Mitä EU:n kyberkestävyyssäädös merkitsee yrityksille, kommenttipuheenvuoro

Jussi Leppälä, 2024-01-23

Kyberala murroksessa -seminaari

Valmet

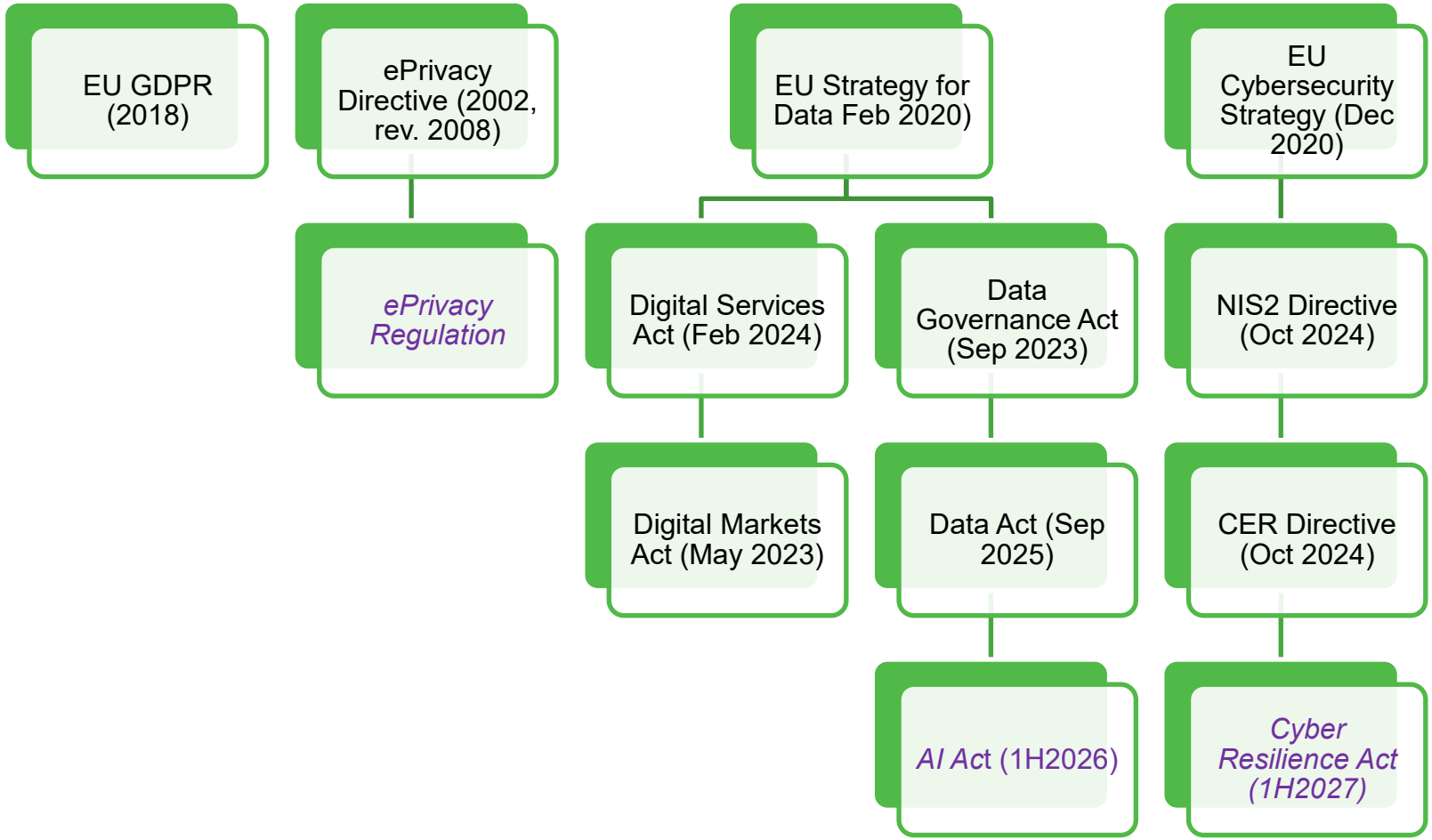
Valmet

- Johtava prosessiteknologian, automaatioratkaisujen ja palvelujen toimittaja ja kehittäjä sellu-, paperi – ja energiateollisuudelle. Automaatiojärjestelmillä ja virtauksensäätöratkaisuilla Valmet palvelee vielä laajempaa prosessiteollisuuden asiakaskuntaa
- Liikevaihto 2022 5 074 milj. euroa. 17 548 työntekijää ympäri maailmaa.
- Valmetin automaatioratkaisut ulottuvat yksittäisistä mittauksista tehdaslaajuisiin prosessiautomaatiojärjestelmiin.
- Automaatiojärjestelmät ja palvelut on suunniteltu maksimoimaan asiakkaiden liiketoimintojen kannattavuutta ja vastuullisuutta tehostamalla raaka-aineiden kestävää käyttöä sekä parantamalla tuotannon suorituskykyä, laadunhallintaa, energiatehokkuutta ja kustannustehokkuutta

