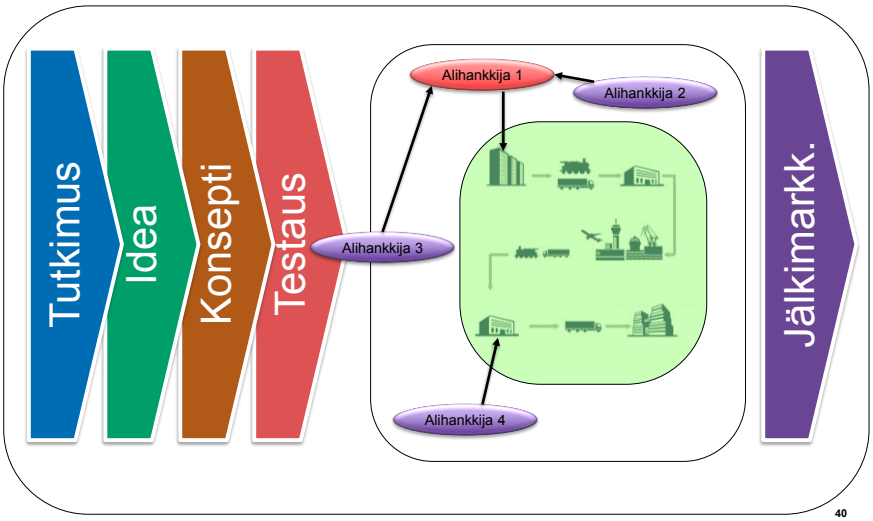
Kyberturvallisuuden haasteet

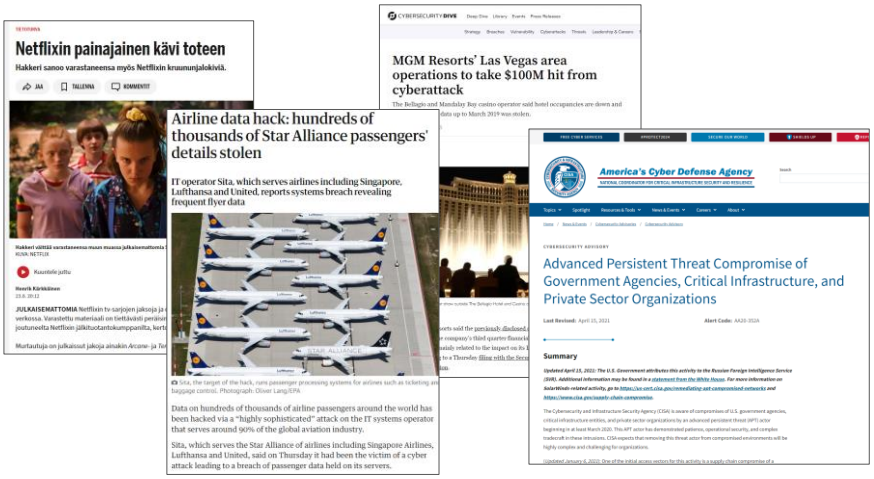
Toimitusketjut

Mitä kuuluu toimitusketjuun?



Intuitiivisesti toimitusketju voidaan ymmärtää logistiikan kannalta, jolloin kyse on valmiin tuotteen “toimittamisesta” valmistajalta perille; tai tuotteen valmistamiseen liittyvä alihankintaketju tai kaikkein laajimmassa merkityksessä koko tuotteen elinkaaren kattava ketju ideoinnista jälkimarkkinointiin.

Mitä, jos toimitusketjun kyberturva pettää?

