2023-02-21

Yttrande över EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

Sammanfattning

Vi har tagit del av förordningen och instämmer med att det är en viktig uppgift att ta fram ett regelverk runt cyber-säkerhet för digitala produkter. Förslaget tar ett bra steg framåt i den riktningen och kan leda till betydligt säkrare produkter och öka medvetandegraden hos både tillverkare och användare. Vårt fokus har varit att kommentera på och ge förslag på förbättringar, inte att lyfta fram det som är bra i förordningen. Vi har en del tankar och förslag som kan föra arbetet ännu ett steg fram och som vi bedömer är värda att fundera över innan förordningen blir skarp.

Det övergripande problemet med förordningen, vilket inte är helt lätt att adressera, är att man överlåter största delen av säkerhetsarbetet till tillverkarna (eller importörer/distributörer). Kundens eller produktens miljö tar man inte hänsyn till och det ställs inga krav på vilken säkerhetsnivå olika kategorier av kunder bör eller måste eftersträva. Jämför man dessutom med krav och standarder från närliggande produktområden, t.ex. från Internet-uppkopplade fordon, så har man här en väldigt förenklad modell och som kanske till och med kan beskrivas vara en naiv approach. Nedan följer lite mer detaljerade kommentarer på förordningen.

Certifiering av kritiska produkter

Det är lite förvånande varför en förordning som denna inte nämner eller relaterar till existerande certifiering av säkerhetsprodukter. Det finns sedan många år tillbaka en certifieringsprocess och etablerade certifieringsorgan för produkter med avseende på säkerhet, Common Criteria (CC) https://www.commoncriteriaportal.org.

Där finns möjligheten för tillverkare att certifiera sina produkter på 7 olika nivåer beroende på vilken säkerhetsnivå man anser att en produkt ska ha, och det finns redan utsedda nationella certifieringsorgan. Det kan mycket väl vara så att det finns skäl till att inte snegla på CC eller att använda denna existerande infrastruktur, men i så fall bör skälen framgå i förordningen.

Vad som speciellt skiljer Artikel 6 i den här förordningen mot CC är att i CC certifierar tillverkare sin produkt på en viss nivå och sedan kan myndigheter och organisationer själva ställa krav på vilken certifieringsnivå som krävs för användning i olika miljöer. Detta löser problemet med att tillverkarna behöver förutse hur produkterna kommer att användas. Ett liknande förfarande skulle kunna användas här.

I CC har man redan tagit fram gemensamma ”protection profiles”, alltså harmoniserade säkerhetskrav som gäller för vissa produktkategorier. Brandväggar har till exempel en sådan profil som anger dom grundläggande kraven man måste kunna ställa. Tillverkare kan även lägga till egna

DEPARTMENT OF Computer Science and Engineering
Chalmers University of Technology
SE- 412 96 Gothenburg, Sweden
+46 31-772 10 00
Tomas.olovsson@chalmers.se
www.chalmers.se

Chalmers University of Technology
Corporate Identity No: 556479-5598

CHALMERS
UNIVERSITY OF TECHNOLOGY

kriterier som dom väljer att få certifierade om dom anser att en produkt är bättre än standardkraven. Då blir det inte en fråga om att lova så lite som möjligt för att slippa skadeståndsanspråk vilket den här förordningen skulle kunna resultera i, utan antingen så uppfyller man kraven för en viss nivå, eller inte.

Sedan certifieras produkten och ju högre certifieringsnivå man väljer, desto rigidare bevis måste man presentera för att (och hur) man klarar dessa uppsatta säkerhetskrav. Exempelvis kräver nivå 1 bara ett funktionstest av produkten, nivå 4 kräver bevis för en metodisk design och nivå 7 en formellt bevisad design, något som är mycket komplicerat och kostsamt och som bara kan göras för mycket små moduler.

Denna metodik med många olika nivåer av certifiering bör övervägas även här, speciellt för kritiska produkter kategori II där förordningen ju faktiskt anger att någon form av tredjepartsgranskning bör ske. Varför inte utnyttja att CC redan har färdiga krav på många produkter i sina protection profiles? Här finns även godkända nationella certifieringsorgan i dom flesta länder inom EU.

