Myndigheten för samhällsskydd och beredskap

Remissvar

Datum
2023-02-08

Ärendenr
MSB 2022-14546

Ert datum
2023-02-21

Er referens
I2022/01758

Enheten för strategi och samordning (CS-ST)
Martin Snygg
010-240 4493
martin.snygg@msb.se

Regeringskansliet
Finansdepartementet
i.remissvar@regeringskansliet.se
i.esd.remisser@regeringskansliet.se

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

Sammanfattning

MSB ställer sig övergripande positivt till förslaget att skapa förutsättningar för utveckling av säkra produkter med digitala inslag genom att försäkra att hård- och mjukvara placeras på marknaden med färre sårbarheter och att tillverkare tar större ansvar för produkters cybersäkerhet genom deras livscykel.

Vi anser dock att det för den marknadskontrollmyndighet som ansvarar för uppföljning och kontroll av regelefterlevnad tydligt framgår att en samordning med MSB är av stor vikt då redan upparbetade samverkansformer mellan ENISA, som ansvarar för att ta emot rapporter om aktivt utnyttjade sårbarheter som omfattas av förordningen, och MSB redan är implementerade i enlighet med NIS-direktivet.

MSB anser även att det är synnerligen viktigt att analysera eventuell överlappning av annan angränsande lagstiftning på området som nu är i olika steg i lagstiftningsprocessen för att undvika dubbelreglering av sektorer. Väsentligt blir därför att föreslagen förordning revideras så att den kompletterar befintlig lagstiftning, och inte överlappar den. Inte minst bör detta säkerställas i förhållande till NIS2-direktivet.

Synpunkter på förslaget

MSB anser det oklart gällande den rapportering som framgår av artikel 11 i föreslagen förordning om den rapportering som ska äga rum vid en produktincident med cyberinslag, ska ske inom 24 timmar till ENISA och till nationell CSIRT-enhet samt även till berörd marknadskontrollmyndighet. Utöver den otydlighet som ligger i att en och samma produkt kan komma att behöva rapporteras till flera organ, finns en uppenbar risk att nationell säkerhet kan äventyras när rapportering i första hand och på kort tid ska gå utanför landets gränser. Förslagsvis bör det tydligt framgå i förordningen att varje medlemsstat ges en rimlig möjlighet att först bedöma om de uppgifter som ska rapporteras in till ENISA berör nationell säkerhet, försvar, militära ändamål eller säkerhetsskyddsklassificerade uppgifter och om så är fallet hantera rapporteringen enligt nationell praxis. Det skulle sannolikt också underlätta för den enskilde med en rapporteringsväg.

Ur ett nationellt perspektiv vill man även undvika en situation där ENISA får information om eventuella sårbarheter i svenska verksamheter som inte vår nationella CSIRT-enhet har tagit del av.

I bilaga I, avsnitt två framgår de krav på sårbarhetshantering som ställs på tillverkare av produkter med digitala element.

I punkterna (2) samt (8) framgår att tillverkarna utan dröjsmål ska åtgärda och avhjälpa sårbarheter, exempelvis genom att fram och sända ut säkerhetsuppdateringar. MSB ser här ett behov av att göra en distinktion mellan kritiska och övriga säkerhetsuppdateringar. Skälet till det är att sårbarheter ofta upptäcks genom att organisationer blir varse att hotaktörer har hittat ett sätt att utnyttja produkter med it-funktionalitet som organisationen använder eller tillhandahåller, på otillåtna sätt och i antagonistiska syften. Sårbarheten upptäcks därmed indirekt, genom att man upptäcker att den redan utnyttjas. Den som arbetar med samordnad delgivning av information om sårbarheter ställs då inför valet att antingen snabbt dela information om sårbarheten och eventuell tillgänglig säkerhetsuppdatering, eller att invänta en tidpunkt (dag) då man vet att många organisationer ändå genomför uppdateringar.

Fördelen med det första alternativet är att organisationer så snabbt som möjligt får möjlighet att agera för att installera de skydd de behöver för att inte kunna utsättas för intrång genom utnyttjande av den upptäckta sårbarheten. Å andra sidan kan organisationer ha begränsade möjligheter att frångå sitt fastlagda schema för installation av säkerhetsuppdateringar. Samtidigt innebär det offentliga publicerandet av information om sårbarheten att fler hotaktörer kan bli inspirerade att försöka hitta sätt att utnyttja sårbarheten, varpå mängden angrepp som utnyttjar sårbarheten ökar.

Nackdelen med det första alternativet kan därför vara att sårbarheten under en tid inte åtgärdas hos många organisationer, samtidigt som fler hotaktörer nu är varse sårbarheten och genomför angrepp med stöd av den.

Fördelen med det andra alternativet är att många organisationer kommer att installera säkerhetsuppdateringen så fort som möjligt efter att den tillgängliggjorts och de har blivit medvetna om den. Nackdelen är att hotaktören eller hotaktörerna som redan känner till och utnyttjar sårbarheten får längre tid på sig att göra det. Då information om sårbarheter, och speciellt utvecklade programvaror som kan utnyttja dem (s.k. ”exploits”) köps och säljs så kan antalet hotaktörer som utnyttjar en viss sårbarhet vara växande även om det här alternativet väljs.