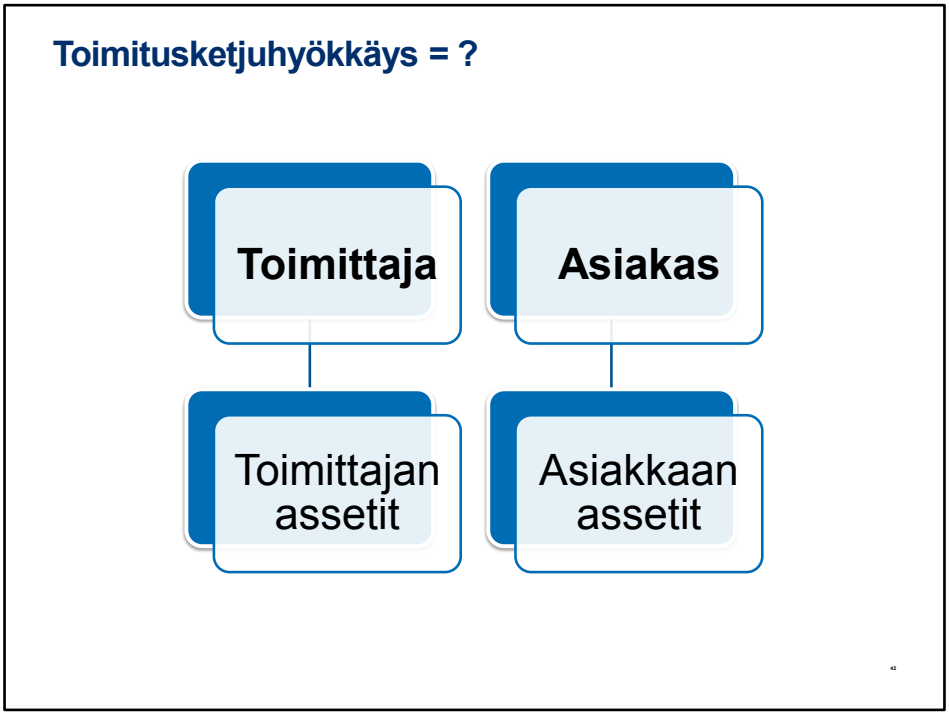


41

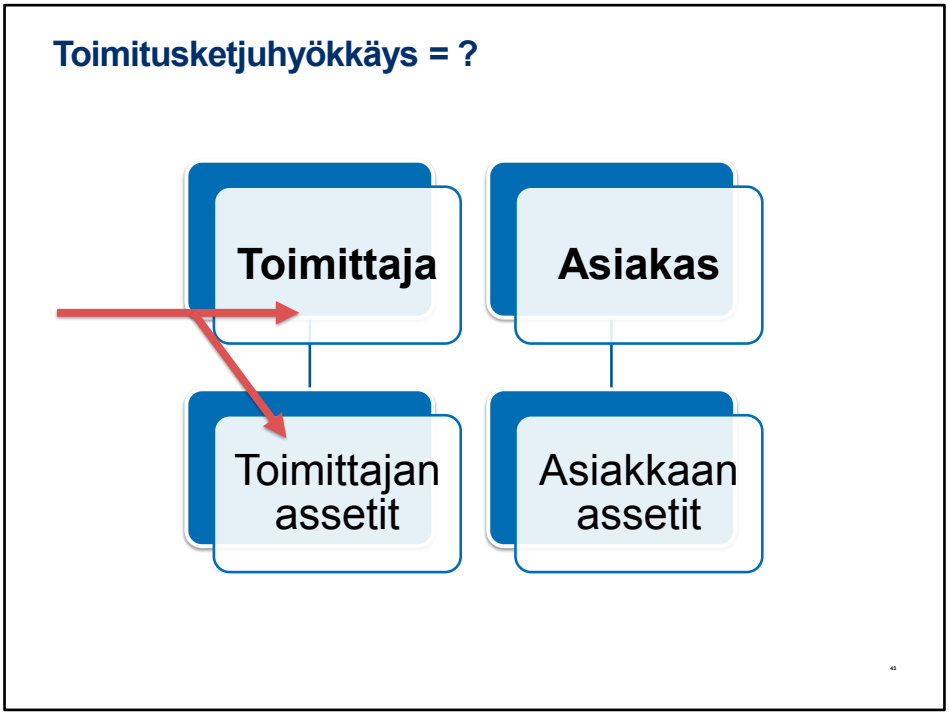
Toimitusketjut ovat osa jokaisen modernin organisaation toimintaa. Ohessa esimerkkejä eri toimialoilta, mitä voi käydä, jos toimitusketjun kyberturvallisuus pettää:

- Media-ala, kesällä 2024: Netflixin jälkituotantoyritys Iyuno, joka tekee useammalle eri tuotantoyhtiölle tesktityksiä ja dubbauksia, joutui hakkeroinnin kohteeksi, ja useita Netflixin suosittujen sarjojen julkaisemattomia jaksoja ja tuotantokausia vuoti piraattiverkkoihin. (Yleisesti ottaen piratismi väheni suoratoistopalveluiden yleistymisen myötä, mutta on kääntynyt nyttemmin uudelleen nousuun)
- Logistiikka-ala: IT-operaattori SITA toimittaa erilaisia IT-järjestelmiä maailman eri lentoyhtiöille. V. 2021. SITAn paikkavarausjärjestelmät hakkeroitiin, ja sitä kautta esimerkiksi Air Indian matkustajatietoja vuosi hyökkääjille
- Hotelliala ja kaupan ala, 2023: Las Vegasissakin hotellia pitävä MGM Resorts joutui kiristyshaittaohjelman kohteeksi. MGM ei pystynyt käyttämään useisiin päiviin maksujärjestelmiään, pankkiautomaattejaan, sisäistä verkkoaan tai hotellihuoneiden avaimia. Tässä tapauksessa myös MGM Resortille tavaroita ja palveluita toimittavat tahot eivät saaneet maksujaan tai kyenneet viemään logistiikkaa perille asti. Lisäksi alihankkijoiden liiketoiminnalle herkkää dataa paljastui hakkereille.

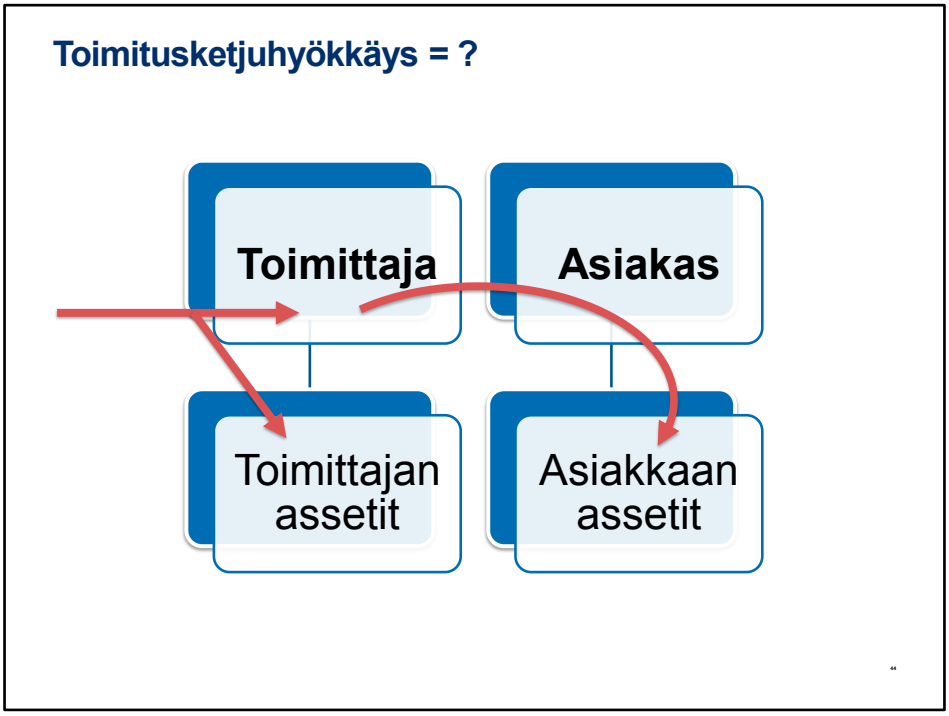
- Yleinen, 2019-: Solarwinds it-toimittajan järjestelmien hakkerointi johti ko. järjestelmää käyttävien organisaatioiden saastumiseen. Arviolta haittaohjelma koski yhteensä 18 000 organisaatiota globaalisti, ja keskimäärin kustannukset olivat yritykselle 11% vuotuisesta liikevaihdosta.



