Evropski parlament
2019-2024

Odbor za ustavne zadeve

2022/0085(COD)

31.1.2023

MNENJE

Odbora za ustavne zadeve

za Odbor za industrijo, raziskave in energetiko

o predlogu uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Pripravljavka mnenja: Markéta Gregorová

PA_Legam

KRATKA OBRAZLOŽITEV

Institucije, organi in agencije Evropske unije v zadnjih letih delujejo v vse bolj digitaliziranem okolju, ki ga zaznamuje stalen tehnološki razvoj in posledično vse večja intenzivnost kibernetskih groženj. Te razmere so se z izbruhom sanitarne krize zaradi COVID-19 in med drugim tudi povečanja dela na daljavo še poslabšale, in v tem času se je stopnjevalo tudi število izpopolnjenih napadov iz najrazličnejših virov.

Trenutno se razmere na področju kibernetske varnosti med institucijami, organi in agencijami Unije močno razlikujejo, tako v smislu upravljanja, kibernetske higiene, splošnih zmogljivosti kot zrelosti, kar je še dodatna ovira na poti do odprte, učinkovite in neodvisne evropske uprave.

Pripravljavka mnenja se zato strinja, da bi bilo treba za vzpostavitev skupnih sistemov kibernetske varnosti in zahtev glede tega v institucijah, organih in agencijah Unije razviti pristop osnovnih ukrepov, da se bo kibernetska varnost razvijala v isto smer, s čimer bi pripomogli k učinkovitosti in neodvisnosti evropske uprave.

Pripravljavka mnenja nadalje meni, da je trden in skladen varnostni okvir izjemnega pomena za zaščito vseh zaposlenih, podatkov, komunikacijskih omrežij, informacijskih sistemov in postopkov odločanja EU, s čimer bo prispeval tudi k demokratičnemu delovanju Evropske unije. Boljša varnostna kultura v institucijah, organih in agencijah Unije bi tudi omogočila, da bo Evropa pripravljena na digitalno dobo, in pa izgradnjo gospodarstva, ki bo primerna za izzive prihodnosti in bo služila ljudem.

PREDLOGI SPREMEMB

Odbor za ustavne zadeve poziva Odbor za industrijo, raziskave in energetiko kot pristojni odbor, da upošteva naslednje predloge sprememb:

Predlog spremembe 1

Predlog uredbe
Uvodna izjava 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(1) V digitalni dobi je informacijska in komunikacijska tehnologija temelj odprte, učinkovite in neodvisne uprave Unije. Razvijajoča se tehnologija ter vse večja kompleksnost in medsebojna povezanost digitalnih sistemov povečujejo tveganja za kibernetsko varnost, zaradi česar je uprava Unije ranljivejša za kibernetske grožnje in incidente, kar posledično ogroža neprekinjeno poslovanje uprave in	(1) V digitalni dobi je informacijska in komunikacijska tehnologija temelj odprte, učinkovite in neodvisne uprave Unije. Razvijajoča se tehnologija ter vse večja kompleksnost in medsebojna povezanost digitalnih sistemov povečujejo tveganja za kibernetsko varnost, zaradi česar je uprava Unije ranljivejša za kibernetske grožnje in incidente, kar posledično ogroža neprekinjeno poslovanje uprave in

zmogljivost zaščite podatkov. Večja uporaba storitev v oblaku, vsesplošna uporaba ***informacijskih tehnologij***, visoka stopnja digitalizacije, delo na daljavo ter razvijajoča se tehnologija in povezljivost so danes ključne značilnosti vseh dejavnosti subjektov uprave Unije, vendar digitalna odpornost še ni zadostno vgrajena.	zmogljivost zaščite podatkov. Večja uporaba storitev v oblaku, vsesplošna uporaba ***informacijske in komunikacijske tehnologije (v nadaljnjem besedilu: IKT)***, visoka stopnja digitalizacije, delo na daljavo ter razvijajoča se tehnologija in povezljivost so danes ključne značilnosti vseh dejavnosti subjektov uprave Unije, vendar digitalna odpornost še ni zadostno vgrajena.

Obrazložitev

V predlogu Komisije je uporabljen izraz „IT“, ko bi pravzaprav moral biti uporabljen izraz „IKT“, ki je standardni izraz v vseh ostalih dokumentih, revidirani direktivi o varnosti omrežij in informacijskih sistemov in aktu EU o kibernetski varnosti.

Predlog spremembe 2

Predlog uredbe
Uvodna izjava 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) Okolje kibernetskih groženj, ki so mu izpostavljeni institucije, organi in agencije Unije, se nenehno razvija. Taktike, tehnike in postopki, ki jih uporabljajo akterji groženj, se nenehno razvijajo, očitni motivi za take napade pa se le malo spreminjajo in zajemajo krajo dragocenih nerazkritih informacij, služenje denarja, manipulacijo z javnim mnenjem ali ogrožanje digitalne infrastrukture. Akterji kibernetske napade izvajajo vse pogosteje, njihove kampanje pa so vse bolj izpopolnjene in avtomatizirane, usmerjene v izpostavljene napadne površine, ki se širijo, ter hitro izkoriščajo ranljivosti.	(2) Okolje kibernetskih groženj, ki so mu izpostavljeni institucije, organi***, uradi*** in agencije Unije, se nenehno razvija. Taktike, tehnike in postopki, ki jih uporabljajo akterji groženj, se nenehno razvijajo, očitni motivi za take napade pa se le malo spreminjajo in zajemajo krajo dragocenih nerazkritih informacij, služenje denarja, manipulacijo z javnim mnenjem ali ogrožanje digitalne infrastrukture. Akterji kibernetske napade izvajajo vse pogosteje, njihove kampanje ***in metode*** pa so vse bolj izpopolnjene in avtomatizirane, usmerjene v izpostavljene napadne površine, ki se širijo, ter hitro izkoriščajo ranljivosti.

Predlog spremembe 3

Predlog uredbe
Uvodna izjava 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) Okolja ***IT*** institucij, organov in agencij Unije so medsebojno povezana in imajo vgrajene podatkovne tokove, njihovi uporabniki pa tesno sodelujejo. Ta medsebojna povezava pomeni, da lahko ima vsaka motnja, tudi če je sprva omejena na eno institucijo, organ ali agencijo Unije, širše kaskadne učinke, ki lahko imajo daljnosežne in dolgotrajne negativne posledice za druge. Poleg tega so okolja ***IT*** nekaterih institucij, organov in agencij povezana z okolji ***IT*** držav članic, kar pomeni, da incident v enem subjektu Unije ogroža kibernetsko varnost okolij ***IT*** držav članic in obratno.	(3) Okolja ***IKT*** institucij, organov***,*** ***uradov*** in agencij Unije so medsebojno povezana in imajo vgrajene podatkovne tokove, njihovi uporabniki pa tesno sodelujejo. Ta medsebojna povezava pomeni, da lahko ima vsaka motnja, tudi če je sprva omejena na eno institucijo, organ***,*** ***urad*** ali agencijo Unije, širše kaskadne učinke, ki lahko imajo daljnosežne in dolgotrajne negativne posledice za druge. Poleg tega so okolja ***IKT*** nekaterih institucij, organov***,*** ***uradov*** in agencij povezana z okolji ***IKT*** držav članic, kar pomeni, da incident v enem subjektu Unije ogroža kibernetsko varnost okolij ***IKT*** držav članic in obratno.

Predlog spremembe 4
Predlog uredbe
Uvodna izjava 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) Institucije, organi in agencije Unije so privlačne tarče, ki jih ogrožajo visoko usposobljeni in dobro podprti akterji groženj in tudi druge grožnje. Hkrati pa se raven in zrelost kibernetske odpornosti ter sposobnost odkrivanja zlonamernih kibernetskih dejavnosti in odzivanja nanje med navedenimi subjekti močno razlikujejo. Zato je za delovanje evropske uprave nujno, da institucije, organi in agencije Unije dosežejo visoko skupno raven kibernetske varnosti z osnovnimi ukrepi za kibernetsko varnost (sklopom minimalnih pravil o kibernetski varnosti, ki jih morajo omrežja in informacijski sistemi ter njihovi upravljavci in uporabniki upoštevati, da ***čim bolj zmanjšajo*** tveganja za kibernetsko varnost), izmenjavo informacij in sodelovanjem.	(4) Institucije, organi***,*** ***uradi*** in agencije Unije so privlačne tarče, ki jih ogrožajo visoko usposobljeni in dobro podprti akterji groženj in tudi druge grožnje. Hkrati pa se raven in zrelost kibernetske odpornosti ter sposobnost odkrivanja zlonamernih kibernetskih dejavnosti in odzivanja nanje med navedenimi subjekti močno razlikujejo. Zato je za delovanje evropske uprave nujno, da institucije, organi***,*** ***uradi*** in agencije Unije dosežejo visoko skupno raven kibernetske varnosti z osnovnimi ukrepi za kibernetsko varnost (sklopom ***skupnih*** minimalnih pravil o kibernetski varnosti, ki jih morajo omrežja in informacijski sistemi ter njihovi upravljavci in uporabniki upoštevati, da ***omejijo*** tveganja za kibernetsko varnost), ***z redno in učinkovito*** izmenjavo informacij in sodelovanjem ***ter usposabljanjem s področja kibernetske varnosti***.

