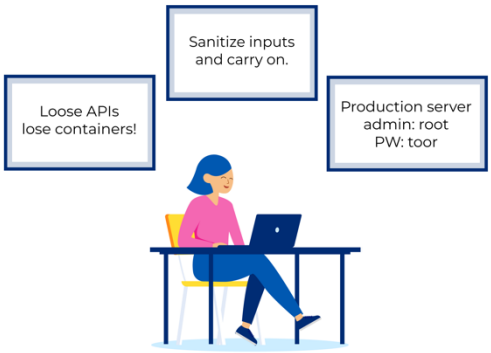
4.3. Ohjelmistokehitystä ohjaavat mallit

Ohjelmistokehitykselle on olemassa erilaisia toimintamalleja, kuten SDLC (*Software Development Life Cycle*) tai SAFe (*Scaled Agile Framework*). Näitä malleja käytetään erityisesti isoissa organisaatioissa ohjaamaan kehitystyötä. Mallit ohjaavat vaatimusten määrittelyä, viestintää, projektinjohtoa ja monia muita kehityksen osa-alueita. Mallien pohjalla on usein jonkin organisaation tai organisaatioiden kokemus heidän tavastaan toteuttaa ohjelmistoja, ja mallit sisältävät siten myös olettamia organisaation ja työn luonteesta. Jotkin mallit saattavat esimerkiksi olettaa, että koko järjestelmä menee kerralla tuotantoon, ja siten painottaa kehitystehtävien koordinaatiota. Toimintamalleja ja standardeja on kuvattu liitteessä 2.

Kyselyssä tietoturvallisuuden hallintajärjestelmästandardi ISO 27001 nousi esille itse organisaation kyberturvallisuutta ohjaavana mallina 65 %:n osuudella

vastauksista. Sen lisäksi käytössä ovat valtionhallinnon VAHTI-ohjeet, Katakri, Kybermittari ja NIST CSF.

Ohjelmistotyön ja -hankintojen turvallisuutta edustavista malleista 69 % vastaajista kertoi käytössä olevan talon sisäisen ohjeistuksen. Lisäksi OWASPin (*Open Worldwide Application Security Project*) ohjeistus oli käytössä noin puolella vastaajista. Yleisimmät ohjelmiston kehitysvirheet kokoava *Top 10 Web Application Security Risks* lienee tunnetuin OWASP-ohje, mutta vastauksissa mainittiin myös ASVS ja SAMM. Muitakin malleja on käytössä, kuten teollisuuden kyberturvastandardi IEC 62443. DevSecOps-toimintamallia noudatti 42 % vastaajista ja Secure Software Development Lifecycle oli käytössä 29 % vastaajista. Bug Bounty -hankkeita, joissa ulkopuolisille maksetaan ohjelmistohaavoittuvuuksien löytämisestä, oli käytössä 16 %:lla vastaajista.



Huomattavaa on, että 7 % vastaajista raportoi, että organisaatiolla ei ole käytössä mitään kyberturvallisuutta tukevaa toimintamallia.

Yllä olevat mallit on tarkoitettu eri käyttötarkoituksiin: osa ohjaa organisaation kyberturvallisuutta, osa turvallisuutta ohjelmistokehitysprosessissa ja osa keskittyy ohjelmoinnin yksityiskohtiin, kuten rajapintojen toteutukseen. Mikään yksittäinen malli ei kata organisaation kaikkia turvallisuustarpeita. Organisaatioilla saattaa olla myös käytössä oma dokumentoitu tai implisiittinen malli, joka sisältyy organisaation prosesseihin, toimintatapoihin ja kulttuuriin.

Tulevaisuuden tarve

Tuetaan keskustelua ja kokemusten vaihtoa ohjelmistotyön organisoinnista ja ohjelmistoturvallisuuden toteutumisesta. Levitetään tietoa eri malleista ja niiden soveltuvuudesta eri tarpeisiin.

4.4. Uhkamallinnus

Uhkamallinnus nousi haastatteluissa ja kyselyssä useamman kerran hyödyllisenä kyberturvallisuuden suunnitteluvälineenä. Uhkamallinnuksessa pyritään systemaattisesti löytämään kehitettävään kokonaisuuteen kohdistuvia uhkia ja sitä voidaan toteuttaa kehityksen eri vaiheissa. Osa vastaajista tuntui käsittävän uhkamallinnuksen tekniseksi arvioinniksi, joka kohdistetaan jo suunniteltuun toteutukseen. Toiset esittivät itse suunnittelun alkavan uhkamallinnuksella, jossa pohditaan ensin haluttuun toiminnallisuuteen kohdistuvia uhkia ja vasta sitten aletaan suunnitella järjestelmää, joka pystyy torjumaan näitä uhkia (osa uhista jää jäännösriskiksi). Uhkamallinnus voidaan kohdistaa esiselvitysvaiheessa itse ideaan, palveluun palvelumuotoilussa ja sitten koko tekniseen toteutukseen tai kohdennetusti sen eri osiin.

Uhkamallinnus on kohtuullisen kevyt prosessi verrattuna muuhun kehitystyöhön, ja sen kautta voidaan luoda ymmärrys järjestelmään kohdistuvista uhista niin tilaajille kuin kehittäjillekin. Kun palveluun ja sen toteuttavaan järjestelmään kohdistuvat uhat konkretisoituvat mallinnuksessa selkeiksi uhkakuvauksiksi, kehitystyön osapuolet ymmärtävät paremmin, mitä ovat tekemässä ja miksi.

Kyselyssä uhkamallinnuksen raportoitiin tapahtuvan seuraavissa vaiheissa: esiselvityksessä 6 %, määrittelyssä 17 %, toteutuksen alkuvaiheessa 22 %. Loppuvaihetta painotti 11 % vastaajista ja 28 % kertoi, ettei uhkamallinnusta tehdä.

Koska ohjelmiston turvallisuuden toteuttaminen ilman jonkinlaista käsitystä mahdollisista uhista saattaa jättää toteutukseen erilaisia aukkoja ja puutteita, antaa 28 % vastaajista puuttuva uhkamallinnus aihetta huoleen toimialalla. Kysymys voi olla näkemyseroista tai saman toiminnon kutsumisesta toisella nimellä, mutta myös toimintatavasta, jossa ohjelmistoon kohdistuvia uhkia ei mietitä erikseen, vaan "tehdään turvallista" ilman uhka-analyysiä. Tällöin huolena on, ettei turvaamistoimilla ole selkeää tavoitetta ja toiminnot eivät kohdistu varsinaisiin uhkiin.

Tulevaisuuden tarve

Uhkamallinnus voidaan ottaa helposti osaksi esisuunnittelua ja varsinaista suunnittelua (katso infolaatikko). Tällöin ohjelmistolle määritellään haluttu toiminnallisuus, käyttäytyminen virhetilanteissa ja myös suojautuminen tahalliselta väärinkäytöltä.

Ohjelmistotyön alkuvaiheen uhkamallinnukseen voidaan tarjota yksinkertaisia ohjeita lähtien kysymyksestä ”Mikä voi mennä pieleen?” Viestinnässä kannattaa tuoda esille, että uhkamallinnuksen kohdalla metodiikka on hyödyllistä, mutta tärkeintä on vain alkaa pohtia uhkia ja huomioida ne hankkeessa. Samalla voidaan korostaa eri näkökulmien merkitystä: asiakaspalvelulla, ohjelmistokehittäjällä tai liiketoimintavastaavalla voi olla hyvin erilainen näkemys kokonaisuuteen.

Haastatteluissa nousi esille tarve yksinkertaiselle ja ymmärrettävälle ohjaukselle. Esimerkiksi tarpeen uhkamallinnukselle voi konkretisoida tarpeeksi toteuttaa ohjelmisto, joka selviää seuraavan tyyppisistä tapauksista:

- *Happy Case* – asiakas käyttää palvelua kännykällä suunnitellusti.
- *Unhappy Case* – Asiakas pudottaa kännykkänsä vessanpönttöön, eikä muista millä tunnuksella tai salasanalla on aktivoinut palvelunsa.

- *Evil Case* – Kännykkäsovellus takaisinmallinnetaan ja muokataan toimimaan aivan, kuten ei ole suunniteltu.

Kolme erityyppistä käyttötapausta on helppo pitää mielessä, ja ne ovat relevantteja vaatimuksia turvalliselle ohjelmistolle ja ohjaavat näkemään, että pelkkä "*Happy Case*" ei ole riittävä pohja suunnittelulle.

4.5. Liiketoiminnan kyky tunnistaa uhkapotentiaali

> *"Mikään turvaorganisaatio ei pysy toiminnassa mukana, jos turvallisuus ei ole mukana liiketoiminnassa."*

Yleisen näkemyksen mukaan liiketoiminnan ja ohjelmistojen toteuttajien maailmankuva on perustavanlaatuisesti erilainen. Tämä ei välttämättä pidä aina paikkaansa, mutta yleistys ei liene täysin perätönkään - osaamisalueissa on eroa. Ohjelmistotyössä erot ilmenevät usein puutteina kommunikoinnissa, esimerkiksi kun liiketoiminnan koettua tarvetta kuvannetaan ohjelmistototeutukseksi. Kommunikaatiovaikeudet heijastuvat myös ohjelmistoturvallisuuteen.