För att hantera de här utmaningarna bör det göras en distinktion mellan kritiska säkerhetsuppdateringar och övriga säkerhetsuppdateringar. Kritiska säkerhetsuppdateringar bör publiceras och spridas direkt när de har tagits fram, och säkerhetsuppdateringar bör endast klassas som kritiska om angrepp som redan utförs med stöd av den upptäckta sårbarheten bedöms som särskilt allvarliga, eller om det är belagt att sårbarheten skulle kunna användas för att orsaka särskilt allvarliga incidenter, exempelvis i form av att människors liv och hälsa hotas. Säkerhetsuppdateringar som inte klassas som kritiska bör klassas som övriga, och sådana uppdateringar bör publiceras och spridas i samband med att många organisationer kan ta emot och installera dem.

I punkterna (1), (2) och (6) ställs krav på tillverkarna att bland annat vidta givna åtgärder. MSB uppfattar dessa formuleringar som ospecifika. Exempelvis bör det i punkt (2) framgå om tillverkaren alltid måste tillhandahålla säkerhetsuppdateringar och i så fall vilka tidsfrister för framtagande av säkerhetsuppdateringar som gäller. Eller, om det inte är möjligt, om mitigerande åtgärder kan ersätta säkerhetsuppdateringar antingen till dess en säkerhetsuppdatering kan göras tillgänglig eller på lång sikt.

Då ENISA föreslås ansvara för att ta emot rapporter om aktivt utnyttjade sårbarheter som omfattas av förordningen samt sprida information om dessa via nationella CSIRT-enheter och/eller nationella kontaktpunkter (enligt NIS2-direktivet) för vidare förmedling till marknadskontrollmyndigheten kommer detta få konsekvenser för MBS:s verksamhet och en förmodat icke oansenlig administrativ börda i denna hantering. Det är av stor vikt att genom fördjupad analys inhämta underlag för att bedöma omfattningen av denna tillkommande börda för att ha möjlighet att tilldela relevanta enheter erforderliga resurser. Det blir i synnerhet viktigt i ljuset av att detta sedan tidigare oreglerade område omfattar en stor mängd ekonomiska operatörer och produkter.

Det hänvisas i förslaget till produkters ”*förväntade livslängd eller en femårsperiod från produktens utsläppande på marknaden, beroende på vilken period som är kortast*” vilket får ses som en orealistisk och kanske även potentiellt innovationshämmande tidsram. Beroende på de omfattade produkternas vitt skilda användningsområden och produktmognad kan en rimligare definition även ta hänsyn till *typen* av produkt. Detta förefaller glädjande nog redan ha framhållits i förhandlingar inom HWPCI. Den nu föreslagna regleringen (och kommande liknande regleringar på cyberområdet) kommer i mångt och mycket förutsätta ett aktivt deltagande från MSB i egenskap av nationell CSIRT-enhet, men även andra tillkommande uppgifter. MSB ser därför positivt på att bli involverad redan på ett tidigt stadium i processen eftersom det ger myndigheten, i egenskap av expertmyndighet på området, möjligheter att stödja i arbetet med ett resurseffektivt genomförande som svarar mot Sveriges behov.

Synpunkter på definitioner i förslaget

I artikel 3 framgår de definitioner som förordningen använder.

I punkt (13) anser MSB att ordvalet privilegium bör ersättas med behörighet. På motsvarande sätt bör utökat privilegium i punkt (14) ersättas med utökad behörighet.

I punkt (39) definieras *aktivt utnyttjad sårbarhet*. MSB anser att definitionen bör ersättas med *sårbarhet för vilken det finns tillförlitliga bevis på att en aktör försökt utnyttja sårbarheten för att påverka ett system utan tillstånd från systemets ägare*. Detta för att en sårbarhet enligt nuvarande definition betraktas som aktivt utnyttjad om den finns på ett system där en aktör använder skadlig kod utan tillstånd från systemets ägare oavsett om det är den sårbarheten aktören försöker utnyttja.

Synpunkter på översättningar/terminologi i förslaget

I Bilaga I, avsnitt 2, punkt (5) framgår att tillverkarna ska *införa och verkställa en policy för samordnad redovisning av sårbarheter*. MSB tolkar detta som *coordinated vulnerability disclosure* och föreslår i så fall att samma terminologi används som i NIS2-direktivet, det vill säga ska *införa och verkställa en policy för samordnad delgivning av information om sårbarheter*.

I Bilaga I, avsnitt 2, punkt (8) bör *programfixar eller uppdateringar* ersättas med *säkerhetsuppdateringar*, alternativt *säkerhetsuppdateringar eller andra tillfälliga åtgärder*, beroende på vad som avses.

I detta ärende har generaldirektör Charlotte Petri Gornitzka beslutat.

Martin Snygg har varit föredragande och i den slutliga handläggningen har också avdelningschefen Åke Holmgren och enhetschefen Johan Turell deltagit.

Charlotte Petri Gornitzka Martin Snygg

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984