Motivering punkt 22 (sid 19): ”*… bör väsentliga krav ställas på sådana produkter*”. Vem ställer kraven? Hur heltäckande ska dom vara? Hur säkerställer man att det blir samma krav på likartade produkter från olika tillverkare/leverantörer och länder? Vem ansvarar för att ta fram krav? Pratar men om tekniska krav bör man titta på protection profiles i CC.

Artikel 23.2.b säger ”*överensstämmelse som grundar sig på fullständig kvalitetssäkring*”. Vad är fullständig kvalitetssäkring om man jämför med CC:s 7 olika nivåer?

Slutsats: Även om man väljer att inte gå samma väg som CC med att ställa krav på både produkter och miljöer, så anser vi att det bör finnas en motivering till varför man valt en annan väg i förarbetet till förordningen.

Övriga kommentarer i prioritetsordning

Hot- och riskanalys

Normalt genomför företag som har mer kritisk verksamhet en TVRA-analys (Threat – Vulnerabiltiy – Risk analysis) när man utvärderar säkerheten. Det finns ett antal standardiserade metoder för utvärdering och gemensamt för dom alla är att man blandar in miljön där produkten kommer att användas i analysen. Det är många faktorer som avgör om en produkt är säker att använda, exempelvis vilka *hot användaren* kan tänkas utsättas för, vilken *miljö* den används i, vilka *funktioner* eller data den hanterar, *var den sitter* i ett nätverk, hur *mogen* organisationen är att hantera produkten, hur *tillgänglig* produkten är för angripare, vilka *attackmöjligheter* som erbjuds angripare, vilken *kunskap* som krävs av en angripare, vilken *skada* ett säkerhetsproblem kan orsaka, etc. Det här tänket finns inte i förordningen utan den fokuserar enbart på produkten och tillverkaren och överlåter hela analysen på denne, vilket i de flesta fall är omöjligt.

DEPARTMENT OF Computer Science and Engineering
Chalmers University of Technology
SE- 412 96 Gothenburg, Sweden
+46 31-772 10 00
Tomas.olovsson@chalmers.se
www.chalmers.se

Chalmers University of Technology
Corporate Identity No: 556479-5598

Olika typer av angripare

Förordningen nämner inte vilken eller vilka typer av angripare som produkter ska klara av att skydda sig mot. Vad är "*tillräckligt*" säker? Kommer tillverkaren och kunden att ha samma perspektiv? Rimligen kan tillverkaren inte heller *förhindra säkerhetsincidenter* som föreskrivs i Artikel 10.2. Det är stor skillnad mellan en hur lång tid systemet kan motstå en medioker angripare, en duktig hacker, en angripare med specialistkompetens eller en statlig organisation med i stort sett obegränsade resurser. Behöver alla produkter klara alla kategorier av angripare? Förordningen bör nog ha ett antal standardiserade säkerhetshot/angripare som tillverkarna kan ange att produkten designats för vilket kan hjälpa till att enligt Bilaga V i förordningen kunna "*beskriva cybersäkerhetsrisker mot vilka produkten utformats och utvecklats*".

Avsedd användning av produkt och restriktiva beskrivningar

Enligt Artikel 5 så får produkter med digitala element "*endast tillhandahållas på marknaden om de uppfyller de väsentliga kraven i avsnitt 1 i bilaga I, förutsatt att de är korrekt installerade och underhållna och används för avsett ändamål …*". Detta är bra eftersom det tvingar tillverkare att specificera under vilka omständigheter en produkt är tänkt att användas. Det ger också *den kunnige* användaren hjälp att mycket grovt bedöma vad man får för säkerhetsnivå med produkten.

Förordningen ger dock ingen mer vägledning än att Artikel 10.2 säger att *"tillverkarna ska göra en bedömning … för att minimera cybersäkerhetsriskerna, förhindra säkerhetsincidenter … och minimera konsekvenserna*." Men vad är acceptabel risk, kan en tillverkare avgöra vad som är acceptabel risk för en användare som använder den i för tillverkaren okänd miljö? Ta t.ex. ett kassasystem, det ställs rimligen olika säkerhetskrav beroende om det är en lokal tidningsbutik eller en stor kedja som ICA eller Coop som använder systemet. Det sistnämnda kan påverka hela samhället om systemet angrips och sätts ur funktion. Det som saknas i förordningen är krav på vilken typ av produkt som krävs av användarna. Att säga att båda ska använda sig av en kategori II produkt är för trubbigt.