Näkemyserot ja kommunikaatioongelmat konkretisoituvat usein riskienhallinnan yhteydessä, etenkin jäännösriskejä hyväksyttäessä. Ohjelmistojen toteuttajat eivät välttämättä ymmärrä riskien merkitystä liiketoiminnalle (esim. asiakastyytyväisyys) ja vastaavasti liiketoiminnan edustajat eivät välttämättä pysty havaitsemaan järjestelmän eri riippuvuuksien vaikutusta asiakkaan saamaan palveluun.

Haastatteluissa nousi esille tuoteomistajan rooli ymmärryksen välittäjänä. Tuoteomistajilla on tyypillisesti toimialaosaamista molemmilta osa-alueilta, ja he pystyvät arvioimaan ohjelmistoa myös osana toimintaympäristöään.

Tulevaisuuden tarve

Tarve ymmärtää teknisten riskien liiketoimintamerkitys on todellinen. Tätä tarvetta ratkotaan tai ollaan ratkomatta eri organisaatioissa eri tavoin.

Ohjelmistoturvallisuuden viestinnässä voidaan pyrkiä tuomaan esille, että kaikki riskit ovat lopulta liiketoimintariskejä ja että riskienhallinnan on huomioitava ohjelmistoturvallisuus osana kokonaisturvallisuutta.

4.6. Organisaation ohjelmisto-osaamisen ylläpitäminen ja seuranta

Muuttuvalla toimialalla osaaminen ja sen ylläpito on keskeistä. Käytännössä kaikkien ohjelmistotyötä tekevien on kehitettävä osaamistaan jatkuvasti työn ohessa. Tämä heijastuu myös rekrytointiin: ammattilaiset edellyttävät työnantajaltaan mahdollisuutta oppia uutta jokaisessa projektissa. Organisaatioilla on aiheellista olla henkilöstön kehitysohjelma, joka ottaa huomioon myös ohjelmistoturvallisuuden osaamisen.

Tässä yhteydessä on huomioitava alalla hyvin yleinen alihankintatoimi, minkä vuoksi ohjelmistoa toteuttavat henkilöt eivät välttämättä ole omaa henkilöstöä. Tilaajan ja toimittajan välinen organisaatioraja voi aiheuttaa ongelmia toiminnalle tai osaamisvajetta molempiin suuntiin. Tilaaja saattaa olettaa toteuttajilla olevan myös turvallisuusosaamista varmistamatta onko näin, tai vastaavasti tilaaja ei osaa hyödyntää tarjoilla olevaa osaamista. Alihankkijan henkilöstö ei myöskään yleensä pääse osallistumaan asiakkaan omalle henkilöstölleen järjestämään koulutukseen, vaikka toimisi muutoin organisaation puitteissa.

Rakenteellinen, koko ohjelmistoalaa koskeva potentiaalinen ongelma on tarve kokeneille kehittäjille ja asiakkaiden taipumus edellyttää senioriteettia alihankinnassa. Pahimmillaan tämä voi johtaa tilanteeseen, jossa tulevan sukupolven juniorit eivät työllisty, ja alan työvoimapula vain pahenee. Ohjelmistojen turvallisen toteuttamisen katsotaan yleensä edellyttävän kokemusta ja kykyä tasapainottaa turvallisuutta suhteessa muihin vaatimuksiin. Juniorikehittäjillä tämä osaaminen karttuu vain konkreettisen kehitystyön myötä.

Tulevaisuuden tarve

Tuodaan esille ajantasaisen osaamisen ja jatkuvan oppimisen merkitystä ohjelmistoalla yleisesti ja erityisesti ohjelmistoturvallisuuden kohdalla. Edistetään organisaation sisäisiä toimintamalleja, kuten:

- Rekrytoinnissa kiinnitetään huomiota ohjelmistoturvallisuuden osaamiseen
- Pidetään koodikatselmointeja, jotka mahdollistavat keskustelun turvallisuudesta ja osaamisen jakamisen
- Hyödynnetään eri projekteissa organisaatiosta usein löytyviä kehittäjiä, jotka ovat omatoimisesti kiinnostuneita ohjelmistoturvallisuudesta.
- Pidetään hankkeen alkuvaiheessa uhkamallinnussessioita, jotka auttavat ymmärtämään turvallisuuden tarvetta. Tässä yhteydessä tuotiin esille, että varsinaisten kehittäjien lisäksi uhkamallinnuksessa on hyvä hyödyntää ulkopuolista näkemystä, kuten eri käyttäjäryhmiä, naapuritiimejä tai liiketoiminnan edustajia
- Hyödynnetään turvallisuusvalmentajan roolia. Tällainen valmentaja ("security champion") voi olla osana kehitysorganisaatiota tai turvallisuustoimintoa.

5 Varsinainen ohjelmistotyö

Tässä osiossa katselemme ohjelmistotyön turvallisuutta kehittäjien näkökulmasta.

5.1. Kyberturvallisuusosaamisen merkitys ohjelmistotyössä

> *"On vaikea tietää mitä pitäisi tietää, jos et tiedä mitä pitäisi tietää"*

Useampi haastateltava toi esille osaamispuutteen. Ohjelmistoturvallisuus ei ole useinkaan ollut osa ohjelmistotyön opetusta tai välttämättä edes erillinen opintomoduuli. Takavuosina turvallisuuskysymykset jäivät opetuksessa lähes täysin huomiotta. Tämän vuoksi osaamista ei ole aina käytettävissä, vaikka kiinnostus turvallisuuteen on kasvamassa,.

Käytettyjä ratkaisumalleja kehittäjien osaamispuutteeseen ovat mm.:

- Turvatiimin tukipalvelut
- Innostuneen henkilöstön hyödyntäminen
- Moniosaajatiimit, joissa on mukana myös turva-asiantuntija
- Turvallisuutta edistävät ohjelmistokehityksen yleiset vaatimukset
- Uhkamallinnus kehityksen alussa ja muutosten aikana sekä turvallisuustarpeiden määritteleminen hankekohtaisiin vaatimuksiin
- Tarkistuslistat (esim. OWASP Top 10)
- Turvatestaus tai -auditointi tuottamassa vaatimus- tai korjauslistan ennen tuotantoon pääsyä.

Kyselyn mukaan noin 40 % kehittäjistä saa tukea organisaation kehitystä ohjaavista prosessista ja 50 % muuta tukea ja koulutusta organisaatioltaan. Samaan aikaan 20 % kokee olevansa omillaan ja tarvitsevansa tukea. Myös 50 % kokee myös olevansa omillaan, mutta osaavansa. Väitteeseen "Saan tietoa parhaimmista käytännöistä kavereilta vapaa-ajalla" vastasi 29 % myöntävästi ja 57 % ilmoitti etsivänsä tietoa verkosta.

Tulevaisuuden tarve

Oppilaitosten toimintaa tarkastellaan jäljempänä.

Osaamisen ongelmat lienevät enimmäkseen siinä, että organisaatioiden resurssit ja osaaminen ovat rajallisia, mutta kyberturvallisuustarpeet vaihtelevat. Tulevina vuosikymmeninä organisaatioiden on aiheellista varautua kehittämään itse osaamistaan oman koulutuksen ja rekrytoinnin kautta. Tavoite tulisi viestiä eri organisaatioille ja kannustaa niitä omatoimisuuteen osaamisen kehittämisessä.

Ala hyötyisi turvallisuutta edistävien toimien kehityspolusta, jonka avulla organisaatio voisi asteittaan nostaa omaa kypsyystasoaan. Esimerkiksi aluksi otettaisiin käyttöön OWASP Top 10 -lista kehittäjille ja epämuodollinen uhkamallinnus suunnittelijoille ja arkkitehdeille. Tämä nostaisi välittömästi tasoa nollasta, minkä jälkeen systemaattisempia menetelmiä voidaan ottaa käyttöön vähitellen.

5.2. Ohjelmistokehykset ja -kirjastot

"Kehittäjän tulisi suosia valmiiden ratkaisujen käyttöä omien sijaan."

Ohjelmistoja ei nykyisin kehitetä avaamalla tyhjä tiedosto editoriin, vaan useimmissa tilanteissa kehittäjän tarpeisiin vastaa paremmin sopiva ohjelmistokehys (*framework*). Kehys on ohjelmistopaketti, joka sisältää suuren määrän tarvittavaa yleiskäyttöistä toiminnallisuutta, kuten WWW-istuntojen hallinnan, tietokantarajapinnan, palvelupyyntöjen työjonon jne. Näitä kokonaisuuksia on saatavina kaupallisina tuotteina, mutta avoimen lähdekoodin Open Source -yhteisö tarjoaa myös useita maksuttomia korkealaatuisia ohjelmistokehyksiä.

Koska ohjelmistokehyksien kehittäjät pyrkivät saamaan tuotteensa käyttöön, he tekevät niiden käyttöönotosta mahdollisimman helppoa. Tarjotut esimerkkikoodit ovat mahdollisimman yksinkertaisia ja helposti ymmärrettäviä, ja oletusasetukset edistävät käyttöönottoa. Tietoturvaominaisuudet ovat oletusarvoisesti pois päältä käyttöönoton helpottamiseksi. Tämä aiheuttaa sen, että ohjelmistoja kehitetään usein kehyksen tarjoaman esimerkkikoodin pohjalta. Tällöin kehitettävä ohjelmisto on jo lähtökohtaisesti turvaton, koska esimerkkikoodi ei sisällä esimerkiksi identiteetin- ja oikeushallintaa.