Predlog spremembe 5

Predlog uredbe
Uvodna izjava 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) Zaradi razlik med institucijami, organi in agencijami Unije je potrebna prožnost v izvajanju, saj ena rešitev ne bo primerna za vse. Ukrepi za visoko skupno raven kibernetske varnosti ***ne*** bi ***smeli vključevati obveznosti, ki bi neposredno posegale v*** opravljanje nalog institucij, organov in agencij Unije ***ali posegale v*** njihovo institucionalno avtonomijo. Zato bi institucije, organi in agencije ***morali*** vzpostaviti lastne okvire za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost ter sprejeti lastne osnovne ukrepe in načrte za kibernetsko varnost.	(7) Zaradi razlik med institucijami, organi***, uradi*** in agencijami Unije je potrebna prožnost v izvajanju, saj ena rešitev ne bo primerna za vse. Ukrepi za visoko skupno raven kibernetske varnosti bi ***morali podpirati*** opravljanje nalog institucij, organov***, uradov*** in agencij Unije ***ter upoštevati*** njihovo institucionalno avtonomijo. Zato bi ***morali*** institucije, organi***, uradi*** in agencije ***na podlagi skupnega okvira, določenega s to uredbo,*** vzpostaviti lastne okvire za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost ter sprejeti lastne osnovne ukrepe in načrte za kibernetsko varnost***, a upoštevati tudi skladnost in interoperabilnost svojih okvirov ter se opreti na skupni okvir, ki ga določa ta uredba***.

Predlog spremembe 6
Predlog uredbe
Uvodna izjava 8

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(8) Da institucijam, organom in agencijam Unije ne bi bilo naloženo nesorazmerno finančno in upravno breme, bi morale biti zahteve glede obvladovanja tveganj za kibernetsko varnost ***sorazmerne s*** tveganjem, ki ga pomenita zadevno omrežje in informacijski sistem, pri čemer bi bilo treba upoštevati dovršenost takih ukrepov. Institucije, organi in agencije Unije bi si morali za izboljšanje ravni kibernetske varnosti prizadevati za ***dodelitev ustreznega deleža*** proračuna za ***IT;*** dolgoročno ***bi si bilo treba prizadevati za cilj v višini 10 %***.	(8) Da institucijam, organom***, uradom*** in agencijam Unije ne bi bilo naloženo nesorazmerno finančno in upravno breme, bi morale biti zahteve glede obvladovanja tveganj za kibernetsko varnost ***ustrezne*** tveganjem, ki ga pomenita zadevno omrežje in informacijski sistem, pri čemer bi bilo treba upoštevati dovršenost takih ukrepov. Institucije, organi***, uradi*** in agencije Unije bi si morali za izboljšanje ravni kibernetske varnosti prizadevati za ***vsaj 10 % svojega*** proračuna za ***IKT in srednjeročno, še bolj pa*** dolgoročno ***doseči vsaj minimalno raven kibernetske***

varnosti, ki bi ustrezala oceni tveganja.

Predlog spremembe 7

Predlog uredbe
Uvodna izjava 9

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(9) Za visoko skupno raven kibernetske varnosti mora imeti nadzor nad kibernetsko varnostjo ***najvišja raven*** upravljanja vsake institucije, organa in agencije Unije, ki bi morala odobriti osnovne ukrepe za kibernetsko varnost, ki bi morali obravnavati tveganja, opredeljena v okviru, ki ga vzpostavi vsaka institucija, organ in agencija. Obravnava kulture kibernetske varnosti, tj. dnevno izvajanje kibernetske varnosti, ***je*** sestavni del osnovnih ukrepov za kibernetsko varnost v vseh institucijah, organih in agencijah Unije.	(9) Za visoko skupno raven kibernetske varnosti mora imeti nadzor nad kibernetsko varnostjo ***skupni odbor EU, ki sodeluje z najvišjo ravnjo*** upravljanja vsake institucije, organa***, urada*** in agencije Unije, ki bi morala odobriti osnovne ukrepe za kibernetsko varnost, ki bi morali obravnavati tveganja, opredeljena v okviru, ki ga vzpostavi vsaka institucija, organ***, urad*** in agencija. Obravnava kulture kibernetske varnosti, tj. dnevno izvajanje kibernetske varnosti, ***bi morala postati*** sestavni del osnovnih ukrepov za kibernetsko varnost v vseh institucijah, organih***, uradih*** in agencijah Unije.

Predlog spremembe 8

Predlog uredbe
Uvodna izjava 10

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(10) Institucije, organi in agencije Unije bi morali oceniti tveganja, povezana z odnosi z dobavitelji in ponudniki storitev, vključno s ponudniki shranjevanja podatkov, storitev obdelave ali upravljanih varnostnih storitev, ter sprejeti ustrezne ukrepe za njihovo obravnavo. Ti ukrepi bi morali biti del osnovnih ukrepov za kibernetsko varnost in podrobneje opredeljeni v smernicah ali priporočilih, ki jih izda CERT-EU. Pri pripravi ukrepov in smernic bi bilo treba ustrezno upoštevati zadevno zakonodajo in politike EU, vključno z ocenami tveganja in priporočili	(10) Institucije, organi***, uradi*** in agencije Unije bi morali oceniti tveganja, povezana z odnosi z dobavitelji in ponudniki storitev, vključno s ponudniki shranjevanja podatkov, storitev obdelave ali upravljanih varnostnih storitev, ter sprejeti ustrezne ukrepe za njihovo obravnavo***. Te dobavitelje in ponudnike storitev bi bilo treba temeljito preveriti in pri tem upoštevati dobavno verigo ter ekonomsko in politično okolje, v katerem delujejo. Če bi odnosi s temi dobavitelji in ponudniki storitev ogrožali integriteto demokratičnih procesov v EU, bi jih bilo treba***

skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov, kot sta usklajena ocena tveganja v EU in nabor orodij EU za kibernetsko varnost omrežij 5G. Poleg tega bi ***lahko bilo*** potrebno certificiranje ustreznih proizvodov, storitev in postopkov IKT, na podlagi specifičnih certifikacijskih shem za kibernetsko varnost EU, sprejetih v skladu s členom 49 Uredbe (EU) 2019/881.

nemudoma prekiniti. Ti ukrepi bi morali biti del osnovnih ukrepov za kibernetsko varnost in podrobneje opredeljeni v smernicah ali priporočilih, ki jih izda CERT-EU. Pri pripravi ukrepov in smernic bi bilo treba ustrezno upoštevati zadevno zakonodajo in politike EU, vključno z ocenami tveganja in priporočili skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov, kot sta usklajena ocena tveganja v EU in nabor orodij EU za kibernetsko varnost omrežij 5G. Poleg tega bi ***moralo biti ob upoštevanju narave grožnje in pomena povečevanja odpornosti*** potrebno certificiranje ustreznih proizvodov, storitev in postopkov IKT***, ki se uporabljajo v institucijah, organih, uradih in agencijah Unije***, na podlagi specifičnih certifikacijskih shem za kibernetsko varnost EU, sprejetih v skladu s členom 49 Uredbe (EU) 2019/881.