Det är även svårt för en tillverkare att specificera vad "avsett ändamål" ska vara. Hur ska det beskrivas för en switch (växel), en uppkopplad lampa, en fjärrstyrd värmepanna för hem och/eller industribruk, en elmätare, en mobiltelefon som kanske kan bli uppkopplad mot en server på ett kärnkraftverk eller en dator med Windows? Varje tillverkare måste då beskriva i detalj hur den får användas och i vilka miljöer. Det finns en reell risk att tillverkare kommer att vara väldigt restriktiva i sina beskrivningar för att ha ryggen fri för ev. skadestånd eller indragna produkter. Därmed blir det slutanvändarnas problem att välja bland produkter som avsäger sig de mesta vad gäller säkerhet genom att kräva att dom bara används i slutna miljöer där dom i teorin inte skulle kunna orsaka skada. Alltså något liknande de skrivningar som används i licensvillkor för programvara där man explicit avsäger sig allt ansvar.

Ett steg mot en lösning på de här problemen kan som tidigare nämnts vara att vissa typer av *verksamheter ska ha krav på sig* som reglerar vilka produkter de får använda. Så är fallet idag inom vissa kritiska områden där man måste använda sig av certifierade produkter enligt Common Criteria, exempelvis inom telekom- och försvarsindustri där vissa system kräver en certifiering på en viss miniminivå. Detta adresseras inte av den här förordningen.

DEPARTMENT OF Computer Science and Engineering
Chalmers University of Technology
SE- 412 96 Gothenburg, Sweden
+46 31-772 10 00
Tomas.olovsson@chalmers.se
www.chalmers.se

Chalmers University of Technology
Corporate Identity No: 556479-5598

Kategorier av produkter, tekniska krav

Produkter delas upp i kritiska produkter klass I, klass II samt övriga produkter. Kritiska produkter är dom flesta nätverksprodukter men det saknas tekniska krav i förordningen. Vad skiljer tekniskt mellan exempelvis en brandvägg i klass I från en i klass II? Vad är det för ytterligare funktioner som krävs för industriellt bruk? Det finns naturligtvis många tänkbara funktioner såsom stöd för centraliserade larmfunktioner, mer avancerad intrångsdetektering, osv, men förordningen ger ingen vägledning. Är det upp till tillverkaren att välja funktioner som ska finnas för att passa i klass I eller II? Vem ställer i slutändan tekniska krav på produkterna? Åter igen, jämför med CC och deras protection profiles. Kanske är det det som avses i förordningen med ”harmoniserade krav”? Det framgår i så fall inte vem som ansvarar för att ta fram dessa.

Testning och standarder

Det framgår inte i förordningen i vilken grad och på vilket sätt tillverkare ska (måste) testa sina produkter. Man kan tänka sig allt från ett ”normalt” funktionstest av den färdiga produkten till att även inkludera s.k. boundary value analysis, condition testing, branch/decision testing, test coverage, unit testing och dessutom i olika grad göra penetrationstester. Vad krävs av tillverkarna för de olika produktkategorierna? Hur långt behöver man gå för att undvika skadeståndskrav? Vem avgör i slutänden vad som ska anses vara tillräckligt?