Alalla puhutaan tyypillisesti käyttöjärjestelmien ja ohjelmistojen "kovennuksesta" (*hardening*), jossa poistetaan käytöstä kohteen toiminnan kannalta turhia ominaisuuksia ja siten myös suljetaan potentiaalisia turva-aukkoja. Aivan yhtä hyvin ohjelmistotuotteet voisivat olla turvallisia oletusarvoisesti ("*Secure by Default*" -suunnitteluperiaate), jolloin vain tarvittavat toiminnallisuudet otetaan käyttöön asennuksen jälkeen.

Tulevaisuuden tarve

Pyritään vaikuttamaan avoimen lähdekoodin yhteisöön niin, että ohjelmistokehyksien turvaominaisuudet otettaisiin oletusarvoisesti käyttöön ja myös mukaan esimerkkiohjelmiin. Nykyisessä ilmapiirissä tämä muutos ei ole mahdoton tavoite, mutta se vaatii kulttuurinmuutosta kehittäjäyhteisöissä, niin vapaaehtoistyössä kuin kaupallisten toimijoidenkin parissa.

Tuodaan esille ohjelmistokehyksen valinnan merkitys jo ohjelmistokehityksen alkuvaiheessa ohjelmistonkehitysmetodiikasta riippumatta. Ketteräkin kehitys edellyttää tiettyjä alkuoletuksia, jotka tulevat vaikuttamaan turvallisuuteen ja joiden muuttaminen jälkikäteen on työlästä.

Pyritään lisäämään ymmärrystä copy-paste-koodauksen vaaroista; ohjelmakoodin kopioiminen sisältää riskejä, olipa lähteenä sitten käytetyn työkalun ohjeistus, verkon keskustelufoorumit tai keskusteleva tekoäly. Vieraan koodin tuominen osaksi tuotetta arvioimatta ja ymmärtämättä sitä mahdollistaa virheiden lisäksi erilaisia hyökkäyksiä ohjelmistoa vastaan.

5.3. Ohjelmistojen elinkaari ja haavoittuvuusseuranta

"Miksi pitäisi maksaa työstä, jos ei saada uusia featureita?"

Ohjelmistot rakennetaan tyypillisesti useista alikomponenteista, joita kutsutaan yleisesti ohjelmistokirjastoiksi. Etenkin avoimen lähdekoodin ohjelmistot voivat sisältää satoja eri tahojen tuottamia kirjastoja. Ne toteuttavat yksittäisiä tehtäviä, kuten loki-ilmoitusten kirjaamista ohjelman toiminnasta tai ohjelman saaman syötteen tarkastusta. Kuten kaikissa ohjelmissa, näissäkin kirjastoissa on ohjelmointivirheitä. Niitä virheitä, jotka johtavat tietoturvaongelmiin, kutsutaan haavoittuvuuksiksi. Haavoittuvuuksia löydetään eri kirjastoista säännöllisesti ja niistä tiedotetaan eri kanavia pitkin. Osa ohjelmistokirjastojen käyttämisen kustannuksia on näiden tiedotteiden seuraaminen ja oman ohjelmiston päivittäminen käyttämään uusia kirjastoversioita.

Ohjelmistojen modulaarisena rakenteen vuoksi niitä on huollettava ja pidettävä kunnossa valmistumisen jälkeen. Olennainen osa tätä ylläpitoa on seurata haavoittuvuustiedotteita ja arvioida, onko ilmoitettu haavoittuvuus ohjelmiston kannalta olennainen ja vaatiiko se välitöntä paikkausta. Tämän tehtävän helpottamiseksi on olemassa työkaluja, jotka seuraavat tiedotteita ja ilmoittavat haavoittuvuuksista. Seuranta kuitenkin edellyttää, että tiedetään mitä komponentteja ohjelmisto sisältää. Tämän mahdollistaa puolestaan ohjelmiston tuoteselosteen (*Software Bill of Materials*, *SBOM*) ylläpitäminen.

Vaikka komponenteista ei löytyisikään haavoittuvuuksia, ohjelmistokehyksien ja kirjastojen tekijät päivittävät tuotteitaan jatkuvasti. Päivityksissä ei ainoastaan lisätä uutta toiminnallisuutta, vaan myös poistetaan vanhoja toimintoja tai muokataan niitä. Tästä seuraa, että päivityksiä ei voi ajaa sisään sellaisenaan, vaan ainakin suurempien muutosten kohdalla on myös testattava muutosten vaikutuksia omaan ohjelmistokoodiin ja korjattava muutosten mahdollisesti aiheuttamat virheet. Toinen vaihtoehto olisi olla ottamatta toiminnallisuuspäivityksiä käyttöön, mutta tällöin taas turvallisuuspäivityksen käyttöönotto saattaa muuttua työlääksi, jos turvapäivitys tulee vain uusimpiin ohjelmistoversioihin. Usein ohjelmistoprojekteille ei ole resurssisyistäkään mahdollista tarjota päivityksiä vanhoihin ohjelmistoversoihin.

Komponenttien jatkuvasta muutoksesta seuraa tarve pitää ohjelmistoa ajan tasalla, tehdä päivitykset vaikka niistä ei olisi välitöntä hyötyä ja tarvittaessa muokata omaa ohjelmistoa muutosten mukaan. Tämä on työtä, joka ei lisää uutta toiminnallisuutta ohjelmistoon. Kyberturvallisuusnäkökulmasta päivitystyö on kuitenkin välttämätöntä, koska muutoin ajaudutaan ennen pitkää tilanteeseen, jossa turvapäivityksiä ei voida enää ottaa käyttöön silloin, kun ohjelmistokomponenteissa paljastuu haavoittuvuus.

Kyselytutkimuksessa tiedusteltiin ohjelmistojen turvallisuutta elinkaaren ajan. 84 % vastanneista toteuttaa haavoittuvuusseurantaa ja 80 % myös korjaa

haavoittuvuudet liki välittömästi. Noin puolet vastaajista toteuttaa muita seurantatoimenpiteitä. 15 % raportoi, että käytössä olevan ohjelmiston turvallisuutta ei seurata aktiivisesti sen elinkaaren aikana.

Tulevaisuuden tarve

Pyritään kannustamaan toimintamallia, jossa ohjelmistoa ylläpidetään sen elinkaaren ajan ja seurataan haavoittuvuuksia. Edistetään ymmärrystä siitä, että ohjelmisto ei ole koskaan valmis, vaan sitä ylläpidetään ja kehitetään jatkuvasti, kunnes siitä luovutaan joku päivä. Dokumentaatio ja arkkitehtuuri tehdään ohjelmiston elinajaksi ja dokumentaation tarkoitus on mahdollistaa ylläpito ja jatkokehitys uusille toimijoille.

5.4. Dokumentaation merkitys

"99 % koodaamisesta on vanhan läpikäyntiä ja sen muokkaamista."

Ohjelmiston dokumentaatio on tunnetusti pakkopullaa, joka kiinnostaa kehittäjiä vähemmän kuin itse ohjelmiston kehittäminen. Elinkaaren kannalta dokumentaatiolla on kuitenkin suuri merkitys, koska selkeä ja ymmärrettävä dokumentaatio mahdollistaa järjestelmän ymmärtämisen ja kehitystoimenpiteiden toteuttamisen nopeasti ja mielekkäästi, arkkitehtuuria ylläpitäen. Hyvä dokumentaatio helpottaa huomattavasti uusien kehittäjien tuomista ohjelmiston pariin ja mahdollistaa sen ylläpidon.

On useita tapoja dokumentoida ohjelmisto, ohjelmakoodin kommenteista formaaleihin esitystapoihin saakka. Olennaista on ymmärtää, että dokumentaatiolla ei ole itseisarvoa, vaan käyttöarvo ja merkitys ohjelmistoinvestoinnin arvon suojaajana.

Tulevaisuuden tarve

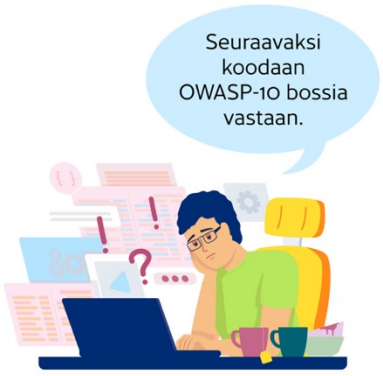
Tuodaan esille dokumentaation merkitystä elinkaarelle ja sen tehtävää ohjelmiston ymmärtämisen mahdollistajana. Koodista näkee mitä ohjelma tekee, dokumentointi kertoo, miksi se tekee mitä tekee ja miten koodi suhtautuu arkkitehtuuriin ja järjestelmän muihin osiin. Dokumentaation tulisi kuvata lukijalle järjestelmän idea, jonka koodi sitten toteuttaa.

5.5. Ohjelmistokehittäjien näkökulma

"Koodaaminen on kivaa, kaikki muu koetaan ylimääräiseksi."

Haastatellut kehittäjät tarjosivat kuvan muuttuvasta toimialasta. Perinteisesti ohjelmistokehityksen fokus on usein ollut itse ohjelmiston toiminnallisuudessa eli toiminnallisissa vaatimuksissa, eikä turvallisuuteen ole välttämättä kiinnitetty huomiota. Eräs haastateltava kuvasi vanhaa toimintamallia kertomalla, kuinka turvallisuuden toteutus alkaa hyväksymistestausvaiheessa, kun ohjelmaa ei saa hyväksytettyä laittamatta turvaa kuntoon. Useampi haasteltu kehittäjä totesi, että

OWASPin Top 10 -ohjeistus (kymmenen yleisintä ohjelmistohaavoittuvuutta) on heidän ohjenuoransa.