Toimitusketjuhyökkäyksessä on neljä pääelementtiä: toimittaja ja asiakas assetteineen (suojattavine kohteineen, esim. varat, liikesalaisuudet, asiakastiedot, ...). Toimitusketjuhyökkäys väärinkäyttää toimittajan ja asiakkaan välille luotujan luottamussuhteita, joita on väkisinkin oltava, jotta liiketoiminta mahdollistuu.



Jotta kyberhyökkäys laskettaisiin toimitusketjuhyökkäykseksi, on tapahduttava vähintään kaksi hyökkäystä, toimitusketjussa olevien eri lenkkejä kohtaan. Ensimmäinen hyökkäys kohdistuu yleensä toimittajaan (ja tämän asseteihin)

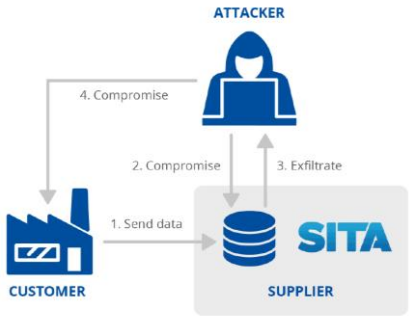


... ja toinen hyökkäys toimittajan ja asiakkaan luottamussuhdetta käyttäen sitten asiakkaaseen ja sen asseteihin.

Toimitusketjuhyökkäyksiä ei ole helppoa tunnistaa, koska monet niiden jättämistä jäljistä (kuten takaportitetut varusohjelmistot) voivat olla tahattomia Bugeja, tai haittaohjelmia, jotka ovat pesiytyneet toimittajalle ilman sen laajempaa suunnitelmaa. Toimitusketjuhyökkäyksen tunnistaminen vaatii lähes aina useamman tahon yhteistyötä ja korkeaa teknista asiantuntemusta.

Toimitusketjuhyökkäysten tavoitteet

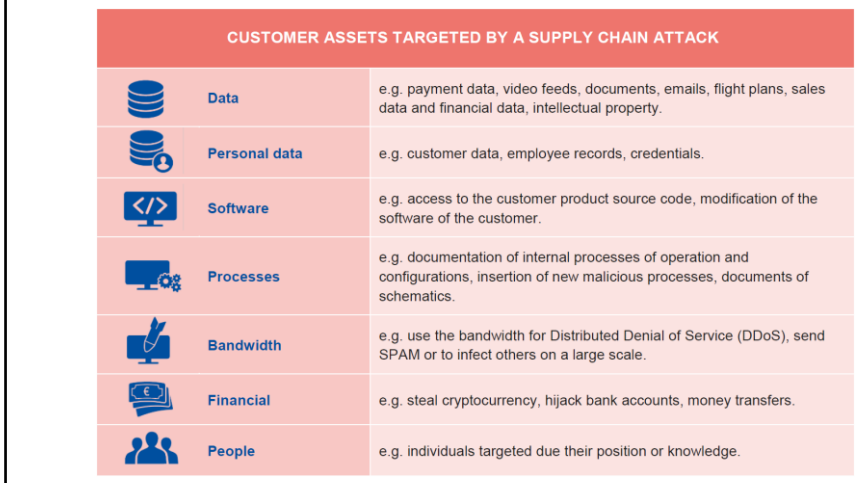
- **Toimittajan IT-sovellusten IPR (lähdekoodi)**
- **Asiakasdata**
- **Liiketoimintaan liittyvä muu data**
- **Muita kohteita: IT-resurssien kaappaaminen esim. DDoSia varten, kryptovaluutan varastaminen,...**



45

ENISAn v. 2022 raportin mukaan, toimitusketjuihin kohdistuvissa kyberhyökkäyksissä tavoiteltiin pääasiassa jonkin toimijan IT-sovellusten lähdekoodeja (66% tutkituista tapauksista), asiakasrekistereitä (58% tapauksista), muuta liiketoimintaan liittyvää data ja tietoa liiketoimintaprosesseista (n. 20% tapauksista) sekä informaatiota organisaatioiden avainhenkilöistä whalingiä varten.

