Gospodarska zbornica Slovenije

Združenje za informatiko in telekomunikacije
Dimičeva 13, 1504 Ljubljana, 01 5898 102,
www.gzs.si/zit, zit@gzs.si

zit Združenje za informatiko in telekomunikacije

IKT horizontalna mreža

URSIV - Sektor za dvig odpornosti
Ulica gledališča BTC 2
1000 Ljubljana

Ljubljana, 23. maj 2023

ZADEVA: Predlog potrebnih sprememb pri Uredbi o kibernetski odpornosti (CRA - Cyber Resilience Act) v EU

Spoštovani,

V Sekciji za kibernetsko varnost (SeKV) pri Združenju za informatiko in telekomunikacije (ZIT) pri Gospodarski zbornici Slovenije (GZS) in IKT Horizontalni mreži smo na podlagi odziva IKT industrije preučili predlog uredbe Evropske komisije o zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi t.i. Aktu o kibernetski odpornosti, ki naj bi Evropi zagotovil varnejšo strojno in programsko opremo ter s tem tudi okrepil kibernetsko varnost v EU. Pri oblikovanju naših predlogov za izboljšanje uredbe smo se naslonili na strokovno znanje naših članov, ki delujejo na področju kibernetske varnosti. V nadaljevanju vam podajamo nekaj predlogov za izboljšave:

1. Časovno obdobje za uveljavitev predlagane uredbe je potrebno podaljšati na najmanj 48 mesecev. S podaljšanjem obdobja uveljavitve, bi se razbremenilo vsa evropska podjetja in se jim dalo čas, da se prilagodijo. Ob enem pa bi tudi pristojne javne institucije (ENISA) dobile čas za oblikovanje skupnih standardov na področju kibernetske varnosti.
2. Podjetjem je potrebno omogočiti uporabo že obstoječih shem certificiranja kibernetske varnosti, ki temeljijo na skupnih standardih, kot dokazilo za skladnost z varnostnimi zahtevami v zakonodaji.
3. Vključitve programske opreme, kot izdelka v področje uporabe uredbe je potrebno dodatno opredeliti. Prav tako mora CRA uredba priznati delno dokončano naravo sestavnih delov v tehnoloških izdelkih.
4. Vključiti relevantne deležnike iz IKT in drugih industrij pri pripravi certifikatov in ocen tveganja posameznih IKT sistemov ali izdelkov. Ocene morajo temeljiti na podlagi tehničnih in strokovnih kriterijev.
5. CRA uredba ne sme predpisovati načina poročanja o neodpravljenih ranljivosti opreme, vendar naj raje oblikuje smernice za poročanje. Vsako podjetje naj predvidi svoj postopek za komunikacijo ranljivosti opreme oz. izdelka svojim strankam in do pristojnih institucij.
6. Pozivamo tudi vse odločevalce, da naj zagotovijo skladnost CRA uredbe z ostalimi EU in lokalnimi zakonskimi akti z namenom preprečitve podvajanja pristojnosti. V trenutnem predlogu uredbe se namreč prekrivajo številna varnostna področja, ki so že v pristojnosti drugih zakonskih aktov, kot npr. NIS-2, RED.

Združenje se tudi pridružuje stališču organizacije DIGITALEUROPE, ki zastopa interese evropske IKT industrije in je pripravilo Skupno stališče evropske industrije o CRA. ter Policy Paper o CRA. Evropske organizacije se zavedajo pomena te uredbe, ki bo vzpostavila horizontalni okvir za zahteve kibernetske varnosti za vse sisteme in izdelke z digitalnimi elementi.

Slovenska IKT industrija, MSP-ji in zagonska podjetja, ki jih to področje zadeva, dodatnih birokratskih zahtev in preprek ne bodo sposobna uveljaviti, saj že sedaj primanjkuje predvsem kadrovskih virov. Zato pozivamo vse odločevalce, da naj v pogajanjih striktno upoštevajo nebirokratske in na stroki preverjene rešitve v korist konkurenčnosti slovenskega gospodarstva in razvoju kibernetske varnosti v Sloveniji.

Združenje vam je s svojim strokovnim znanjem dosegljivo za dodatna vprašanja na zit@gzs.si in sekv@gzs.si.

S spoštovanjem,

Mihael Nagelj, predsednik SeKV
za Mihael Nagelj, Tomaž Čebela
Tomaž Čebela

Nenad Šutanovac, direktor ZIT

NENAD ŠUTANOVAC
Digitalno podpisal NENAD ŠUTANOVAC
Datum: 2023.05.23 14:17:54 +02'00'