CI-putki (*continuous integration pipeline*) on nykyään melko yleinen metodi ohjelmistotuotannossa. Siinä eri kehittäjien työ integroidaan päivittäin toimivaksi versioksi ohjelmistokokonaisuudesta, johon voidaan kohdistaa automaattisia testaustyökaluja. Useampi haastateltava kertoi, että testauspalettiin on liitetty myös erilaisia tietoturvatestaustyökaluja, kuten staattisia koodianalysaattoreita, jotka etsivät mahdollisia turvallisuutta vähentäviä ohjelmistovirheitä.

Aiemmin on ollut tyypillistä, että ohjelmistokehitys ja palveluja näillä ohjelmistoilla toteuttava tuotanto on pidetty selvästi erillään. Tämä on muuttumassa DevOps-mallin myötä, kun ohjelmiston kehittänyt ja sitä ylläpitävä tiimi vastaa myös ohjelmiston toiminnasta tuotannossa. Eri organisaatioissa on kuitenkin tuotannossa eri aikoina luotuja järjestelmiä, jotka on usein tehty oman aikansa parhaalla osaamisella. Ohjelmistoja ylläpitävän kehittäjän maailmankuva saattaakin vaihdella, kuten myös käytössä olevat työkalut esimerkiksi testaukseen ja ongelmien selvittämiseen.

Tulevaisuuden tarve

Pyritään levittämään tietoisuutta ja osaamista parhaista käytännöistä. Parhaat käytännöt elävät ja muuttuvat, minkä vuoksi on oltava aktiivinen vain pysyäkseen ajan tasalla.

Kyselytutkimuksen tulosten ja haastattelujen mukaan kehittäjiltä puuttuvat vertaistukiryhmät tiedon ja parhaiden käytänteiden jakoon. Kannattaa harkita kehittäjien vertaistukiryhmien tukemista tai tarvittaessa jopa sellaisen luomista.

Vertaistukea ja hyvien käytäntöjen jakamista tarvitaan oletettavasti muillekin ohjelmistotyön alueille, kuten riippuvuuksien ja haavoittuvuuksien hallintaan.

5.6. Ohjelmistotyön laatu ja turvallisuus

"Laadukas koodi on myös turvallista"

Turvallisuus aletaan yhä enemmän mieltää ohjelmiston laatuominaisuudeksi. Vaikka turvallisuuteen tarvitaan myös salauksen ja pääsynhallinnan kaltaisia konkreettisia turvallisuusominaisuuksia, a, turvallisuuden nähdään toteutuvan ohjelmistossa kaikkialla, itse koodista arkkitehtuuriin.

Ohjelmointivirheiden välttäminen edistää turvallisuutta, ja se on myös kiinteästi yhteydessä testaukseen ja laatutyöhön. Testaus on perinteisesti mielletty keskeiseksi osaksi ohjelmistotyötä. Turvallisuuden merkitys on noussut nykyiselle tasolleen vasta, kun palveluiden avaaminen Internetiin on laajentanut hyökkäysrajapinnan globaaliksi. Testauksen ja muun laatutyön katsotaan yleensä tuottavan säästöjä, kun mahdolliset virheet saadaan kiinni tuoreeltaan, jolloin niiden korjaaminen on helpompaa. Tässä on mahdollisuus edistää synergiaa laatutyön ja turvallisuuden välillä.

Edellä mainitun automaattitestauksen lisäksi voidaan toteuttaa ihmisvoimin muuta turvatestausta, johon on olemassa useita työkaluja ja toimintamalleja. Testauksen lisäksi toinen yleinen laatua ylläpitävä toimi on koodikatselmointi, jossa ohjelmoija selittää oman työnsä toiselle ohjelmoijalle tai koko tiimille. Koodikatselmointia voidaan hyödyntää laadunvarmistamisen lisäksi tilaisuutena jakaa kokemuksia ja osaamista. Mikäli organisaation turvaosaajien määrä on rajallinen, resursseja voidaan keskittää juuri koodikatselmointiin

Tulevaisuuden tarve

Tiedottaminen hyvistä käytänteistä, konkreettisten ohjeiden jakaminen ja kustannusvaikutuksen tuominen esille voisi edistää ohjelmiston yleisen laadun ja sitä myöten myös turvallisuuden kehittymistä.

Koodikatselmoinnin merkitystä voidaan korostaa, koska se palvelee turvallisuuden lisäksi ohjelmiston laatua ja tuottaa tiimin sisällä myös yhteistä ymmärrystä työn alla olevasta ohjelmistosta.

5.7. Tekoälyn vaikutus ohjelmistoturvallisuuteen

"Koodareilta loppuu työt, kun asiakas osaa määritellä yksiselitteisesti mitä haluaa."

Tekoäly ja erityisesti erilaiset kielimallit ovat olleet vahvasti esillä julkisuudessa talvella 2023. Yleinen mielipide tuntuu olevan, että ne tulevat vaikuttamaan ohjelmistotyöhön, mutta kukaan ei osaa ennustaa varmasti, miten. Melko todennäköisinä kehityskulkuina pidetään testauksen tehostumista ja ohjelmoijan rutiinitehtävissä avustamista.

Ihmistyön merkittävää korvaantumista tekoälyllä ei pidetä todennäköisenä lyhyellä aikavälillä etenkään arkkitehtuurityössä tai vaativassa suunnittelutyössä, mutta ei myöskään perustason ohjelmoinnissa. Pidemmän aikavälin vaikutukset ovat kuitenkin vaikeasti ennustettavissa nopeasti kehittyvän uuden teknologian kohdalla.

Ohjelmistotyön lisäksi tekoäly tulee vaikuttamaan myös uhkakuvaan hyökkääjien työkaluna, mahdollistaen muiden muassa laadukkaamman lähdekoodianalyysin tai tiedusteluhavaintojen tehokkaamman analysoinnin. Vaaraksi koettiin myös tekoälyn luoman ohjelmakoodin ottaminen käyttöön harkitsemattomasti: Generatiiviset kielimallit ovat jo osoittaneet taipumusta tehdä yllättäviä virheitä.

Tulevaisuuden tarve

Tekoäly eri muodoissaan on jatkuvaa seurantaa vaativa teknologia-alue, joka tulee vaikuttamaan niin ohjelmistokehitykseen kuin ohjelmistoihin kohdistuviin uhkiin. Viestinnässä kannattaa kehottaa varovaisuuteen ja välttämään kritiikitöntä luottamusta tekoälymallien kykyihin, erityisesti korostaen arvioimattoman ohjelmakoodin kopioinnin riskejä.

6 Ohjelmistoturvallisuuden koulutus oppilaitoksissa

Ohjelmistoturvallisuuden koulutustarjontaa kartoitettiin neljän korkea-asteen oppilaitoksen haastattelulla.

Kyberturvallisuus on nykyään osa kaikkia tietotekniikan opintoja, mutta ohjelmistokehityksen turvallisuudessa alalla on aukko. Kyberturvallisuuden opinnoissa on mukana myös ohjelmistoturvallisuus ja yleiset tekniset haasteet, mutta erillään ohjelmoinnin tai ohjelmistotyön opetuksesta. Usein ymmärrys turvallisuutta luovasta suunnitteluprosessista jää puuttumaan ohjelmistotyön opetuksesta.

Haaste on siis sama kuin yritysten ohjelmistotyössä: turvallisuus jää enemmän tekniseksi elementiksi kuin koko työn kattavaksi laatuaspektiksi. Opiskelijat ymmärtävät puskurin ylivuodon tai injektion riskit, mutta turvallisuus ohjelmistokehitysprosessissa tai sen ylläpito elinkaaren aikana jää puuttumaan. Kurssitarjonnassa on kiinnostavia opintojaksoja salaustekniikoista ja penetraatiotestauksesta, mutta kokonaisvaltainen näkemys jää heikoksi.

Ohjelmistoturvallisuus edellyttää kahdenlaista osaamista. On ymmärrettävä tarve turvallisuudelle, esimerkiksi liiketoimintaan kohdistuvien riskien vuoksi. Sen lisäksi on pystyttävä toteuttamaan ohjelmisto turvallisesti suunnittelusta ylläpitoon. Jälkimmäinen osa voidaan jakaa turvallisuustarpeiden määrittelyyn vaatimuksiksi ja niiden ohjelmointiteknistä osaamista edellyttävään toteuttamiseen.

Tulevaisuuden tarve

Yleistä ymmärrystä turvan tarpeesta voidaan edistää esimerkiksi tuomalla liiketalouden opetukseen viesti IT-teknologioiden kriittisyydestä yritysten ja organisaatioiden toiminnalle. Kyberriskit ovat osa yrityksen liiketoimintariskejä.

Turvallisuus olisi hyödyllistä ottaa osaksi ohjelmistotyötä ja etenkin ohjelmistojärjestelmien opetusta. Esimerkiksi uhkamallinnuksen voi tuoda ohjelmistotuotannon kurssille tai sen harjoitustyön vaatimuksiin. Samoin ohjelmistotestaukseen voi liittää turvallisuustestauksen yhtenä laatutekijänä. Näin opiskelijoille luodaan tietoisuus turvallisuudesta osana ohjelmistotyötä.