Predlog spremembe 9

Predlog uredbe
Uvodna izjava 13

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(13) Veliko kibernetskih napadov je del širših kampanj, usmerjenih v skupine institucij, organov in agencij Unije ali interesnih skupnosti, ki vključujejo institucije, organe in agencije Unije. Da bi omogočili proaktivno odkrivanje, odzivanje na incidente ali blažilne ukrepe, bi morali institucije, organi in agencije Unije CERT-EU obvestiti o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih ter deliti ustrezne tehnične podrobnosti, ki omogočajo odkrivanje ali blaženje podobnih kibernetskih groženj, ranljivosti in incidentov ter odzivanje nanje v drugih institucijah, organih in agencijah Unije. V skladu s pristopom, enakim tistemu, ki je	(13) Veliko kibernetskih napadov je del širših kampanj, usmerjenih v skupine institucij, organov***, uradov*** in agencij Unije ali interesnih skupnosti, ki vključujejo institucije, organe***, urade*** in agencije Unije. Da bi omogočili proaktivno odkrivanje, odzivanje na incidente ali blažilne ukrepe, bi morali institucije, organi***, uradi*** in agencije Unije CERT-EU obvestiti o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih ter deliti ustrezne tehnične podrobnosti, ki omogočajo odkrivanje ali blaženje podobnih kibernetskih groženj, ranljivosti in incidentov ter odzivanje nanje v drugih institucijah, organih***, uradih*** in agencijah Unije. V skladu s pristopom,

predviden v Direktivi [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov], bi morali subjekti, ko se seznanijo s pomembnim incidentom, v 24 urah CERT-EU ***predložiti začetno priglasitev***. Taka izmenjava informacij bi morala CERT-EU omogočiti širjenje informacij drugim institucijam, organom in agencijam Unije ter tudi ustreznim sorodnim organom za pomoč pri zaščiti vseh okolij ***IT*** v Uniji in okolij ***IT*** sorodnih organov Unije pred podobnimi incidenti, grožnjami in ranljivostmi.

enakim tistemu, ki je predviden v Direktivi [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov], bi morali subjekti, ko se seznanijo s pomembnim incidentom, ***nemudoma, v nobenem primeru pa ne v več kot*** v 24 urah CERT-EU ***poslati zgodnje opozorilo***. ***Institucijam, organom, uradom in agencijam Unije bi bilo treba dodeliti zadostna sredstva, da bodo lahko hitro in učinkovito izpolnili svoje obveznosti poročanja in se bo zagotovilo, da bo zasnovani sistem pravilno deloval.*** Taka izmenjava informacij bi morala CERT-EU omogočiti širjenje informacij drugim institucijam, organom***, uradom*** in agencijam Unije ter tudi ustreznim sorodnim organom za pomoč pri zaščiti vseh okolij ***IKT*** v Uniji in okolij ***IKT*** sorodnih organov Unije pred podobnimi incidenti, grožnjami in ranljivostmi.

Predlog spremembe 10

Predlog uredbe
Uvodna izjava 14

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(14) Poleg tega, da se CERT-EU dodeli več nalog in razširjena vloga, bi moral biti ustanovljen tudi Medinstitucionalni odbor za kibernetsko varnost (IICB), ki bi moral olajšati doseganje visoke skupne ravni kibernetske varnosti med institucijami, organi in agencijami Unije s spremljanjem izvajanja te uredbe s strani institucij, organov in agencij Unije, nadzorovanjem izvajanja splošnih prednostnih nalog in ciljev s strani CERT-EU in zagotavljanjem strateških usmeritev CERT-EU. IICB bi moral zagotoviti zastopanost institucij ter vključevati predstavnike agencij in organov prek mreže agencij Unije.	(14) Poleg tega, da se CERT-EU dodeli več nalog in razširjena vloga, bi moral biti ustanovljen tudi Medinstitucionalni odbor za kibernetsko varnost (IICB), ki bi moral olajšati doseganje visoke skupne ravni kibernetske varnosti med institucijami, organi***, uradi*** in agencijami Unije s spremljanjem izvajanja te uredbe s strani institucij, organov***, uradov*** in agencij Unije, nadzorovanjem izvajanja splošnih prednostnih nalog in ciljev s strani CERT-EU in zagotavljanjem strateških usmeritev CERT-EU. IICB bi moral zagotoviti ***enako*** zastopanost institucij ter vključevati predstavnike agencij***, uradov*** in organov prek mreže agencij Unije.

Predlog spremembe 11

Predlog uredbe
Uvodna izjava 16

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(16) IICB bi moral spremljati skladnost s to uredbo ter nadaljnje ukrepanje na podlagi smernic, priporočil in pozivov k ukrepanju, ki jih izda CERT-EU. V zvezi s tehničnimi vprašanji bi ga bilo treba podpreti s tehničnimi svetovalnimi skupinami, ki ***so sestavljene, kot se IICB zdi ustrezno, in ki*** bi morale tesno sodelovati s CERT-EU, institucijami, organi in agencijami Unije ter ***po potrebi*** z drugimi deležniki. IICB bi moral po potrebi izdati ***nezavezujoča*** opozorila in ***priporočiti*** revizije.	(16) IICB bi moral spremljati skladnost s to uredbo ter nadaljnje ukrepanje na podlagi smernic, priporočil in pozivov k ukrepanju, ki jih izda CERT-EU. V zvezi s tehničnimi vprašanji bi ga bilo treba podpreti s tehničnimi svetovalnimi skupinami, ki bi morale tesno sodelovati s CERT-EU, institucijami, organi***, uradi*** in agencijami Unije ter z drugimi deležniki***, kot je ustrezno***. IICB bi moral po potrebi izdati opozorila in ***priporočila za*** revizije.

Predlog spremembe 12

Predlog uredbe
Uvodna izjava 17

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(17) CERT-EU bi moral imeti nalogo prispevati k varnosti okolja ***IT*** vseh institucij, organov in agencij Unije. Imeti bi moral vlogo, enakovredno imenovanemu koordinatorju za institucije, organe in agencije Unije, za namene usklajenega razkrivanja ranljivosti evropskemu registru ranljivosti iz člena 6 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].	(17) CERT-EU bi moral imeti nalogo prispevati k varnosti okolja ***IKT*** vseh institucij, organov***, uradov*** in agencij Unije. Imeti bi moral vlogo, enakovredno imenovanemu koordinatorju za institucije, ***urade*** organe in agencije Unije, za namene usklajenega razkrivanja ranljivosti evropskemu registru ranljivosti iz člena 6 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].

Predlog spremembe 13

Predlog uredbe
Uvodna izjava 18

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*

(18) Leta 2020 je usmerjevalni odbor CERT-EU določil nov strateški cilj za CERT-EU, da bi se zagotovila celovita ter ustrezno obsežna in poglobljena raven kibernetske obrambe za vse institucije, organe in agencije Unije ter stalno prilagajanje sedanjim ali prihodnjim grožnjam, vključno z napadi na mobilne naprave, okolja v oblaku in naprave interneta stvari. Strateški cilj vključuje tudi zelo različne centre za varnostne operacije, ki spremljajo omrežja, in spremljanje 24 ur na dan, sedem dni v tednu, za zelo resne grožnje. V zvezi z večjimi institucijami, organi in agencijami Unije bi moral CERT-EU podpirati njihove ekipe za varnost ***IT***, vključno s primarnim spremljanjem 24 ur na dan, sedem dni v tednu. Manjšim in nekaj srednjim institucijam, organom in agencijam Unije bi CERT-EU moral zagotavljati vse storitve.	(18) Leta 2020 je usmerjevalni odbor CERT-EU določil nov strateški cilj za CERT-EU, da bi se zagotovila celovita ter ustrezno obsežna in poglobljena raven kibernetske obrambe za vse institucije, organe***, urade*** in agencije Unije ter stalno prilagajanje sedanjim ali prihodnjim grožnjam, vključno z napadi na mobilne naprave, okolja v oblaku in naprave interneta stvari. Strateški cilj vključuje tudi zelo različne centre za varnostne operacije, ki spremljajo omrežja, in spremljanje 24 ur na dan, sedem dni v tednu, za zelo resne grožnje. V zvezi z večjimi institucijami, organi***, uradi*** in agencijami Unije bi moral CERT-EU podpirati njihove ekipe za varnost ***IKT***, vključno s primarnim spremljanjem 24 ur na dan, sedem dni v tednu. Manjšim in nekaj srednjim institucijam, organom***, uradom*** in agencijam Unije bi CERT-EU moral zagotavljati vse storitve.

Predlog spremembe 14

Predlog uredbe
Uvodna izjava 19 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(19a) Da se zagotovi boljše izvajanje ukrepov in smernic za kibernetsko varnost za institucije, organe, urade in agencije Unije ter da se pri njih utrdi kultura kibernetske varnosti, bi moral CERT-EU okrepiti tudi sodelovanje z evropsko kompetenčno mrežo in kompetenčnim centrom za kibernetsko varnost.