Toimitusketjuhyökkäysten tavoitteet



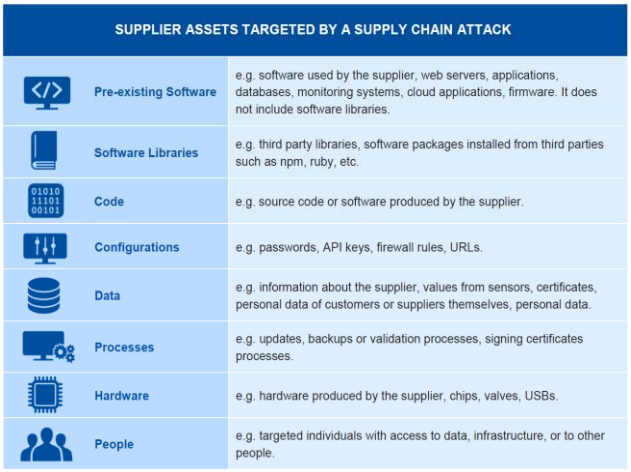
CUSTOMER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Data	e.g. payment data, video feeds, documents, emails, flight plans, sales data and financial data, intellectual property.
Personal data	e.g. customer data, employee records, credentials.
Software	e.g. access to the customer product source code, modification of the software of the customer.
Processes	e.g. documentation of internal processes of operation and configurations, insertion of new malicious processes, documents of schematics.
Bandwidth	e.g. use the bandwidth for Distributed Denial of Service (DDoS), send SPAM or to infect others on a large scale.
Financial	e.g. steal cryptocurrency, hijack bank accounts, money transfers.
People	e.g. individuals targeted due their position or knowledge.

Lähde: ENISA

46

Tässä tarkemmin esimerkkejä, mitä lopulliselta kohteelta pyritään saamaan ulos

Toimitusketjuhyökkäysten tavoitteet



SUPPLIER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Pre-existing Software	e.g. software used by the supplier, web servers, applications, databases, monitoring systems, cloud applications, firmware. It does not include software libraries.
Software Libraries	e.g. third party libraries, software packages installed from third parties such as npm, ruby, etc.
Code	e.g. source code or software produced by the supplier.
Configurations	e.g. passwords, API keys, firewall rules, URLs.
Data	e.g. information about the supplier, values from sensors, certificates, personal data of customers or suppliers themselves, personal data.
Processes	e.g. updates, backups or validation processes, signing certificates processes.
Hardware	e.g. hardware produced by the supplier, chips, valves, USBs.
People	e.g. targeted individuals with access to data, infrastructure, or to other people.

Lähde: ENISA

47

Johtuen siitä, että toimittaja on toimitusketjuhyökkäyksessä pelkkä astinlauta, siltä halutaan yleensä varastaa asiakkaan verkkoihin pääsyn kannalta hyödyllisiä tietoja ja luoda luvattomia uusia luottamussuhteita olemassa Olevia yhteyksiä väärinkäyttämällä.

Näitä on esitelty tässä, esimerkiksi...