Teknisempää kyberturvallisuusopetusta tarjotaan jo, ja siinä voidaan korostaa koko ohjelmistoprosessin merkitystä ja elinkaariajattelua.

Lisäksi tarve täydennyskoulutukselle ja osaamisen ajan tasalla pitämiselle on ilmeinen, joko oppilaitosten tarjoamana tai organisaatioiden omana koulutuksena. Ala kehittyy nopeasti ja monilla toimijoilla on jo aikaa opinnoistaan. Etenkin YAMK-opinnot sisältävät mahdollisuuden osaamisen päivittämiseen.

7 Ohjelmistohankinnat

Kyberturvallisuuden huomioiminen ohjelmistohankinnoissa vaikuttaa tällä hetkellä olevan puutteellista. Selvitystyössä ei löytynyt alan yhteisiä käytäntöjä tai jaettua vahvaa näkemystä turvallisuuden huomioimisesta hankinnoissa.

Hankittaessa räätälöityä ohjelmistoa asiakas voi asettaa projektikohtaiset vaatimukset tai osallistua aktiivisesti kehitystyöhön. Kaikissa hankinnoissa ei tähänkään aina paneuduta.

Varsinaiset haasteet ovat valmisohjelmiston tai -palvelun hankinnassa (esim. SaaS-ohjelmistot, jotka sijaitsevat palveluntarjoajan tietojärjestelmässä). Kun ohjelmisto hankitaan valmiina, mahdolliset muutostarpeet tulevat kalliiksi.

Palvelun tai tuotteen toimittaja saattaa ohjelmistoturvallisuuden osoitukseksi esimerkiksi viitata alalla yleiseen ISO 27001 -sertifiointiin. Sertifiointi osoittaa kuitenkin vain, että organisaatio on luonut prosessit tietoturvan hallintaan, ei välttämättä sitä, miten nämä prosessit suojaavat asiakasta.

Haastatteluissa ohjelmistopalveluita tarjoavat yritykset raportoivat asiakkaiden edellyttävän tarjoajalta kyberturvallisuutta, joskin usein pintapuolisesti "onhan kunnossa" -tasolla. Yritykset ovat myös vaihtelevan tietoisia asemastaan toimitusketjussa ja haluavat nostaa oman toimintansa tasoa varmistaaksensa, että ovat luotettava kumppani.

Kyselytutkimuksessa noin 50 % vastaajista koki kyberturvallisuuden merkitykselliseksi kilpailutekijänä. 11 % huomautti asiakkaan vaativan turvallisuutta, mutta ei seuraavan sen toteutumista. 17 % kertoi lisäksi itse kouluttavansa asiakkaita ymmärtämään kyberturvallisuuden merkitystä.

7.1. Mitä hankitaan

Käytännössä kaikki organisaatiot tekevät ohjelmistohankintoja. Toimisto-ohjelmat, taloushallinto, HR-järjestelmä jne. ovat perustyövälineitä kaikille yrityksille. Osa hankituista ohjelmistoista asennetaan organisaation omiin koneisiin, osaa käytetään verkon ylitse SaaS-palveluna, jolloin tietoa siirretään organisaation järjestelmien ulkopuolelle.

Myös ohjelmistotyössä tehdään hankintoja. Kehysohjelmistojen ja kirjastojen sekä muiden kehitystyökalujen valinnat ja käyttöönotot ovat hankintoja, myös käytettäessä maksuttomia Open Source -työkaluja. Tämä unohdetaan usein, vaikka kyseessä on muiden ohjelmistohankintojen tapainen toimi. Molemmissa tapauksissa otetaan käyttöön ohjelmistoja, joiden turvallisuus ja toimitusketju

tulisi arvioida. Nämä hankinnat myös sitovat organisaatiota, esimerkiksi Open Source -komponenttien käyttöä rajoittavat lisenssiehdot. On siis syytä huomata, ettei hankinnan vaikutusta voi arvioida hinnan perusteella.

Nämä hankinnat muodostavat osan organisaation tuotantoketjua, ja tuleva sääntely (mm. NIS2) tulee edellyttämään tuotantoketjujen turvallisuuden varmistamista. Tämä tulee luomaan paineita hankintojen turvallisuuden määrittelemiselle ja kehittämiselle.

7.2. Hankkijan näkökulma

"Hankittiin dedikoitu ohjelmisto, oletettiin tietoturvan toteutuvan."

Hankinnassa on syytä huomioida hankintamenettelyn/kilpailutuksen aikaisten turvallisuusvaatimusten lisäksi sopimuskauden aikaiset vaatimukset ja niiden mahdollinen muuttuminen, kuten myös teknologian kehittyminen ja uhkakuvan muutokset. Sopimuskautta arvioitaessa on huomioitava sekä ohjelmiston tai palvelun kehitysvaihe että sen käyttö- ja ylläpitovaihe – kuten myös käytöstäpoisto elinkaaren päättyessä. Erityisen tärkeää on edellyttää ohjelmiston turvallisuuden jatkuvaa ylläpitoa.

Haastattelujen perusteella hankintavaiheessa on hankalaa arvioida kohteen todellista laatua, eikä hankinnan jälkeiseen seurantaan yleensä kiinnitetä suurta huomiota. Kyselytutkimuksen mukaan ohjelmistohankinnoissa määritellään yleensä tietoturvavaatimukset. Oman osaamisen puutetta raportoi kuitenkin noin 40 % vastaajista. Lisäksi 10 % koki toimittajan toteutuksen olleen läpinäkymätön, mikä on vaikeuttanut turvallisuuden arviointia. Vastanneista osa kertoi organisaatiolla olevan yleiset hankintojen tietoturvavaatimukset ja osaamista niiden tapauskohtaiseen tarkentamiseen.

Kysyttäessä hankintapäätöksen jälkeistä turvallisuuden seurantaa vastaukset olivat huomattavasti hajanaisempia. Noin kolmannes vastaajista totesi, ettei turvallisuuden toteutumista seurata tai seurannan sijaan luotetaan toimittajaan.

7.3. Tarjoajan näkökulma

"Yritys tarvitsee tavan osoittaa turvallisuuden KV-markkinoilla"

Hankintavaiheessa asiakas voi asettaa vaatimuksia tiedon käsittelylle ja säilytykselle, toimittajan osaamiselle, toimittajan sertifioinnille, henkilöstön osaamiselle, prosesseille jne. Vaatimusten valvominen ja seuranta on kuitenkin melko työlästä, ja osa vaadituista tiedoista on myös toimittajien yrityssalaisuuksia. Jos jokainen hankkija luo omat vaatimuksensa, tuotteen tai palvelun tarjoaminen käy työlääksi tai jopa mahdottomaksi. Alalle olisi hyödyksi luoda yhtenäiset käytännöt tietoturvavaatimuksille. Suurin hyöty saavutettaisiin jaetuista kansainvälisistä käytännöistä. Käytännöt voidaan kirjata turvallisuussopimukseen, jossa sovitaan osapuolten välisestä toiminnasta ja sen seurannasta.

Tulevaisuuden tarve

Tiedonhallintalautakunta on antanut suosituksen julkishallinnon hankintojen tietoturvallisuudesta. Tämän lisäksi on tarvetta ohjeistaa myös yritysten hankintoja ja luoda niihin yhteisiä käytäntöjä.

Ohjelmistovientialan kannalta olisi hyödyllistä saada luotua kansainvälinen menettelytapa ohjelmistoturvallisuuden varmistamiselle hankinnoissa hankitun tuotteen tai palvelun elinkaaren ajan. Tämä lienee vielä melko kaukana tulevaisuudessa.

8 Johtopäätökset

Selvitysraportti antaa kattavan kuvan ohjelmistoturvallisuuden tilasta Suomessa kevätkesällä 2023. Alan laajuuden vuoksi raportti ei ole yksityiskohtaisen tarkka, mutta muodostaa kokonaiskuvan jatkotoimenpiteiden tueksi. Havaintojen perusteella tasovaihtelu on huomattavaa ja turvallisuuden tasoa voidaan nostaa jakamalla edistyneempien organisaatioiden toimintamalleja ja osaamista koko ohjelmistoalalle.

Kyberturvallisuus koetaan tärkeäksi ohjelmistotyön aspektiksi ja sitä halutaan edistää, mutta se on vain yksi tavoite muiden joukossa. Selvitystyössä on pyritty löytämään ja kuvaamaan toimenpiteitä asian edistämiseksi. Ne jaetaan alla viiteen osa-alueeseen.

8.1. Johdon tuki

Turvallisuus nähdään edelleenkin ohjelmistotyössä ylimääräisenä tehtävänä, joka ei suoraan edistä ohjelmiston varsinaista toiminnallisuutta. Tekemistä on vielä turvallisuuskulttuurissa: johto ei yleensä seuraa turvallisuuden toteutumista ja käytäntöjen jalkautumista. Organisaation johdon tehtävä on asettaa prioriteetit toiminnalle ja siksi kyberturvallisuuden toteutuminen edellyttää johdon tukea. Tulossa oleva lainsäädäntö ohjaa vahvasti organisaatioiden johtoa panostamaan riskienhallintaan ja digitaalisten toimintojen turvallisuuteen.