Predlog spremembe 15

Predlog uredbe
Uvodna izjava 20

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(20) Pri podpori operativni kibernetski	(20) Pri podpori operativni kibernetski

varnosti bi moral CERT-EU izkoriščati razpoložljivo strokovno znanje Agencije Evropske unije za kibernetsko varnost prek strukturiranega sodelovanja, kot je predvideno v Uredbi (EU) 2019/881 Evropskega parlamenta in Sveta[5]. ***Po potrebi*** bi bilo treba ***sprejeti*** posebne dogovore med tema dvema subjektoma, s katerimi bi določili praktično izvajanje takega sodelovanja in ***se izogibali podvajanju*** dejavnosti. CERT-EU bi moral z Agencijo Evropske unije za kibernetsko varnost sodelovati v zvezi z analizo groženj in ji redno posredovati svoje poročilo o grožnjah.

varnosti bi moral CERT-EU izkoriščati razpoložljivo strokovno znanje Agencije Evropske unije za kibernetsko varnost prek strukturiranega sodelovanja, kot je predvideno v Uredbi (EU) 2019/881 Evropskega parlamenta in Sveta[5]. ***Sprejeti*** bi bilo treba posebne dogovore med tema dvema subjektoma, s katerimi bi določili praktično izvajanje takega sodelovanja in ***preprečili podvajanje*** dejavnosti. CERT-EU bi moral z Agencijo Evropske unije za kibernetsko varnost sodelovati v zvezi z analizo groženj in ji redno posredovati svoje poročilo o grožnjah.

---

[5] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

[5] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

Predlog spremembe 16
Predlog uredbe
Uvodna izjava 24

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(24) Ker so storitve in naloge CERT-EU v interesu vseh institucij, organov in agencij Unije, bi morala vsaka institucija, organ ali agencija Unije z izdatki za ***IT*** prispevati ***pravičen*** delež k tem storitvam in nalogam. Taki prispevki ne posegajo v proračunsko avtonomijo institucij, organov in agencij Unije.	(24) Ker so storitve in naloge CERT-EU v interesu vseh institucij, organov***, uradov*** in agencij Unije, bi morala vsaka institucija, organ***, urad*** ali agencija Unije z izdatki za ***IKT*** prispevati ***sorazmeren*** delež k tem storitvam in nalogam. Taki prispevki ne posegajo v proračunsko avtonomijo institucij, organov***, uradov*** in agencij Unije.

Predlog spremembe 17

Predlog uredbe
Uvodna izjava 25

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(25) IICB bi moral ob pomoči CERT-EU pregledati in oceniti izvajanje te uredbe ter Komisiji poročati o svojih ugotovitvah. Na podlagi tega prispevka bi morala Komisija poročati Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij –	(25) IICB bi moral ob pomoči CERT-EU pregledati in oceniti izvajanje te uredbe ter Komisiji poročati o svojih ugotovitvah. Na podlagi tega prispevka bi morala Komisija ***vsaj vsaka tri leta*** poročati Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij –

Predlog spremembe 18

Predlog uredbe
Člen 1 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) obveznosti za institucije, organe in agencije Unije, v skladu s katerimi morajo vzpostaviti notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost;	(a) obveznosti za institucije, organe***,*** ***urade*** in agencije Unije, v skladu s katerimi morajo vzpostaviti notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost;

Predlog spremembe 19

Predlog uredbe
Člen 1 – odstavek 1 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) pravila o organizaciji in delovanju centra za kibernetsko varnost za institucije, organe in agencije Unije (CERT-EU) ter o organizaciji in delovanju Medinstitucionalnega odbora za kibernetsko varnost.	(c) pravila o organizaciji in delovanju centra za kibernetsko varnost za institucije, organe***, urade*** in agencije Unije (CERT-EU) ter o ***poslovanju,*** organizaciji in delovanju Medinstitucionalnega odbora za kibernetsko varnost ***(IICB)***.

Predlog spremembe 20

Predlog uredbe

Člen 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Člen 2a
	Obdelava osebnih podatkov
	Obdelava osebnih podatkov po tej uredbi, ki jo izvajajo CERT-EU, IICB ter vse institucije, organi, uradi in agencije Unije, poteka v skladu z Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta.

Predlog spremembe 21

Predlog uredbe
Člen 3 – odstavek 1 – točka 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(2) „omrežje in informacijski sistem“ pomeni omrežje in informacijski sistem v ***smislu člena 4***(1) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];	(2) „omrežje in informacijski sistem“ pomeni omrežje in informacijski sistem***,*** ***kot sta opredeljena*** v ***členu 6, točka*** (1)***,*** Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];

Predlog spremembe 22

Predlog uredbe
Člen 3 – odstavek 1 – točka 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(4) „kibernetska varnost“ pomeni kibernetsko varnost v ***smislu člena 4(3) Direktive [predlog revidirane direktive o varnosti omrežij*** in ***informacijskih sistemov]***;	(4) „kibernetska varnost“ pomeni kibernetsko varnost***, kot je opredeljena*** v ***členu 2, točka (1), Uredbe (EU) 2019/881 Evropskega parlamenta*** in ***Sveta***[1a];
	[1a] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske

	tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

Predlog spremembe 23

Predlog uredbe
Člen 3 – odstavek 1 – točka 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(5) „najvišja raven upravljanja“ pomeni vodjo, vodstvo ali organ za usklajevanje in nadzor na najvišji upravni ravni, ob upoštevanju ureditev upravljanja na visoki ravni v vsaki ***institucij***, organu ali agenciji Unije;	(5) „najvišja raven upravljanja“ pomeni vodjo, vodstvo ali organ za usklajevanje in nadzor na najvišji upravni ravni, ***ki je pooblaščen za sprejemanje ali odobritev odločitev,*** ob upoštevanju ureditev upravljanja na visoki ravni v vsaki ***instituciji***, organu***, uradu*** ali agenciji Unije;

Predlog spremembe 24

Predlog uredbe
Člen 3 – odstavek 1 – točka 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) „pomembni incident“ pomeni vsak incident, ***razen če ima omejen učinek in obstaja verjetnost, da*** je ***z vidika metode*** ali ***tehnologije že dobro razumljen.***	(7) „pomembni incident“ pomeni vsak incident, ***ki povzroči ali je zmožen povzročiti resne operativne motnje v delovanju subjekta Unije ali finančno izgubo temu subjektu Unije ali ki prizadene ali*** je ***zmožen prizadeti druge fizične*** ali ***pravne osebe, s tem ko jim povzroči znatno premoženjsko ali nepremoženjsko škodo;***

Predlog spremembe 25

Predlog uredbe
Člen 3 – odstavek 1 – točka 11

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(11) „pomembna kibernetska grožnja“ pomeni kibernetsko grožnjo ***z namenom***,	(11) „pomembna kibernetska grožnja“ pomeni kibernetsko grožnjo***, kot je***

priložnostjo in zmožnostjo povzročiti pomemben incident;	***opredeljena v členu 6**, **točka (11), Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov]***;

Predlog spremembe 26

Predlog uredbe
Člen 3 – odstavek 1 – točka 14

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(14) ***„tveganje za kibernetsko varnost“*** pomeni vsako ***razumno določljivo okoliščino ali dogodek**, **ki ima lahko negativen učinek na varnost omrežja*** in informacijskih ***sistemov***;	(14) ***„tveganje“*** pomeni vsako ***tveganje, kot je opredeljeno v členu 6**, **točka (9), Direktive [predlog revidirane direktive o varnosti omrežij*** in informacijskih ***sistemov]***;

Predlog spremembe 27

Predlog uredbe
Člen 3 – odstavek 1 – točka 14 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(14a) „okolje IKT“ pomeni vsak lokalni ali virtualni proizvod IKT, storitev IKT in postopek IKT, kot so opredeljeni v členu 2, točke (12), (139 in (14), Uredbe (EU) 2019/881, ter vsako omrežje in informacijski sistem, ki je bodisi v lasti in upravljanju institucije, organa, urada ali agencije Unije bodisi ga zanj gosti ali upravlja tretja oseba, vključno z mobilnimi napravami, korporativnimi in poslovnimi omrežji, ki niso povezana z internetom, ter vsemi napravami, povezanimi z okoljem IKT;

Obrazložitev

Izraz se iz člena 4(2) tega predloga prenese v člen o opredelitvah pojmov, saj se ta izraz dosledno uporablja v celotnem besedilu. Predlagana opredelitev tega izraza izhaja iz opredelitev njegovih sestavnih delov iz člena 2 Uredbe (EU) 2019/881 o zakonu o kibernetski varnosti.