Sisältö

- Säätely-ympäristö
- Sovellusala
- Keskeiset vaatimukset

EU:n data- ja digisäätelyä

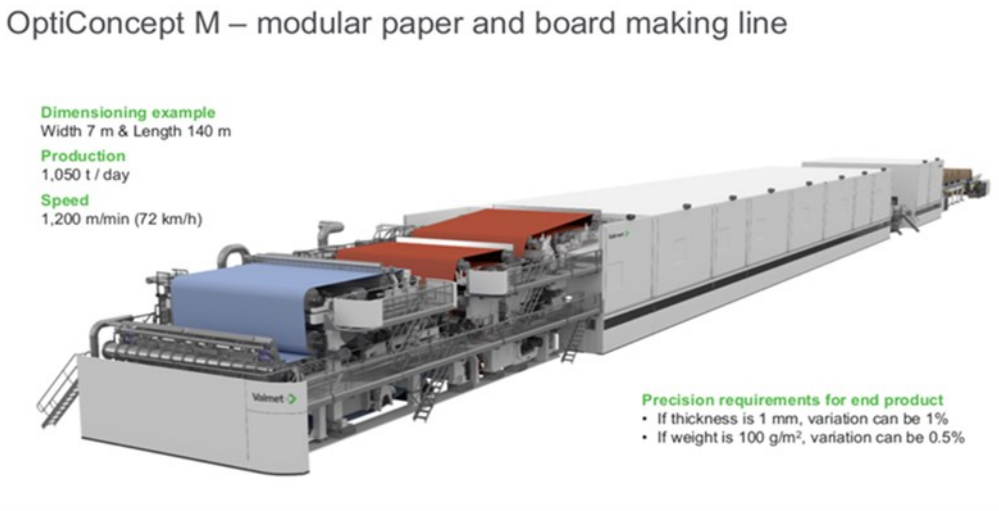


EU:n kyberturvallisuutta koskevaa säätelyä

- Kyberturvallisuusasetus (EU) 2019/881
  - Säätää Euroopan unionin kyberturvallisuusvirasto ENISAn asemasta sekä kyberturvallisuussertifioinnista
- NIS2-direktiivi, (EU) 2022/2555
  - Jäsenvaltiot ja kriittiset toimijat
- Direktiivi kriittisten toimijoiden häiriönsietokyvystä, CER, (EU) 2022/2557
- Alakohtaista säätelyä
  - Asetus finanssialan digitaalisesta häiriönsietokyvystä DORA, (EU) 2022/2554
  - Radiolaitedirektiivi, 2014/53/EU
  - Asetus lääkinnällisistä laitteista, 2017/745/EU
  - …
- Tulevaa liittyvää säätelyä
  - Tekoälysäädös, COM(2021) 206
  - Datasäädös, (EU) 2023/2854
  - Asetus konetuotteista, (EU) 2023/1230

Kyberkestävyyssäädös, sovellusala

- *Sovelletaan kaikkiin digitaalisia elementtejä sisältäviin tuotteisiin, joiden aiottu tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai epäsuoran loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon*
  - *Automaatiojärjestelmät, teolliset venttiilit, Valmetin teollinen internet?*
- Sovellusala on erittäin laaja, vaikka puhtaat SaaS-palvelut eivät ole säädösehdotuksen piirissä.
  - Avoimen lähdekoodin komponentteja koskevat rajoitetut velvoitteet
  - Johdanto-osan kohta 9 täsmentää, että puhtaat SaaS-palvelut eivät kuulu säädöksen piiriin. Sellaiset tuotteeseen liittyvät pilvipalvelut (tai ”etäkäsittely”) taas kuuluvat, joiden puuttuminen estäisi tuotteen suorittamasta jotain toimintoaan



Keskeisimmät vaatimukset

Digitaalisia elementtejä sisältävien tuotteiden tulee täyttää ”*olennaiset kyberturvallisuusvaatimukset*”, jotka on esitetty liitteessä 1:

- Riskipohjainen lähestymistapa
- Tuotteet on toimitettava ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia
- Vaatimuksia koskien tehdasasetuksia, käyttäjänhallintaa, salaamista, tiedon eheyttä, tietojen minimointia, toimintojen saatavuutta, hyökkäyspintojen minimointia, lokitusta ja tietoturvapäivityksiä

Valmistajan tulee lisäksi täyttää ”*haavoittuvuuksien käsittelyä*” koskevat vaatimukset liitteessä 1:

- Dokumentointi, korjaus, testaus, ilmoittamisen periaatteet ja ohjeet, tietoturvapäivitysten maksuton jakelu

Käyttäjien informointi

- Yhteystiedot, versiotiedot, käyttötarkoitus, käyttöolosuhteet, ohjelmistosisältöluettelon saatavuus, vaatimustenmukaisuusvakuutus, valmistajan tietoturvatuki, ohjeistus

Valmistajien raportointivelvollisuudet

- *Valmistajan on ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun se on tullut asiasta tietoiseksi, ilmoitettava samanaikaisesti kansalliselle CSIRT-yksikölle ja ENISAlle kaikista digitaalisia elementtejä sisältävän tuotteen sisältämistä aktiivisesti hyödynnetyistä haavoittuvuuksista.*
- *Valmistajan on ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun se on tullut asiasta tietoiseksi, ilmoitettava kaikista digitaalisia elementtejä sisältävän tuotteen tietoturvaan vakavasti vaikuttavista poikkeamista.*
- Ennakkovaroituksen lisäksi on 72 tunnin kuluttua jätettävä varsinainen ilmoitus ja lopullinen raportti 14/30 päivän kuluttua siitä, kun haavoittuvuuden korjaava tai lieventävä toimenpide on saatavilla tai siitä, kun poikkeamailmoitus on tehty
- Käyttäjien informointi

Maahantuojien ja jakelijoiden velvollisuudet

Maahantuojien pitää huolehtia siitä, että tuote täyttää säädöksen vaatimukset mukaan lukien CE-merkintä ja tarvittava dokumentaatio ja ohjeet käyttäjän ja viranomaisen helposti ymmärtämällä kielellä. Maahantuojan on lisäksi annettava omat yhteystietonsa.

Jakelijan taas tulee puolestaan tarkastaa, että valmistaja ja maahantuoja ovat huolehtineet omista velvoitteistaan

Maahantuojiin ja jakelijoihin sovelletaan valmistajiin kohdistettuja velvoitteita, jos ne tuovat tuotteen markkinoille omalla nimellään tai tekevät siihen merkittäviä muutoksia

Kriittisyysluokitus

Tavalliset digitaalisia elementtejä sisältävät tuotteet (~90% kaikista tuotteista)

Tärkeät tuoteryhmät, luokka I

- Selaimet, virustentorjuntaohjelmistot, SIEM-järjestelmät, käyttöjärjestelmät, mikroprosessorit, -kontrollerit, ASICit ja FPGA-piirit, joissa on turvallisuusominaisuuksia

Tärkeät tuoteryhmät, luokka II

- Virtualisointijärjestelmät, palomuurit

Kriittisten tuotteiden ryhmät

- Älykortit, älykkäät mittausjärjestelmät (sähköverkossa, kuten määritelty direktiivissä (EU) 2019/944

Vaatimustenmukaisuuden osoittaminen

- Tavalliset digitaalisia elementtejä sisältävät tuotteet
  - Itsearviointi, EU-vaatimustenmukaisuusvakuutus (CE-merkintä)
  - Yhdenmukaistetut standardit tai komission spesifikaatiot (”eritelmät”)
- Tärkeät tuoteryhmät, luokka I
  - Standardinmukaisuus, yhteisten eritelmien tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän noudattaminen tai EU-tyyppitarkastusmenettely tai täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuusarviointi
- Tärkeät tuoteryhmät, luokka II
  - EU-tyyppitarkastusmenettely tai täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuusarviointi
- Kriittisten tuotteiden ryhmät
  - Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän noudattaminen tai jos sellaista ei ole, niin EU-tyyppitarkastusmenettely tai täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuusarviointi

Seuraamukset ja siirtymäajat

- Liitteen 1 oleellisten kyberturvallisuusvaatimusten ja 10 ja 11 artiklassa säädettyjen velvoitteiden täyttämättä jättämisestä on määrättävä hallinnollinen sakko, 15 M€ tai enimmillään 2,5 % maailmanlaajuisesta liikevaihdosta
- Muista rikkomuksista 10 M€ tai 2 %
- Puutteellisten tai harhaanjohtavien tietojen toimittamisesta viranomaisille 5 M€ tai 1 %
- Soveltaminen aloitetaan 36 kuukauden kuluttua voimaantulosta, artiklan 11 (raportointi) soveltaminen 21 kuukauden kuluttua

Miten valmistautua?

- Suurimmat velvoitteet kohdistuvat valmistajiin
- Tunnetun kyberturvallisuusstandardin noudattaminen tullee tarjoamaan hyvän pohjan vaatimustenmukaisuudelle
- Dokumentointi ja yhteydenpito tulee teettämään paljon töitä
- Raportointivaatimuksissa on lyhyempi siirtymäaika mutta nekin edellyttävät muutoksia toimintatapoihin


Valmet
FORWARD