Tiedotus organisaatioiden ja niiden johdon kyberturvallisuusvastuista nopeuttaa siirtymää uuteen normaaliin. Pakollisen ja vaadittavan laatuominaisuuden lisäksi voidaan korostaa turvallisuuden ja hyvien ohjelmistotyön käytäntöjen merkitystä pitkän aikavälin säästöjä tuovana laatutekijänä.

8.2. Keskijohdon haasteet

Tässä selvityksessä keskijohto edusti niiden toimijoiden näkökulmaa, jotka asettavat vaatimuksia ohjelmistotyölle mutta eivät toteuta sitä itse, esimerkiksi muu liiketoiminta tai tuote- ja palveluomistajat. Heillä on oletusarvoisesti ristiriita tarpeiden ja niiden saavuttamista hidastavan turvallisuustyön välillä.

Keskijohdon kohdalla suurin vaikuttavuus voidaan oletettavasti saavuttaa korostamalla turvallisuuden merkitystä ohjelmistotyön jokaisessa vaiheessa ja etenkin alkuvaiheen suunnittelutyössä. Oletettavasti suurin kynnys on alan osaamisen vähyydessä, ja turvallisuutta voidaan edistää tuomalla esille toimintamalleja, jotka eivät nosta ohjelmistotyön työkuormaa merkittävästi.

8.3. Ohjelmistokehitys

Varsinaisessa ohjelmistotyössä nousi selvästi esille osaamisen ja organisaation tuen puute. Silloinkin kuin organisaatio haluaa panostaa turvallisuuteen, sillä ei ole omaa osaamista tai osaavaa henkilöstöä ei pystytä rekrytoimaan helposti.

Puutteita voidaan korjata alan koulutuksen ja täydennyskoulutuksen kautta, mutta myös tiedotuksella hyvistä toimintatavoista ja alan toimijoiden vertaistuella. Erityisesti nousi esille mahdollisuus vaikuttaa yleisten ohjelmistokirjastojen ja -kehysten esimerkkeihin ja valmiisiin kehityspohjiin.

8.4. Hankinta

Hankintatoimen selkeä haaste on yleisten standardien ja läpinäkyvyyden puute. Hankkijan on vaikea ottaa selvää tarjotun ohjelmiston tai palvelun turvallisuuden tasosta, ja tarjoajan on vaikea osoittaa tämä hankkijan ymmärtämällä tavalla.

Pitkällä aikavälillä yhteiskunnan turvallisuutta nostaisi kansainvälisten ohjelmistojen turvallisuutta määrittävien standardien luominen. Odotellessa turvallisuuden huomioimista ohjelmistohankinnoissa voidaan edistää ohjeilla ja toimintaesimerkeillä.

8.5. Koulutus

Varsinaista ohjelmistotyön turvallisuutta koulutetaan melko vähän, useimmissa oppilaitoksissa ohjelmistotyö ja kyberturvallisuus ovat erillään toisistaan ja ohjelmistoturvallisuudenkin koulutus painottuu tekniseen toteutukseen.

Oppilaitoksia voidaan kannustaa integroimaan ohjelmistoturvallisuus muun ohjelmistotyön koulutukseen, etenkin ohjelmistotyön prosessien opetukseen.

Liitteet

Liite 1: Selvityksessä käytetyt tutkimusmenetelmät

1.1. Haastattelut

Selvitystyö aloitettiin haastattelemalla ohjelmistoalan toimijoita maalis-huhtikuussa 2023. Haastattelujen tarkoitus oli kartoittaa alan toimijoiden maailmankuvaa ja auttaa kohdistamaan varsinaista kyselytutkimusta.

Haastattelut toteutettiin puolistrukturoidulla (semi-structured), metodilla, jossa haastattelijalla oli valmisteltuja kysymyksiä ja teemoja, mutta nämä eivät rajanneet haastattelun kulkua. Haastatteluihin pyrittiin saamaan henkilöitä eri rooleista; kehittäjiä, tuoteomistajia ja liiketoimintavastuussa toimivia henkilöitä. Tässä onnistuttiin ja haastattelut muodostivat kiinnostavan kvalitatiivisen kuvan tietoturvan toteutumisesta ohjelmistotyössä ja hankinnoissa.

1.2. Kyselytutkimus

Kyselytutkimus toteutettiin osana selvitystyötä huhti-toukokuussa 2023. Kyselyyn vastasi 89 henkilöä. Kysely toteutettiin verkkokyselynä, jota mainostettiin eri kanavissa. Kyselyn tuloksissa on siten huomioitava itsevalinnan vaikutus (self-selection bias). Kyselyä voidaan kuitenkin pitää kustannustehokkaana tapana saada tietoa kattavasti toimialalta ja sen tuloksia voidaan varauksella pitää kvantitatiivisena katsauksena ajankohtaan.

Vastaajien jakauma aseman mukaan:

20% Liiketoimintavastuu ja ylin johto

55% Keskijohto, tuoteomista, projektipäällikkö

25% Kehittäjä, suunnittelija, asiantuntija

83% vastanneista ilmoitti tietoturvaratkaisujen olevan vastuullaan.

74% vastanneista osallistui päätöksentekoon tietoturva-asioissa.

Toimialoissa oli huomattavasti hajontaa yli yksityisten ja julkisten alojen. IT-ala korostui jonkin verran ylitse muiden. Organisaatioiden koko vaihteli myös pienistä suuriin, 46% edusti huoltovarmuuskriittistä alaa.

Organisaation kyberturvallisuuden kehitystarpeista kysyttäessä vastaajilla vaikutti olevan selvä näkemys tarpeesta kehittää turvallisuutta, yksikään vastaus ei todennut tason olevan riittävän ja muutama vastaus totesi kehityksen olevan jatkuvaa muuttuvan uhkakuvan johdosta. Vastaukset olivat hyvin hajanaisia, mutta yleinen teema oli lisätä suunnitelmallisuutta ja kypsyyttä turvallisuustoimintaan esimerkiksi kehittämällä hallintajärjestelmää ja prosesseja. Oman organisaation osaamisen puute ja asenteet koettiin haasteiksi.

Kysely nosti esille myös tarpeita, joita vastaaja ei tunne pystyvänsä toteuttamaan, tässä yleisenä teemana oli resurssien rajallisuus, sekä organisaation tai henkilöstön muutosvastarinta. Muutama (alle 10%) vastaajista totesi pystyvänsä toteuttamaan turvallisuutta haluamallaan tasolla.

Avustavia toimenpiteinä kysyttäessä vastaajat toivat esille tarpeen lisäresursseille (rahaa ja/tai aikaa) sekä koulutuksen tarpeen itsellensä, muulle henkilöstölle ja myös yhteistyökumppaneille.

Kysyttäessä onnistumisia kyberturvallisuuden saralla, melko yleisiä vastauksia olivat: turvallisuuspoikkeamilta välttyminen, johdon tuen saavuttaminen ja osaamistason lisääminen. Selkeä vastaustyyppi oli myös jonkin osatoiminnallisuuden (teknisen tai organisatorisen) käyttöönotto.

Tiedusteltaessa millainen turvapoikkeama aiheuttaisi suurimman haitan, tietovuoto ja toiminnan jatkuvuuden estyminen (esim. ransomware) kattoivat suurimman osan vastauksista. Tietovuodon aiheuttamaa vahinkoa vastaajat eivät eritelleet erikseen, tapahtumastahan voi seurata korvausvelvollisuus, asiakkaiden menettäminen tai muu mainehaitta.

1.3. Työpajat

Edellisten lisäksi järjestettiin kaksi työpajaa, joissa pohdittiin ohjelmistoturvallisuuden haasteita ja ratkaisuja. Työpajojen tuloksia on hyödynnetty selvitystä laadittaessa.

Liite 2: Ohjelmistoturvallisuuden ohjeet, standardit ja lähteet

Osana Turvallisen ohjelmistokehityksen selvitystyötä kartoitetaan mitä kansainvälisiä ja kansallisia ohjeita, standardeja ja muita julkaisuja on saatavilla turvallisen ohjelmistokehityksen tueksi. Julkaisut kootaan tähän dokumenttiin. Dokumentin rakenne muotoutuu sitä mukaa kun julkaisuja kertyy. Julkaisuista muodostetaan taulukkoja kokonaisuuden hahmottamiseksi.

Ohjelmistotyön turvallisuuden ohjeistuksesta ei ole varsinaista pulaa, ohjelmistohankintojen kohdalla tarjonta on suppeampaa. Ohjeet ja standardit eivät ole juurikaan ristiriitaisia keskenänsä, ne painottavat usein eri osa-alueita ja esittävät asiat eri tavoin, tai eri näkökulmasta. Prosessimalleissa, toimintatavoissa ja arvioinnin kohteissa on kuitenkin sen verran eroavaisuutta eri ohjeiden välillä, että useamman päällekkäisen mallin noudattaminen voi olla työlästä.

Osa ohjeistuksesta on toimintatapasuosituksia tai oppaita, osa formaalimpia vaatimuksia sisältäviä standardeja tai viranomaisvaatimuksia. Esimerkiksi OWASP:n ohjeet ovat melko käytännönläheisiä teknisiä ohjeita, joista osaa (Top-10, Secure Coding Practices Checklist) yksittäinen kehittäjä voi hyödyntää itsenäisestikin, kun toiset ohjaavat koko kehitysprosessia (kuten IEC 62443 tai SAFe) ja edellyttävät kehitysorganisaation laajuista soveltamista liiketoimintakytköksineen.