Predlog spremembe 28

Predlog uredbe
Člen 3 – odstavek 1 – točka 15

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(15) „skupna kibernetska enota“ pomeni virtualno in fizično sodelovalno platformo za različne skupnosti za kibernetsko varnost v Uniji, s poudarkom na operativnem in tehničnem usklajevanju zoper večje čezmejne kibernetske grožnje in incidente v smislu Priporočila Komisije z dne 23. junija 2021;	***črtano***

Predlog spremembe 29
Predlog uredbe
Člen 4 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Vsaka institucija, organ in agencija Unije vzpostavi lasten notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost (v nadaljnjem besedilu: okvir) v podporo poslanstvu subjekta in izvajanju njegove institucionalne avtonomije. To delo nadzoruje najvišja raven upravljanja subjekta, ***da se zagotovi učinkovito in preudarno obvladovanje vseh tveganj*** za kibernetsko varnost. Okvir se vzpostavi najpozneje do …. [15 mesecev po ***začetku*** veljavnosti te uredbe].	1. Vsaka institucija, organ***, urad*** in agencija Unije ***na podlagi celovite revizije varnosti*** vzpostavi lasten notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost (v nadaljnjem besedilu: okvir) v podporo poslanstvu subjekta in izvajanju njegove institucionalne avtonomije***, pri tem pa upošteva tudi skladnost in interoperabilnost svojega okvira z okviri drugih relevantnih institucij, organov, uradov in agencij***. To delo nadzoruje najvišja raven upravljanja subjekta, ***ki mora poskrbeti, da se vsa tveganja*** za kibernetsko varnost ***učinkovito in preudarno obvladujejo***. Okvir se vzpostavi najpozneje do …. [15 mesecev po ***datumu začetka*** veljavnosti te uredbe].

Predlog spremembe 30

Predlog uredbe
Člen 4 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Okvir zajema celotno okolje ***IT*** zadevne institucije, organa ali agencije, vključno z morebitnim okoljem ***IT*** v njenih prostorih, sredstvi in storitvami v okoljih računalništva v oblaku, ki jih upravlja zunanji izvajalec ali gostijo tretje osebe, mobilnimi napravami, korporativnimi omrežji, poslovnimi omrežji, ki niso povezana z internetom, in vsemi napravami, povezanimi z okoljem ***IT***. Okvir upošteva neprekinjeno poslovanje in krizno upravljanje ter varnost dobavne verige in obvladovanje človeških tveganj, ki bi lahko vplivali na kibernetsko varnost zadevne institucije, organa ali agencije Unije.	2. Okvir zajema celotno okolje ***IKT*** zadevne institucije, organa***, urada*** ali agencije, vključno z morebitnim okoljem ***IKT*** v njenih prostorih, sredstvi in storitvami v okoljih računalništva v oblaku, ki jih upravlja zunanji izvajalec ali gostijo tretje osebe, mobilnimi napravami, korporativnimi omrežji, poslovnimi omrežji, ki niso povezana z internetom, in vsemi napravami, povezanimi z okoljem ***IKT***. Okvir upošteva neprekinjeno poslovanje in krizno upravljanje ter varnost dobavne verige in obvladovanje človeških tveganj, ki bi lahko vplivali na kibernetsko varnost zadevne institucije, organa***, urada*** ali agencije Unije.

Predlog spremembe 31
Predlog uredbe
Člen 4 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. Vse institucije, organi in agencije Unije imajo vzpostavljene učinkovite mehanizme za zagotavljanje, da se za kibernetsko varnost nameni ***ustrezen delež*** proračuna za ***IT***.	4. Vse institucije, organi***, uradi*** in agencije Unije imajo vzpostavljene učinkovite mehanizme za zagotavljanje, da se za kibernetsko varnost ***srednjeročno*** nameni ***vsaj 10 % celokupnega*** proračuna za ***IKT***.

Predlog spremembe 32

Predlog uredbe
Člen 4 – odstavek 5 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	5a. Lokalni uradnik za kibernetsko varnost sodeluje s pooblaščeno osebo za varstvo podatkov iz člena 43 Uredbe (EU) 2018/1725, da bi obravnavala prekrivajoče se dejavnosti, in sicer pri ukrepih za kibernetsko varnost uporabljata vgrajeno in privzeto varstvo podatkov, pri izbiranju ukrepov za

	kibernetsko varnost, ki vključujejo varstvo osebnih podatkov, pa vgrajeno obvladovanje tveganj in vgrajeno obravnavanje varnostnih incidentov.

Predlog spremembe 33

Predlog uredbe
Člen 5 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Najvišja raven upravljanja vsake institucije, organa in agencije Unije odobri osnovne ukrepe subjekta za kibernetsko varnost za obravnavo tveganj, opredeljenih v okviru iz člena 4(1). To stori v podporo svojemu poslanstvu in pri izvajanju svoje institucionalne avtonomije. Osnovni ukrepi za kibernetsko varnost so vzpostavljeni najpozneje do ... [18 mesecev po ***začetku*** veljavnosti te uredbe] ter se nanašajo na področja iz Priloge I in ukrepe iz Priloge II.	1. Najvišja raven upravljanja vsake institucije, organa***, urada*** in agencije Unije odobri osnovne ukrepe subjekta za kibernetsko varnost za obravnavo tveganj, opredeljenih v okviru iz člena 4(1). To stori v podporo svojemu poslanstvu in pri izvajanju svoje institucionalne avtonomije***, pri čemer popolnoma spoštuje zahteve iz te uredbe ter upošteva skladnost in interoperabilnost svojega okvira z okviri drugih relevantnih institucij, organov, uradov in agencij, pa tudi smernice in priporočila, ki jih na predlog CERT-EU sprejme IICB, in veljavne certifikacijske sheme EU za kibernetsko varnost***. Osnovni ukrepi za kibernetsko varnost so vzpostavljeni najpozneje do ... [18 mesecev po ***datumu začetka*** veljavnosti te uredbe] ter se nanašajo na področja iz Priloge I in ukrepe iz Priloge II.

Predlog spremembe 34

Predlog uredbe
Člen 5 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Višje vodstvo vsake institucije, organa in agencije Unije redno opravlja posebno usposabljanje, da pridobi dovolj znanja in spretnosti za razumevanje in oceno tveganj za kibernetsko varnost in praks obvladovanja ter njihovega vpliva na	2. Višje vodstvo vsake institucije, organa***, urada*** in agencije Unije redno opravlja posebno usposabljanje, da pridobi dovolj znanja in spretnosti za razumevanje in oceno tveganj za kibernetsko varnost in praks obvladovanja ter njihovega vpliva na

delovanje organizacije.	delovanje organizacije ***z ustreznimi viri***. ***Poleg tega namenskega usposabljanja in za utrditev kulture kibernetske varnosti se v načrt za kibernetsko varnost vključi redno usposabljanje zaposlenih na področju kibernetske varnosti, ki se najmanj vsaki dve leti posodobi. Zagotovijo se zadostna sredstva za kakovostno usposabljanje.***

Predlog spremembe 35

Predlog uredbe
Člen 6 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Vsaka institucija, organ in agencija Unije najmanj ***vsaka tri leta*** izvede oceno kibernetskovarnostne zrelosti, ki vključuje vse elemente njenega okolja ***IT***, kot je opisano v členu 4, ob upoštevanju ustreznih smernic in priporočil, sprejetih v skladu s členom 13.	Vsaka institucija, organ***, urad*** in agencija Unije ***najpozneje do ... [šest mesecev po začetku veljavnosti te uredbe] in nato*** najmanj ***vsaki dve leti*** izvede oceno kibernetskovarnostne zrelosti, ki vključuje vse elemente njenega okolja ***IKT***, kot je opisano v členu 4, ob upoštevanju ustreznih smernic in priporočil, sprejetih v skladu s členom 13. ***Ocena zrelosti mora temeljiti na neodvisnih revizijah kibernetske varnosti, ki jih opravijo preverjeni izvajalci.***