Toimitusketjuhyökkäysten tekijät

SUPPLIER	SUPPLIER CATEGORY	YEAR	IMPACT	ATTRIBUTED GROUPS
Mimecast	Security Software	2021	Global	APT29
SITA	Aviation	2021	Global	APT41
Ledger	Blockchain	2021	Global	-
Verkada	Physical security	2021	Global	Hacktivist Group
BigNox NoxPlayer	Software	2021	Regional	-
Stock Investment Messenger	Financial Software	2021	Regional	Thallium APT
ClickStudios	Security Software	2021	Regional	-
Apple Xcode	Development Software	2021	Global	-
Myanmar Presidential Website	Public Administration	2021	Regional	Mustang Panda APT
Ukraine SEI EB	Public Administration	2021	Regional	-
Codecov	Enterprise Software	2021	Global	-
Fujitsu ProjectWEB	Cloud Collaboration	2021	Regional	-
Kaseya	IT management	2021	Global	REvil Group
MonPass	Certificate Authority	2021	Regional	Winnti APT Group
SYNNEX	Technology Distributor	2021	Regional	APT 29
Microsoft Windows HCP	Software	2021	Global	-
SolarWinds	Cloud Management	2020	Global	APT29
Accellion	Security Software	2020	Global	UNC2546
Wizvera VeraPort	Identity Management	2020	Regional	Lazarus APT
Able Desktop	Enterprise Software	2020	Regional	TA428
Aisino	Financial Software	2020	Regional	-
Vietnam VGCA	Certificate Authority	2020	Regional	TA413, TA428
NetBeans	Development Software	2020	Global	-
Unimax	Telecommunication	2020	Regional	-

Lähde: ENISA

48

Toimitusketjuhyökkäykset ovat lähes aina hyvin monimutkaisia ja teknisesti vaativia kyberhyökkäyksiä. Tästä kertoo jo sekin, että kaksi kolmasosaa tekniikoista jää kokonaan pimentoon, 40% prosentissa tekijä jää tuntemattomaksi, ja 50% tapauksista tekijäksi paljastuu erittäin hyvin resursoitu, APT-tason uhkatekijä, jolla on usein valtiollinen tausta.

Esimerkiksi APT29 (Cozy Bear, Venäjän SVR:n alainen ryhmä) on osattu tunnistaa tässä taulukossa ainakin kolmeen hyökkäykseen. APT41 (Wicked Panda, yhteyksiä myös WINNTI [-haittaohjelmaa käyttävään-] APT ryhmään) on Kiinan valtionhallinnon tukema uhkatoimija.

Toimitusketjun kyberturvallisuuden riskienhallinta

- **NIST C-SCRM-ohjelma: Cybersecurity Supply Chain Risk Management**
  - Päädokumenttina NIST SP 800-161 (r1, periytyy NIST SP 800-53:sta)
- **Perusteellinen ohjeistus toimitusketjun kyberturvallisuuden hallinnasta**
  - Idea: normaalia kyberturvallisuuden hallintaa: velvoitteita asiakkaille, valvontaa alihankkijoille
    - Ohjelmistokomponenttien haavoittuvuushallinta
    - Koko toimitusketjun kattava IAM
  - Toimitusketjuosuuksien painottaminen
  - C-SCRM:n integrointi osaksi organisaation riskienhallintaa
  - C-SCRM avainkäytänteiden tasot (perusta, ylläpito, kehittyvä)

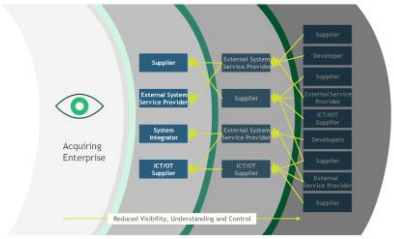


Fig. A-1: C-SCRM Security Controls in NIST SP 800-161, Rev. 1

49

Onko toimitusketjujen kyberturvallisuuden hallinnalle sitten tehtävissä mitään? Ohjeistusta sinänsä on. NISTin dokumentaatio on ilmaisena helpommin saatavilla, ja siellä alueen päädokumenttin on NIST SP 800-161, jossa määritellään nk. C-SCRM-ohjelma, eli Cybersecurity Supply Chain Risk Management

C-SCRM lähtee siitä, että organisaation näkymä toimitusketjussa muuttuu sitä sumeammaksi, mitä kauempana verkostossa toimija on. Perusideana onkin, että sinänsä C-SCRM on normaalia kyberturvallisuuden riskienhallintaa, mutta tiedostetaan se, että omat asiakkaat asettavat omalle toiminnalle erilaisia velvoitteita, ja toisaalta pyritään valvomaan omien alihankkijoiden toimintaa, mukaanlukien toimitusketjun riskienhallinta.