Koska IT-ala on kehittynyt nopeasti ja enemmän käytännön kuin teorian ohjaamana, monet ohjeet ja standardit heijastavat ohjeen luojien toimintaympäristöä ja kokemuksia. Esimerkiksi yksi ohje (Katakri) saattaa olettaa tiedon haltijan olevan ensisijainen tietojen käsittelijä ja tiedon vaihdon olevan rajallista, kun toinen ohje keskittyy yleisölle avoimeen verkkopalveluun (PCI-DSS). Tai yhden ohjeen (ISO 27001) lähtöpyrkimys saattaa olla turvallinen tietojenkäsittely-ympäristö, kun toinen (NIST CSF) olettaa asioiden menevän pieleen kumminkin ja korostaa poikkeamien hallintaa ja toipumista.

2.1. Eri mallien ominaisuuksia

Tyypillisesti eri ohjeiden ja standardien kuvaamista toimintamalleista löytyy seuraavia ominaisuuksia.

- Vaatimukset ja tarkistuspisteet: Edellytetään konkreettinen vaatimus (eri turvatasojen järjestelmät on eriytettävä toisistaan) tai edellytetään toimintoa määritteleмättä tarkkaa toteutusta (järjestelmä on suunniteltava riskiperustaisesti uhkamallinnuksen pohjalta).
- Prosessi ja hyväksyntäportit: Ohjelmistokehityksen malleissa kuvataan yleensä prosessin vaiheet ja edellytetään menettely vaiheen päättämiseksi (esim. ketterän kehityksen "definition of done": ohjelmistovaatimuksesta on pystyttävä määrittelemään, milloin se on toteutettu).
- Seuranta, mittaaminen ja vuosikello: Useat mallit edellyttävät toimintaa seurattavan. Organisaatioturvaa ja elinkaarta käsittelevät mallit edellyttävät yleensä toistuvaa uhkakuvan ja toteutettujen suojausten tarkastelua ja uudelleenarviointia.
- Kypsyysmalli: Osassa ohjelmistotyön turvallisuuden malleista (esim. C2M2, SAMM) on oletuksena, että organisaatio kasvattaa osaamistaan tai kyvykkyyttänsä ajan kanssa, eikä korkeaan osaamistasoon ole oikopolkua.

Tämä edustaa näkemystä ohjelmistotyöstä käytännön kokemusta vaativana artesaanityönä.

2.2. Turvallisen ohjelmistotyön organisointi

Turvallisuus voidaan toteuttaa ohjelmistohankkeen eri vaiheissa ja eri metodein, nämä ohjeet kuvaavat tapoja tehdä se.

2.2.1. DVV:n Turvallisen sovelluskehityksen käsikirja

Digi- ja väestötietoviraston Turvallisen sovelluskehityksen käsikirja on suunnattu julkisen hallinnon organisaatioille, mutta soveltuu myös muille ketterää sovelluskehitystä soveltaville organisaatioille.

Käsikirjan kantava teema on secure by design -ajattelu ketterässä ohjelmistokehityksessä ja että tietoturva- ja tietosuojatyö tehdään näkyväksi tiketöimällä niihin liittyvät työt ja niitä töitä tehdään kaikissa ohjelmistokehityksen vaiheissa. Käsikirja perustuu ns. alan yleisiin hyviin käytänteisiin. Siinä viitataan mm. OWASP:n Top 10:iin ja ASVS:ään. Ohje tuo myös esille turvallista ohjelmointia tukevan prosessimallin.

DVV on uudistamassa käsikirjaa siten, että siitä tulisi kevyempi käyttää jokapäiväisessä työssä. Käsikirja tullaan jakamaan SDLC- tai DevSecOps-mallin vaiheisiin ja jokaiseen vaiheeseen nostetaan ne tietoturva- ja tietosuojatyöt, jotka ko. vaiheessa pitää tehdä. Näin käsikirjaa voi käyttää myös tarkistuslistana.

https://www.suomidigi.fi/ohjeet-ja-tuki/tyokalut/turvallisen-sovelluskehityksen-kasikirja

https://www.suomidigi.fi/sites/default/files/2020-05/Turvallisen%20sovelluskehityksen%20k%C3%A4sikirja.pdf

Uusin online-versio Wikissä:
https://wiki.dvv.fi/pages/viewpage.action?pageId=230470940

2.2.2. KTK: Turvallinen tuotekehitys – kohti hyväksyntää

Opas on tarkoitettu kaikille ohjelmistopohjaisten ratkaisujen kehittäjille, erityisesti salausratkaisujen tuottajille. Se sisältää parhaita käytäntöjä haavoittuvuuksien ja muiden yleisimpien ongelmien välttämisestä ohjelmistotuotannossa. Ohje ei ota kantaa näitä käytäntöjä toteuttavaan prosessiin.

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf

2.2.3. NIST Secure Software Development Framework

SSDF on lyhyt vaatimuslista ja prosessimalli turvallisuuden huomioimiseen ohjelmistokehityksessä.

https://csrc.nist.gov/pubs/sp/800/218/final

2.2.4. OWASP Software Assurance Maturity Model (SAMM)

SAMM on viitekehys ohjelmistotyön turvallisuuden organisointiin ja koordinointiin.

https://owaspsamm.org/

2.2.5. Scaled Agile Framework (SAFe)

SAFe on prosessimalli suurehkon organisaation ketterään ohjelmistokehitykseen, jossa useat tiimit toimivat saman kokonaisuuden parissa.

https://scaledagileframework.com/

2.2.6. IEC 62443 -perhe ja sen osa 4-1

IEC 62443 on automaatiojärjestelmien ja -verkkojen turvallisuutta käsittelevä standardiperhe. Sen osa 4-1 käsittelee turvallisuuden hallintaa tuotteen elinkaaren ylitse ja standardia käytetään ohjelmistokehityksen turvallisuuden viitekehyksenä.

IEC 62443-4-1:2018 Secure product development lifecycle requirements

2.3. Ohjelmointityö

Varsinaista ohjelmointityötä koskevat ohjeet ovat melko konkreettisia ja keskittyvät tunnettuihin toteutustekniikkoihin ja tunnettujen virheiden välttämiseen.

2.3.1. OWASP Top 10

Open Worldwide Application Security Project -säätiön (OWASP) säännöllisesti päivittyvä OWASP Top 10 -lista kuvaa julkaisuajankohtansa kymmenen yleisintä ohjelmistohaavoittuvuutta ja mainittiin usein sekä haastatteluissa että kyselyssä ensimmäisenä astinlautana turvalliseen ohjelmointiin. OWASP Top 10 avulla voidaan taklata yleisimmät haavoittuvuudet.

On aiheellista huomauttaa, että Top 10 kuvaa vain kymmenen yleisintä ongelmaa, eikä sen noudattaminen riitä toteuttamaan kattavaa ohjelmistoturvallisuutta. Top 10 on hyvä aloitusohje, jonka toteuttamisen jälkeen voi ponnistaa eteenpäin.

https://owasp.org/www-project-top-ten/

2.3.2. OWASP Application Security Verification Standard (ASVS)

ASVS on käytännönläheinen lista tarkastuskohteita Web-teknologioihin perustuville sovelluksille ja niiden kehitystyölle (suuri osa moderneista sovelluksista on tällaisia).

https://owasp.org/www-project-application-security-verification-standard/

2.3.3. OWASP tarjoaa myös pikaohjeen ja tarkastuslistan kehittäjille:

https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

2.3.4. CMU SEI CERT Coding Standards

Carnegie Mellon -yliopiston Software Engineering Institute on laatinut joukon ohjelmistokielikohtaisia ohjelmointistandardeja, jotka määrittävät yksityiskohtaisesti kyseisen kielen tai ympäristön turvallista ohjelmointia.

https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

2.4. Koulutusympäristöjä

Henkilöstön osaamistasoa nostavaa koulutusta on tarjoilla myös verkkoympäristössä. Alla oleva lista ei ole täydellinen lista, mutta antaa suuntaa saatavilla olevista koulutusympäristöistä.

2.4.1. Fraktal – DevSecLab

DevSecLab on Suomessa kehitetty web-sovellusten turvallisuuden opettelualusta.

https://www.devseclab.io/

2.4.2. OWASP Coding Dojo

Coding Dojo on pelillistetty koulutusalusta, jossa harjoitellaan hyökkäyksiä ja puolustuksia niitä vastaan.

https://owasp.org/www-project-secure-coding-dojo/

2.4.3. Security Knowledge Framework

OWASP-hankkeesta erilleen kehittynyt Security Knowledge Framework on turvallisen ohjelmoinnin koulutusympäristö, joka ohjaa rakentamaan turvallisen ohjelmistoprojektin.

https://www.securityknowledgeframework.org/

2.5. Ohjelmiston hankinta

Yleistä ohjelmistoturvallisuuden hankintaohjeistusta vaikuttaa olevan lähinnä julkishallinnon hankintoihin.

