Till regeringskansliet Dnr V-2022-0730

Remiss av Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020, I2022/01758

Med reservation för vissa element rörande fri och öppen källkod som vi diskuterar närmare i denna remiss kan KTH tillstyrka förordningen. Det är särdeles angeläget att stärka skyddet mot cyberangrepp i största allmänhet, och det är helt rätt att supplera NIS2 direktivet genom obligatoriska åtgärder som riktar sig mot alla företag som producerar, distribuerar, eller marknadsför ”produkter med digitala element” på den inre marknaden. Vi ser även positivt på att förordningen inkluderar livscykelaspekter, särskilt hanteringen av sårbarheter.

Förordningen som den är utformad har potential att få betydande positiv inverkan på läget inom cyberområdet, dels tack vara obligatoriet, dels via hotet om sanktioner (upp till 2,5% av årsomsättningen).

Dock finns det även betydande skäl för pessimism. Branschen har under många år vant sig vid en modell där mängder med kända och okända sårbarheter rutinmässigt lämnas utan åtgärd. En systematisk hantering av sådana sårbarheter i ett typisk större programsystem kommer sannolikt att kräva investeringar som vida överskrider möjliga sanktionskostnader.

Samtidigt kan sanktionshotet visa sig problematisk för fri och öppen källkod (FOSS = Free and Open Source Software) miljön på flera sätt, som påpekas i [1]. Producenter av FOSS är en blandad skara, och spänner från IT-industrins giganter till enskilda utvecklare som underhåller viktiga programpaket, ibland på ren hobbybasis. Historisk har FOSS, inte minst genom forskarvärlden, spelat en helt avgörande roll i utvecklingen av internet och webben, och dess betydelse för industrin ökar snarare än minskar. Detta reflekteras även av EU kommissionens strategi för öppen källkod 2020-2023 [2]. Med tanke på FOSS ekosystemets betydelse för innovationstakten i samhället är det därför av stor vikt att inga onödiga hinder ställs i vägen för dess vidare utveckling. Hotet om sanktioner, till exempel, kan visa sig ödeläggande för små oberoende producenter, och i värsta fall kan det resultera i att FOSS-miljön fragmenteras, till exempel genom att tillgänglighet till repositorier som Github begränsas geografisk eller genom licensvillkor.

Frågan är vilka krav som med rimlighet kan ställas på öppen programvara som är fri att användas och potentiellt modifieras kostnadsfritt av vem som helst. Bör principen när det gäller FOSS inte vara att det är den kommersiella avnämaren snarare än utvecklaren som bör ha det juridiska ansvaret för FOSS programvarans säkerhet? En sådan princip ger den kommersiella aktör incitament att själva, direkt eller indirekt, bidra till FOSS produktens kvalité, vilket är positivt.

Visserligen föreslås i inledningen till förordningen, pkt. 10, att ”fri programvara med öppen källkod som utvecklas eller tillhandahålls utanför ramen för kommersiell verksamhet inte omfattas av denna förordning.” Som [1] påpekar borde en sådan rekommendation inkluderas som en artikel i själva förordningen, om undantaget ska ha verkan. Ett större problem är kanske att begreppet ”kommersiell verksamhet” är otydligt, och en för bred tolkning kan visa

sig kontraproduktiv, särskilt för små utvecklare med begränsade resurser och för kritiska produkter som i flertalet fall distribueras som fri källkod.

Det bör även noteras att det inte finns någon tradition i FOSS miljön att skilja på kommersiell och icke-kommersiell verksamhet. Det finns många exempel där delning av källkod kan ge fördelar i termer av kvalité, säkerhet och underhåll som ofta visar sig uppväga det kommersiella incitamentet att undanhålla koden.

Vårt förslag därför är att FOSS produkter helt undantas från denna förordning.

Detta kan få som konsekvens att produkter marknadsförs utan essentiell säkerhetskritisk mjukvara, men nedladdningsbart från en FOSS distributör som Github. Vi ser dock detta som ett mer marginellt problem som bör kunna hanteras genom passande lagstiftning.

Ett relaterat problem rör distributionen av FOSS, till exempel genom plattformar som Github, Sourceforge o.a. Enligt art. 14.2 skall en distributör, innan en produkt som omfattas av förordningen görs tillgänglig på marknaden, säkra att produkten är försedd med CE märkning, och att kraven i 10.10, 10.11 och 13.4 uppfylls. De senare kraven rör i huvudsak tillgång till instruktioner i lättillgänglig form och språk, och att en EU-försäkran om överensstämmelse med förordningen är tillgänglig. I motsats till [1] läser vi inte dessa krav som krav på distributören att själva validera överenstämmelse. Vårt förslag är att distributionen av FOSS produkter utgår från bestämmelserna i art. 14.

Rörande certifiering har detta, särskilt i de fall där tredjepartsbedömningar är nödvändiga, historiskt visat sig kostsamt och i många fall av tveksamt värde. Kraven är uppdelade i tre klasser där klass I och klass II täcker säkerhetskritiska produkter. Vi noterar att uppdelningen mellan produkter i klass I och klass II inte är helt tydlig i alla delar. Allmänt är det vår åsikt att kommissionen har hittat en lämplig balans mellan kritikalitet och krav på certifiering. Det är rätt att undvika krav om tredjepartsbedömningar även för klass I produkter, om EU-harmoniserade processer eller system för certifiering använts. I linje med våra rekommendationer förordar vi att FOSS produkter undantas från krav om certifiering.

KTH:s beredning av ärendet

Ärendet har handlagts av Mads Dam, professor i teleinformatik, vid skolan för elektroteknik och datavetenskap med kommentarer från kolleger vid institutionen för datavetenskap.

Stockholm 2023-02-13

Anders Söderholm
Rektor

Referenser

[1] Olaf Kolkman: The EU's proposed cyber resilience act will damage the open source ecosystem. Internet Society blog post 24 Oct. 2022, URL: https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/. Retrieved 2 Feb 2023

[2] The European Commission: Open-source software strategy 2020-2023. URL: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en. Retrieved 2 Feb 2023.