C-SCRM:n juuret ovat ohjelmistoteollisuuden toimitusketjujen hallinnassa, mutta siitä on kehitetty paljon yleisempi versio. C-SCRM perii paljon NISTin 800-53-suosituksesta (joka on ISO 27001:n kaksonen), ja sisältää perusteellisen ohjauksen toimitusketjun kyberturvallisuuden hallinnasta.

Kontrollien suosituksessa C-SCRM:ssä on ensin tunnistettu ne perustietoturvan kontrollit, jotka pätevät myös toimitusketjujen

riskienhallinnassa, ja selitetty Kuinka niitä tulisi käyttää SCRM:ssä. Tämän lisäksi esitellään uusia kontrolleja:

- MAINTENANCE MONITORING AND INFORMATION SHARING (MA-8): Kontrolli: organisaatio valvoo järjestelmiensä ja komponenttiensa tilaa, ja tiedottaa riskirajat ylittävät toiminnot omalle toimittajaverkostolleen.
- SUPPLIER INVENTORY (SR-13) Kontrolli: Organisaation tulee tuottaa lista ensimmäisen tason toimittajistaan, jotka voivat tuottaa kyberriskejä toimitusketjussa

Erityisiä kohteita, joita alihankkijoilta voidaan vaatia, on ohjelmistokomponenttien haavoittuvuushallinta ja koko toimitusketjun kattava identiteetin- ja pääsynhallinta.

Toimitusketjujen hallinta tulisi ottaa osaksi organisaation kokonaisriskienhallintaa.

C-SCRM tunnistaa organisaatiolle tiettyjä avainkäytänteitä kyberturvallisuuden hallinnan toteuttamiseksi, ja jakaa ne kolmeen “kypsyys”tasoon: perusta (foundational), ylläpito (sustaining) ja kehittyvä (enhancing). Tasot mukailevat yleisiä organisaation kypsyystasoja: alimmalla on kriittiset elementit, jotta kyberturvallinen toimitusketjujen luottamussuhteiden luominen on ylipäätään mahdollista, ja päättyy korkeimmalla tasolla adaptiiviseen ja mitattuun toimintamalliin.

Toimitusketjuturvallisuuden muuta ohjeistusta

Standardi	Kuvaus
ISO 20243	ICT-sovellusten toimitusketjuille tarkoitettu. Suosituksia ICT-laitteiston ja sovellusten eheydelle.
ISO-28004-2	Yleinen ohjeistus SME:lle (Small and Middle-sized Enterprises) toimitusketjun turvallisuuden takaamiseksi
SAE AS5553D	Ilmailualalle tarkoitettu standardi elektroniikkaosien toimittajien hallintaan, hankintaan, jäljitettävyyteen ja valvontaan
SAE AS6081A	Kuten AS5553D, mutta kohdistettu avoimilta markkinoilta tapahtuvaan hankintaan
SAE ARP6178A	Riskinarviointityökalu väärennettyjen elektroniikka komponenttien varalta ilmailualalle
SAE ARP9134A	Yleinen ohjeistus toimitusketjujen riskinhallintaan (ilmailualalle räätälöity)
UL 2900-2-2	UL (Underwriters Laboratories) Solutions LLC on USA:ssa toimiva käyttöturvallisuuden standardointi ja evaluointitaho. 2900-standardisarja määrittelee yleisiä varusohjelmistojen turvallisuusvaatimuksia ml. softankehityksen toimitusketju. Osa 2-2 antaa teollisuusautomaatiokohtaisia vaatimuksia

Toimitusketjujen turvallisuuden varmistamiseksi on muutakin ohjeistusta esim. ISO:lta. SAE standardoi ilmailualan turvallisuutta, ja keskittyy toimitusketjun hallinnassa pääasiassa väärennettyjen komponenttien havaitsemiseen ja niiden aiheuttaman riskin käsittelyyn. Tästä huolimatta, monet siellä esitetyt kontrollimekanismit pätevät liiketoimintaprosesseissa yleisemminkin toimitusketjun riskienhallintaan.