Predlog spremembe 36

Predlog uredbe
Člen 7 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Najvišja raven upravljanja vsake institucije, organa in agencije Unije na podlagi sklepov ocene zrelosti in ob upoštevanju sredstev in tveganj, opredeljenih v skladu s členom 4, po vzpostavitvi okvira za obvladovanje, upravljanje in nadzor tveganj ter osnovnih ukrepov za kibernetsko varnost nemudoma odobri načrt za kibernetsko varnost. Cilj	1. Najvišja raven upravljanja vsake institucije, organa***, urada*** in agencije Unije na podlagi sklepov ocene zrelosti in ob upoštevanju sredstev in tveganj, opredeljenih v skladu s členom 4, po vzpostavitvi okvira za obvladovanje, upravljanje in nadzor tveganj ter osnovnih ukrepov za kibernetsko varnost nemudoma odobri načrt za kibernetsko varnost. Cilj

načrta je izboljšati splošno kibernetsko varnost zadevnega subjekta, s tem pa prispeva k doseganju ali zvišanju visoke skupne ravni kibernetske varnosti vseh institucij, organov in agencij Unije. V podporo poslanstvu subjekta na podlagi institucionalne avtonomije načrt vključuje najmanj področja, navedena v Prilogi I, ukrepe, navedene v Prilogi II, ter ukrepe v zvezi s pripravljenostjo na incidente, odzivanjem nanje in okrevanjem po njih, kot ***sta varnostno*** spremljanje in vodenje dnevnikov. Načrt se pregleda najmanj ***vsaka tri leta***, in sicer na podlagi ocen zrelosti, izvedenih v skladu s členom 6.

načrta je izboljšati splošno kibernetsko varnost zadevnega subjekta, s tem pa prispeva k doseganju ali zvišanju visoke skupne ravni kibernetske varnosti vseh institucij, organov***, uradov*** in agencij Unije. V podporo poslanstvu subjekta na podlagi institucionalne avtonomije načrt vključuje najmanj področja, navedena v Prilogi I, ukrepe, navedene v Prilogi II, ter ukrepe v zvezi s pripravljenostjo na incidente, odzivanjem nanje in okrevanjem po njih, kot ***so varnostna ocena dobaviteljev in ponudnikov storitev,*** spremljanje in vodenje dnevnikov. Načrt se pregleda najmanj ***vsaki dve leti***, in sicer na podlagi ocen zrelosti, izvedenih v skladu s členom 6.

Predlog spremembe 37

Predlog uredbe
Člen 7 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Načrt za kibernetsko varnost vključuje vloge članov osebja in odgovornosti za njegovo izvajanje.	2. Načrt za kibernetsko varnost vključuje vloge članov osebja***, pripravljenost*** in odgovornosti za njegovo izvajanje.

Predlog spremembe 38

Predlog uredbe
Člen 7 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Načrt za kibernetsko varnost ***upošteva*** vse ***veljavne smernice*** in ***priporočila***, ki jih izda CERT-EU.	3. Načrt za kibernetsko varnost ***vključuje*** vse ***predlagane ukrepe, zajete v veljavnih smernicah*** in ***priporočilih***, ki jih izda CERT-EU.

Predlog spremembe 39

Predlog uredbe
Člen 7 – odstavek 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	3a. Vse institucije, organi, uradi in agencije Unije predložijo IICB svoje načrte za kibernetsko varnost. Načrti se izmenjajo do te mere, da se nepooblaščenim tretjim osebam ne razkrijejo občutljive ali zaupne informacije o konkretni tehnični ureditvi kibernetske varnosti in zmogljivostih subjekta Unije.

Predlog spremembe 40

Predlog uredbe
Člen 9 – odstavek 2 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) spremljanje, kako institucije, organi in agencije Unije izvajajo to uredbo, ter	(a) spremljanje, kako institucije, organi***, uradi*** in agencije Unije izvajajo to uredbo, ter ***podajanje priporočil, kako doseči visoko skupno raven kibernetske varnosti;***

Predlog spremembe 41

Predlog uredbe
Člen 9 – odstavek 3 – pododstavek 1 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
IICB sestavljajo trije predstavniki, ki jih imenuje mreža agencij Unije (EUAN) na predlog svojega svetovalnega odbora za IKT in ki zastopajo interese agencij in organov, ki upravljajo svoje okolje ***IT***, ter po en predstavnik, ki ga imenuje vsak od spodaj navedenih:	IICB sestavljajo trije predstavniki, ki jih imenuje mreža agencij Unije (EUAN) na predlog svojega svetovalnega odbora za IKT in ki zastopajo interese ***uradov,*** agencij in organov, ki upravljajo svoje okolje ***IKT***, ter po en predstavnik, ki ga imenuje vsak od spodaj navedenih:

Predlog spremembe 42

Predlog uredbe
Člen 9 – odstavek 3 – pododstavek 1 – točka k a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(ka) Evropski nadzornik za varstvo podatkov.

Predlog spremembe 43

Predlog uredbe
Člen 10 – odstavek 1 – točka a a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(aa) na podlagi predloga vodje CERT-EU odobri priporočila za dosego skupne visoke ravni kibernetske varnosti, namenjene eni ali vsem institucijam, organom, uradom in agencijam Unije;

Predlog spremembe 44

Predlog uredbe
Člen 11 – odstavek 1 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) izda opozorilo; po potrebi zaradi velikega tveganja za kibernetsko varnost je krog prejemnikov opozorila ustrezno omejen;	(a) izda opozorilo; po potrebi zaradi velikega tveganja za kibernetsko varnost je krog prejemnikov opozorila ustrezno omejen***, in sicer po skupno dogovorjeni metodologiji***;

Predlog spremembe 45

Predlog uredbe
Člen 11 – odstavek 1 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) ustrezni službi za reviziji ***predlaga*** izvedbo revizije.	(b) ustrezni službi za reviziji ***naloži*** izvedbo revizije.

Predlog spremembe 46

Predlog uredbe
Člen 12 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Poslanstvo CERT-EU, samostojnega medinstitucionalnega centra za kibernetsko varnost za vse institucije, organe in agencije Unije, je prispevati k varnosti okolja netajnih podatkov ***IT*** vseh institucij, organov in agencij Unije, tako da jim svetuje glede kibernetske varnosti ter jim pomaga preprečiti, odkriti in ublažiti incidente ter se odzivati nanje, deluje pa tudi kot njihovo vozlišče za izmenjavo informacij o kibernetski varnosti in za usklajevanje odzivanja na incidente.	1. Poslanstvo CERT-EU, samostojnega medinstitucionalnega centra za kibernetsko varnost za vse institucije, organe***, urade*** in agencije Unije, je prispevati k varnosti okolja netajnih podatkov ***IKT*** vseh institucij, organov***, uradov*** in agencij Unije, tako da jim svetuje glede kibernetske varnosti ter jim pomaga preprečiti, odkriti in ublažiti incidente ter se odzivati nanje, deluje pa tudi kot njihovo vozlišče za izmenjavo informacij o kibernetski varnosti in za usklajevanje odzivanja na incidente.

Predlog spremembe 47

Predlog uredbe
Člen 12 – odstavek 2 – točka d

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(d) IICB opozori na ***katero koli vprašanje***, ***ki se nanaša na izvajanje*** te uredbe ali smernic, priporočil in pozivov k ukrepanju;	(d) IICB opozori na ***morebitne težave***, ***povezane z izvajanjem*** te uredbe ali smernic, priporočil in pozivov k ukrepanju***, ter pripravi predloge za popravne ukrepe***;

Predlog spremembe 48

Predlog uredbe
Člen 12 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. CERT-EU strukturirano sodeluje z Agencijo Evropske unije za kibernetsko varnost pri krepitvi zmogljivosti, operativnem sodelovanju in dolgoročnih strateških analizah kibernetskih groženj v skladu z Uredbo (EU) 2019/881	4. CERT-EU strukturirano sodeluje z Agencijo Evropske unije za kibernetsko varnost pri krepitvi zmogljivosti, operativnem sodelovanju in dolgoročnih strateških analizah kibernetskih groženj v skladu z Uredbo (EU) 2019/881

Evropskega parlamenta in Sveta.	Evropskega parlamenta in Sveta. ***Poleg tega lahko CERT-EU sodeluje in izmenjuje informacije z Evropskim centrom za boj proti kibernetski kriminaliteti.***

Predlog spremembe 49

Predlog uredbe
Člen 12 – odstavek 5 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. CERT-EU lahko zagotavlja naslednje storitve, ki niso opisane v njegovem katalogu storitev (v nadaljnjem besedilu: storitve, ki se zaračunajo):	5. CERT-EU lahko ***institucijam, organom, uradom in agencijam Unije*** zagotavlja naslednje storitve, ki niso opisane v njegovem katalogu storitev (v nadaljnjem besedilu: storitve, ki se zaračunajo):