Det är även intressant att jämföra den här förordningen och dess cybersäkerhetskrav med vad som nyligen tagits fram gällande cybersäkerhet för uppkopplade fordon. Där har man arbetat med liknande säkerhetsproblem och standardiserat hur arbetet ska gå till. Det har resulterat i en betydligt mer komplex standard (influerad av CC) och man kan fråga sig om det är görligt att förenkla arbetet till den grad som är gjort här. Två närliggande standarder vi föreslår bör studeras:

ISO/SAE 21434: Road vehicles – Cybersecurity engineering
SAE J3061: Cybersecurity Guidebook for Cyber-Physical vehicle systems

Det är visserligen så att man ställer högre krav i dessa standarder än vad som kanske är rimligt här, men metodiken och approachen till hur man bygger säkra produkter är intressant liksom hur man kräver att man gör riskanalys, design och testning. Nu kan det vara så att man redan analyserat dessa standarder och har bra argument för att inte gå den vägen, men i så fall bör man nämna detta i förarbetet. Som det ser ut nu så ger förordningen intrycket av att man inte studerat närliggande områden och helt ignorerat relaterade ISO-standarder för cybersäkerhet.

Produkter och produktens livslängd

Artikel 10.12 anger att man ska underhålla produkten *”under hela förväntade livslängden eller under en femårsperiod från utsläppandet på marknaden beroende på vilken period som är kortast*.” Det lämnar det öppet för tolkning av tillverkaren och svårtolkat för kunden:

DEPARTMENT OF Computer Science and Engineering
Chalmers University of Technology
SE- 412 96 Gothenburg, Sweden
+46 31-772 10 00
Tomas.olovsson@chalmers.se
www.chalmers.se

Chalmers University of Technology
Corporate Identity No: 556479-5598

1. Vad är förväntad livslängd? För programvara, är det ok att anse att version 1.0 har nått end-of-life när version 1.1 kommer ut? Eller måste man på förhand deklarera ett utgångsdatum liknande det som Microsoft gör för t.ex. Windows 10? Detta framgår inte av förordningen.

2. Många programvaror kräver supportavtal eller att kunden betalar för uppgradering till nästa version. Kan man kräva att få gratis support på tidigare versioner? Förordningen nämner inget om kostnader för underhåll och om det är tillåtet. Är kundens eller tillverkarens / importörens / distributörens fel att produkten inte uppdateras om där finns en kostnad kopplad till det?

3. Räcker det att en tillverkare deklarerar att end-of-life för en produkt inträffar ”när nästa modell kommer ut på marknaden”, något som är vanligt för många produkter (exempelvis navigatorer)? Därefter erbjuds inga uppdateringar med mindre än att man köper en helt ny produkt. Det är dessutom omöjligt för kunden att veta när nästa version kommer ut på marknaden så man kan inte heller bedöma hur lång support man kan tänkas få.

4. Minst en mobiltelefontillverkare garanterar idag uppdateringar till en modell i tre år från det att den släppts på marknaden. Det betyder att den som köper produkten mot slutet av produktionstiden riskerar att inte få några uppdateringar alls. Är det kundens uppgift att ta reda på när produkten lanserades? Är detta förenligt med förordningen? Tycker inte att det framgår i förordningen hur tydligt end-of-life ska beskrivas.

Undantagna produkter

Är det rimligt att kräva att alla produkter med digitala element ska kunna uppdateras? Det lägger ett stort ansvar hos tillverkarna på att implementera ett för slutkunden användbart system för fjärruppdatering. Detta kommer att vara kostsamt, inte minst för små och billiga prylar. Men det kräver också att slutkunden förstår, kan och bryr sig om att uppdatera. Kanske kan man tänka sig undantag för uppdateringar om produkten anses tillräckligt bra vid lansering? Men det finns i förordningen inget utrymme för undantagna produkter. Det kommer helt säkert att komma krav på att undanta vissa produkter från att kunna bli uppdaterade, åtminstone om dom är enkom för hemmabruk. Förordningen bör kanske ta höjd för detta och flagga redan nu för att undantag kan bli aktuella och ha en lista som uppdateras på samma sätt som man gör för produkter som ska klassas som kritiska.

I tjänsten
Tomas Olovsson, handläggare
Tomas.olovsson@chalmers.se
+46 31 772 1000

DEPARTMENT OF Computer Science and Engineering
Chalmers University of Technology
SE- 412 96 Gothenburg, Sweden
+46 31-772 10 00
Tomas.olovsson@chalmers.se
www.chalmers.se

Chalmers University of Technology
Corporate Identity No: 556479-5598

CHALMERS
UNIVERSITY OF TECHNOLOGY