2.5.1. Tiedonhallintalautakunnan Suositus tietoturvallisuudesta hankinnoissa

Tiedonhallintalautakunnan suositus pohjautuu Tiedonhallintalakiin ja Julkriin. Suositus on tarkoitettu erityisesti julkishallinnolle, mutta on sovellettavissa muihinkin hankintoihin.

http://urn.fi/URN:ISBN:978-952-367-645-9

2.5.2. SOTEn hankintavaatimukset

Tietoturva- ja tietosuojavaatimusten lista on luonteeltaan sote-alan kyberturvallisuuden ja tietosuojan asiantuntijoiden yhteinen käsitys hyvistä käytännöistä. Ei ole virallinen ohje tai suositus.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja

2.6. Ohjelmisto- ja muiden tuotteiden sertifiointimallit

Johtuen ohjelmistojen suuresta kompleksisuudesta, tietokoneohjelmia ei yleensä voi todistaa oikeiksi tai edes turvallisiksi. Ohjelmistotuotteiden turvallisuuden validointiin on kuitenkin kehitetty toimintamalleja, joita noudattamalla ohjelmiston on todennäköisesti suunniteltu ja toteutettu oikein ja turvallisesti.

Nämä sertifioinnit ovat yleensä melko työläitä ja kattavat vain osan järjestelmästä tai sertifiointi hankitaan rajoitettuja uhkia vastaan.

2.6.1. Common Criteria

The Common Criteria for Information Technology Security Evaluation formalisoi ohjelmiston suunnittelu- ja toteutusprosessin verifioitaviksi askeleiksi, joiden perusteella tuotteelle voidaan myöntää sertifiointi. Sertifiointi perustuu oletuksiin uhista, kuten hyökkääjän kyvykkyyksistä.

https://www.commoncriteriaportal.org/

2.6.2. Federal Information Processing Standard 140-2 ja uudempi 140-3

USA:n valtionhallinnon FIPS-standardit kattavat erilaisia julkishankintojen vaatimuksia. FIPS 140 standardit määrittävät salausteknisen moduulin hyväksyntävaatimukset ja tyypillisesti esimerkiksi sähköisen tunnistautumisen mahdollistavat laitteet on sertifioitu FIPS 140-2 tai 140-3 mukaisiksi.

https://csrc.nist.gov/pubs/fips/140-2/upd2/final

https://csrc.nist.gov/pubs/fips/140-3/final

2.7. Suomalaiset arviointikriteeristöt

Suomessa on laadittu, lähinnä julkishallinnon käyttöön, kansallisia arviointikriteeristöjä, joiden vaatimuksia voidaan käyttää ohjaamaan organisaation kyberturvallisuustyötä.

2.7.1. Katakri

Tietojärjestelmästandardi. Ei sovellu ohjelmistokehitykseen. Viranomaisten käyttöön tarkoitettu arviointityökalu, jonka avulla voidaan arvioida kohdeorganisaation kykyä suojata viranomaisen turvallisuusluokiteltua tietoa.

https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

2.7.2. Julkri

Tietojärjestelmästandardi. Ei sovellu ohjelmistokehitykseen. Tiedonhallintalautakunnan laatima kriteeristö julkishallintoa varten.

http://urn.fi/URN:ISBN:978-952-367-458-5

2.7.3. Pitukri

Pilvipalveluiden turvallisuuden arviointikriteeristö. Ei sovellu ohjelmistokehitykseen. Kriteeristö auttaa viranomaisia arvioimaan oman salassa pidettävän tietonsa turvallisuutta tilanteissa, joissa niiden tietoja käsitellään pilvipalveluissa.

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

2.8. EU:n regulaatio

Euroopan unioni pystyy kokonsa vuoksi antamaan regulaatiota, jolla on merkittävä kansainvälinen painoarvo, myös unionin ulkopuolella. Unioni on panostamassa kyberturvallisuuden regulointiin, ulottuen myös ohjelmistoalalle.

2.8.1. Kyberturvallisuusdirektiivi

Kyberturvallisuusdirektiivi eli NIS2 direktiivi asettaa kyberturvallisuuden riskienhallintatoimenpiteet keskeisille viestintäverkko- ja tietojärjestelmäpalveluiden tarjoajille sekä yhteiskunnalle kriittisille toimijoille.

https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX%3A32022L2555#d1e40-80-1

Hankesivu Euroopan unionin kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

https://valtioneuvosto.fi/hanke?tunnus=LVM027:00/2023#

2.8.2. Kyberkestävyyssäädös

Kyberkestävyyssäädös (Cyber Recilience Act, CRA) asettaa perustason tietoturvavaatimukset Internetiin yhteydessä oleville laitteille ja ohjelmistotuotteille niiden koko elinkaaren ajalle ja edellyttää haavoittuvuuksien korjaamista.

Säädäksen luonnosteksti:

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

CRA factsheet: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

2.8.3. Radiolaitedirektiivin delegoidut säädökset

Radiolaitedirektiivin (Radio Equipment Directive, RED) delegoidut säädökset langattomien laitteiden tietoturvalle:

https://single-market-economy.ec.europa.eu/news/commission-strengthens-cybersecurity-wireless-devices-and-products-2021-10-29_en

Tietoturvavaatimukset ovat tulleet voimaan helmikuussa 2022 ja siirtymäaika on parhaillaan menossa. Säädöstä sovelletaan 1.8.2025 alkaen.

varsinainen säädösteksti: https://single-market-economy.ec.europa.eu/system/files/2021-10/C_2021_7672_F1_COMMISSION_DELEGATED_REGULATION_EN_V10_P1_1428769.PDF

ja komission FAQ: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_5635

2.9. Yleiset kyberturvallisuusstandardit ja -ohjeet

Nämä ohjeet ja standardit on tarkoitettu tukemaan organisaation kyberturvallisuutta ja ne eivät välttämättä ota suoraan kantaa ohjelmistoturvallisuuden yksityiskohtiin, mutta huomioivat sen osana kokonaisuutta.

2.9.1. ISO/IEC 27001

ISO 27001-perhe on hyvin yleisesti käytetty organisaation tietoturvallisuuden hallintaa ja prosesseja ohjaava standardi. Uusin, 2022 julkaistu versio listaa myös ohjelmistokehityksen turvallisuuteen liittyviä vaatimuksia.

ISO/IEC 27001:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. **Tietoturvallisuuden hallintajärjestelmät**. **Vaatimukset**.

ISO/IEC 27002:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. **Tietoturvallisuuden hallintakeinot**.

2.9.2. NIST Cybersecurity Framework

USA:n standardointivirasto NIST:n CSF on ISO 27001:n tapainen turvallisuuden hallintaa ohjaava standardi. CSF on uudempi kuin ISO 27001 ja ottaa hivenen erilaisen näkökulman aiheeseen, mutta kattaa olennaisesti saman alueen.

https://www.nist.gov/cyberframework

2.9.3. Kybermittari

Kyberturvallisuuskeskuksen kehittämä Kybermittari ei ole standardi, vaan työkalu organisaation kyberturvallisuuden tason itsearviointiin. Se perustuu Cybersecurity Capability Maturity Modeliin (C2M2) ja NIST CSF-malliin, antaen kuvan organisaation kypsyystasosta kyberturvallisuuden alueella.

https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

2.9.4. ITIL

Information Technology Infrastructure Library (ITIL) on IT-palveluiden hallintaa ohjaava laaja (n. 30 kirjaa) ohjeisto, jonka näkökulma on palvelua toteuttavissa prosesseissa ja niiden kehittämisessä ja seurannassa. ITIL ei ole varsinaisesti kyberturvallisuusohjeisto, mutta liittyy palvelutuotannon prosesseihin ja siten myös turvallisuuteen.

2.10. Toimialakohtaiset ohjeet

Kyberturvallisuuden merkityksen kasvaessa eri toimialat ovat laatineen omia alakohtaisia ohjeitansa. Nämä eivät yleensä ulotu varsinaiseen ohjelmistotyöhön.

Esimerkiksi maksukorttialan Payment Card Industry Data Security Standard (PCI-DSS), sisältää samantapaisia tietoturvavaatimuksia turvallisuuden prosesseista, ylläpidosta ja järjestelmäsuunnittelusta kuin yleisemmätkin ohjeet, mutta kuvailee ne spesifisesti maksukorttitapahtumaan sovellettuna.

https://www.pcisecuritystandards.org/

Esimerkkinä trendistä, kansainvälinen satamajärjestö IAPH (International Association of Ports and Harbors) on julkaissut satamien kyberturvallisuutta koskevan ohjeen " IAPH Cybersecurity Guidelines for Ports and Port Facilities", joka soveltaa yleiset kyberturvallisuuden hallintaohjeet satama ympäristöön, mutta ei ota tarkempaa kantaa ohjelmistoturvallisuuteen tai ohjelmistojen ja palveluiden hankintoihin.

https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

Lienee oletettavissa, että lähivuosina eri toimialoilla tullaan laatimaan alakohtaisia kyberturvallisuusohjeistoja, jotka sisältävät pääpiirteissänsä saman sisällön kuin ISO 27001 tai NIST CSF, mutta toimialakohtaiseksi muokattuna.

2.11. Muita kansallisia ohjeita

2.11.1. USA

https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

2.11.2. UK - NCSC

Motivaatiokirjeitä turvallisen koodin kehittämiseen

https://www.ncsc.gov.uk/blog-post/motivating-developers-to-write-secure-code

https://www.riscs.org.uk/project/motivating-jenny-to-write-secure-software-community-and-culture-of-coding/

https://www.ncsc.gov.uk/collection/developers-collection/principles

Liikenne- ja viestintävirasto Traficom
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

TRAFICOM
Liikenne- ja viestintävirasto