Predlog spremembe 50

Predlog uredbe
Člen 12 – odstavek 5 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) storitve, ki podpirajo kibernetsko varnost okolja ***IT*** institucij, organov in agencij Unije, razen storitev iz odstavka 2, in sicer na podlagi sporazumov o ravni storitev in glede na razpoložljive vire;	(a) storitve, ki podpirajo kibernetsko varnost okolja ***IKT*** institucij, organov***, uradov*** in agencij Unije, razen storitev iz odstavka 2, in sicer na podlagi sporazumov o ravni storitev in glede na razpoložljive vire;

Predlog spremembe 51

Predlog uredbe
Člen 12 – odstavek 5 – točka b

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(b) storitve, ki podpirajo operacije ali	(b) storitve, ki podpirajo operacije ali

projekte institucij, organov in agencij Unije za kibernetsko varnost, razen tistih za zaščito njihovih okolij ***IT***, in sicer na podlagi pisnih dogovorov in s predhodno odobritvijo IICB;	projekte institucij, organov***, uradov*** in agencij Unije za kibernetsko varnost, razen tistih za zaščito njihovih okolij ***IKT***, in sicer na podlagi pisnih dogovorov in s predhodno odobritvijo IICB;

Predlog spremembe 52
Predlog uredbe
Člen 12 – odstavek 5 – točka c

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(c) storitve, ki podpirajo varnost okolja ***IT*** organizacij, ki niso institucije, organi in agencije Unije, ki tesno sodelujejo z institucijami, organi in agencijami Unije, ki so jim na primer bile dodeljene naloge ali odgovornosti v skladu s pravom Unije, na podlagi pisnih sporazumov in s predhodno odobritvijo IICB.	(c) storitve, ki podpirajo varnost okolja ***IKT*** organizacij, ki niso institucije, organi***, uradi*** in agencije Unije, ki tesno sodelujejo z institucijami, organi***, uradi*** in agencijami Unije, ki so jim na primer bile dodeljene naloge ali odgovornosti v skladu s pravom Unije, na podlagi pisnih sporazumov in s predhodno odobritvijo IICB.

Predlog spremembe 53

Predlog uredbe
Člen 12 – odstavek 6

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
6. CERT-EU lahko organizira vaje na področju kibernetske varnosti ali priporoča udeležbo na obstoječih vajah, v tesnem sodelovanju z Agencijo Evropske unije za kibernetsko varnost, ***kadar se zdi primerno, da preizkusi*** raven kibernetske varnosti institucij, organov in agencij Unije.	6. CERT-EU lahko organizira vaje na področju kibernetske varnosti ali priporoča udeležbo na obstoječih vajah, ***kadar se presodi kot primerno,***v tesnem sodelovanju z Agencijo Evropske unije za kibernetsko varnost, ***da redno preizkuša*** raven kibernetske varnosti institucij, organov***, uradov*** in agencij Unije. ***Poleg tega lahko CERT-EU z okrepljenim sodelovanjem in skupnimi programi z evropsko kompetenčno mrežo in kompetenčnim centrom za kibernetsko varnost (ECCC) podpre raziskave in inovacije ter pomaga okrepiti zmogljivosti institucij, organov, uradov in agencij Unije na področju kibernetske varnosti.***

Predlog spremembe 54

Predlog uredbe
Člen 12 – odstavek 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
7. CERT-EU ***lahko*** institucijam, organom in agencijam Unije zagotovi pomoč v zvezi z incidenti v tajnih okoljih ***IT***, če to izrecno zahteva ***zadevni udeleženec***.	7. CERT-EU institucijam, organom***,*** ***uradom*** in agencijam Unije zagotovi pomoč v zvezi z incidenti v tajnih okoljih ***IKT***, če to izrecno zahteva ***zadevna institucija, organ, urad ali agencija Unije in če ima CERT-EU potrebne vire za to ali te vire prejme od zadevnega subjekta***.

Predlog spremembe 55

Predlog uredbe
Člen 14 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Vodja CERT-EU IICB in njegovemu predsedniku ***redno*** posreduje poročila o delovanju CERT-EU, finančnem načrtovanju, prihodkih, izvrševanju proračuna, sporazumih o ravni storitev in sklenjenih pisnih sporazumih, sodelovanju s sorodnimi organi in partnerji ter službenih potovanjih osebja, vključno s poročili iz člena 10(1).	Vodja CERT-EU IICB in njegovemu predsedniku ***vsaj enkrat letno*** posreduje poročila o delovanju CERT-EU, finančnem načrtovanju, prihodkih, izvrševanju proračuna, sporazumih o ravni storitev in sklenjenih pisnih sporazumih, sodelovanju s sorodnimi organi in partnerji ter službenih potovanjih osebja, vključno s poročili iz člena 10(1).

Predlog spremembe 56

Predlog uredbe
Člen 16 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. CERT-EU sodeluje in si izmenjuje informacije z nacionalnimi sorodnimi organi v državah članicah, vključno s skupinami CERT, nacionalnimi centri za kibernetsko varnost, skupinami CSIRT in enotnimi kontaktnimi točkami iz člena 8 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih	1. CERT-EU sodeluje in si izmenjuje informacije z nacionalnimi sorodnimi organi v državah članicah, vključno s skupinami CERT, nacionalnimi centri za kibernetsko varnost, skupinami CSIRT in enotnimi kontaktnimi točkami iz člena 8 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih

sistemov], v zvezi s kibernetskimi grožnjami, ranljivostmi in incidenti, možnimi protiukrepi ter vsemi zadevami, pomembnimi za izboljšanje zaščite okolij ***IT*** institucij, organov in agencij Unije, vključno prek mreže skupin CSIRT iz člena 13 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].	sistemov], v zvezi s kibernetskimi grožnjami, ranljivostmi in incidenti, možnimi protiukrepi ter vsemi zadevami, pomembnimi za izboljšanje zaščite okolij ***IKT*** institucij, organov***, uradov*** in agencij Unije, vključno prek mreže skupin CSIRT iz člena 13 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].

Predlog spremembe 57

Predlog uredbe
Člen 16 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. CERT-EU si lahko za olajšanje odkrivanja podobnih kibernetskih groženj in incidentov z nacionalnimi sorodnimi organi v državah članicah izmenjuje z incidenti povezane informacije brez ***soglasja prizadetega udeleženca***. CERT-EU si lahko z incidenti povezane informacije, ki razkrivajo identiteto tarče kibernetskega incidenta, izmenjuje le s soglasjem ***prizadetega udeleženca***.	2. CERT-EU si lahko za olajšanje odkrivanja podobnih kibernetskih groženj in incidentov z nacionalnimi sorodnimi organi v državah članicah izmenjuje z incidenti povezane informacije brez ***dovoljenja prizadete institucije, organa, urada ali agencije Unije, dokler se pri obdelavi osebnih podatkov spoštujejo veljavne določbe Uredbe (EU) 2018/1725***. CERT-EU si lahko z incidenti povezane informacije, ki razkrivajo identiteto tarče kibernetskega incidenta, izmenjuje le s soglasjem ***prizadete institucije, organa, urada ali agencije Unije***.

Predlog spremembe 58

Predlog uredbe
Člen 17 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. CERT-EU lahko s sorodnimi organi, ki niso iz držav članic, vključno s sorodnimi organi iz posameznih industrijskih sektorjev, sodeluje v zvezi z orodji in metodami, kot so tehnike, taktike, postopki in dobre prakse, ter v zvezi s kibernetskimi grožnjami in ranljivostmi. Za vse sodelovanje s takimi sorodnimi organi,	1. CERT-EU lahko s sorodnimi organi, ki niso iz držav članic, vključno s sorodnimi organi iz posameznih industrijskih sektorjev, sodeluje v zvezi z orodji in metodami, kot so tehnike, taktike, postopki in dobre prakse, ter v zvezi s kibernetskimi grožnjami in ranljivostmi. Za vse sodelovanje s takimi sorodnimi organi,

tudi kadar sorodni organi, ki niso iz EU, sodelujejo z nacionalnimi sorodnimi organi držav članic, CERT-EU pridobi predhodno soglasje IICB.	tudi kadar sorodni organi, ki niso iz EU, sodelujejo z nacionalnimi sorodnimi organi držav članic, CERT-EU pridobi predhodno soglasje IICB. ***Pri vsakem takem sodelovanju se spoštuje demokratična celovitost EU.***

Predlog spremembe 59

Predlog uredbe
Člen 17 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. CERT-EU lahko za zbiranje informacij o splošnih in specifičnih kibernetskih grožnjah, ranljivostih in možnih protiukrepih sodeluje z drugimi partnerji, kot so komercialni subjekti, mednarodne organizacije, nacionalni subjekti, ki ne prihajajo iz Evropske unije, ali posamezni strokovnjaki. Za širše sodelovanje s takimi partnerji si CERT-EU pridobi predhodno soglasje IICB.	2. CERT-EU lahko za zbiranje informacij o splošnih in specifičnih kibernetskih grožnjah, ranljivostih in možnih protiukrepih sodeluje z drugimi partnerji, kot so komercialni subjekti, mednarodne organizacije, nacionalni subjekti, ki ne prihajajo iz Evropske unije, ali posamezni strokovnjaki. Za širše sodelovanje s takimi partnerji si CERT-EU pridobi predhodno soglasje IICB. ***Pri vsakem takem sodelovanju se spoštuje demokratična celovitost EU.***

Predlog spremembe 60

Predlog uredbe
Člen 17 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. CERT-EU lahko s soglasjem ***udeleženca***, ki ***ga*** je incident prizadel, partnerjem, ki lahko prispevajo k njegovi analizi, zagotovi z incidentom povezane informacije.	3. CERT-EU lahko s soglasjem ***institucije, organa, urada ali agencije Unije***, ki ***jih*** je incident prizadel, partnerjem, ki lahko prispevajo k njegovi analizi, zagotovi z incidentom povezane informacije.

Predlog spremembe 61

Predlog uredbe
Člen 19 – odstavek -1 (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	-1. Institucije, organi, uradi in agencije Unije lahko CERT-EU prostovoljno predložijo informacije o kibernetskih grožnjah, incidentih, skorajšnjih incidentih in ranljivostih, ki so jih prizadeli. CERT-EU poskrbi, da so na voljo učinkovita komunikacijska sredstva, da se olajša izmenjava informacij s subjekti Unije. CERT-EU lahko da prednost obveznim priglasitvam in jih obravnava pred prostovoljnimi.

Predlog spremembe 62

Predlog uredbe
Člen 19 – odstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
1. Da bi CERT-EU lahko ***usklajeval obvladovanje ranljivosti*** in ***odzivanje na incidente***, lahko ***institucije, organe in agencije*** Unije zaprosi za predložitev informacij iz njihovih zbirk sistemov ***IT***, ***ki so pomembne za podporo CERT-EU. Zaprošena institucija***, ***organ ali agencija*** nemudoma posreduje zahtevane informacije in vse njihove naknadne posodobitve.	1. Da bi CERT-EU lahko ***izvajal svoje poslanstvo*** in ***naloge iz člena 12***, lahko institucije, organe, urade in agencije Unije zaprosi za predložitev informacij iz njihovih zbirk sistemov ***IKT***, ***kar zajema informacije v zvezi s kibernetskimi grožnjami***, ***skorajšnjimi dogodki, ranljivostmi, kazalniki ogroženosti, opozorili glede kibernetske varnosti in priporočili glede konfiguracije orodij za kibernetsko varnost za odkrivanje kibernetskih incidentov. Zaprošeni subjekt*** nemudoma posreduje zahtevane informacije in vse njihove naknadne posodobitve.

Predlog spremembe 63

Predlog uredbe
Člen 19 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Institucije, organi in agencije Unije na zahtevo CERT-EU nemudoma zagotovijo digitalne informacije, ustvarjene	2. Institucije, organi***, uradi*** in agencije Unije na zahtevo CERT-EU nemudoma zagotovijo digitalne informacije, ustvarjene

z elektronskimi napravami, uporabljenimi v zadevnih incidentih. CERT-EU lahko dodatno pojasni, katere vrste takih digitalnih informacij potrebuje za situacijsko zavedanje in odzivanje na incidente.	z elektronskimi napravami, uporabljenimi v zadevnih incidentih. CERT-EU lahko dodatno pojasni, katere vrste takih digitalnih informacij potrebuje za situacijsko zavedanje in odzivanje na incidente.

Predlog spremembe 64
Predlog uredbe
Člen 20 – naslov

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Obveznosti ***obveščanja***	Obveznosti ***poročanja***

Predlog spremembe 65

Predlog uredbe
Člen 20 – odstavek 1 – pododstavek 1

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
Vse institucije, organi in agencije Unije CERT-EU nemudoma ***predložijo začetno priglasitev o*** pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih, vsekakor pa najpozneje 24 ur po seznanitvi z njimi.	Vse institucije, organi***, uredi*** in agencije Unije CERT-EU nemudoma ***poskrbijo za zgodnje opozorilo*** pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih, vsekakor pa najpozneje 24 ur po seznanitvi z njimi. ***V zgodnjem opozorilu bi bilo treba po možnosti navesti, ali obstaja sum, da je pomembni incident nastal zaradi nezakonitih ali zlonamernih dejanj, in ali je verjetno, da bo imel čezmejni učinek.***

Predlog spremembe 66

Predlog uredbe
Člen 20 – odstavek 1 – pododstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
V ustrezno utemeljenih primerih in v dogovoru s CERT-EU ***lahko zadevna institucija, organ ali agencija Unije***	***Zadevna institucija, organ, urad ali agencija Unije lahko*** v ustrezno utemeljenih primerih in v dogovoru s

odstopa od ***roka, določenega v prejšnjem odstavku***.	CERT-EU odstopa od ***tega roka***.

Predlog spremembe 67

Predlog uredbe
Člen 20 – odstavek 2 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Institucije, organi in agencije Unije ***nadalje*** nemudoma ***obvestijo*** CERT-EU o ***ustreznih tehničnih podrobnostih o kibernetskih grožnjah***, ***ranljivostih*** in ***incidentih***, ki omogočajo odkrivanje, odzivanje na ***incidente*** ali blažilne ukrepe. Obvestilo vsebuje naslednje, če so na voljo:	2. ***Poleg tega*** institucije, organi***, uradi*** in agencije Unije nemudoma***, v vsakem primeru pa v 72 urah po tem, ko izvedo za pomembni incident, pošljejo uradno obvestilo*** CERT-EU o ***incidentu, posodobijo zgodnje opozorilo in navedejo začetno oceno pomembnega incidenta***, ***njegovo resnost*** in ***učinek z ustreznimi tehničnimi podrobnostmi***, ki omogočajo odkrivanje, odzivanje na ***incident*** ali blažilne ukrepe. Obvestilo vsebuje naslednje, če so na voljo:

Predlog spremembe 68
Predlog uredbe
Člen 20 – odstavek 2 – pododstavek 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	Zadevna institucija, organ, urad ali agencija Unije lahko v ustrezno utemeljenih primerih in v dogovoru s CERT-EU odstopa od tega roka.

Predlog spremembe 69

Predlog uredbe
Člen 20 – odstavek 2 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2a. Institucije, organi, uradi in agencije Unije najpozneje v enem mesecu po predložitvi obvestila o incidentu organu CERT-EU predložijo končno

poročilo, v katerem navedejo vsaj naslednje:

(a) podroben opis pomembnega incidenta, njegove resnosti in učinka;

(b) vrsto grožnje ali temeljni vzrok, ki je pomembni incident verjetno sprožil;

(c) uporabljene in še potekajoče ukrepe za ublažitev posledic;

(d) po potrebi čezmejni učinek pomembnega incidenta.

Če pomembni incident v času predložitve končnega poročila iz prvega pododstavka še vedno poteka, se predloži poročilo o napredku v tem času, končno poročilo pa v enem mesecu po incidentu.

Predlog spremembe 70

Predlog uredbe
Člen 20 – odstavek 2 b (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	2b. Zadevna institucija, organ, urad ali agencija Unije lahko v ustrezno utemeljenih primerih in v dogovoru s CERT-EU odstopi od roka iz odstavka 2a.

Predlog spremembe 71

Predlog uredbe
Člen 20 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. CERT-EU agenciji ENISA vsak mesec predloži zbirno poročilo, vključno z anonimiziranimi in zbirnimi podatki o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih, priglašenih v skladu z odstavkom 1.	3. CERT-EU agenciji ENISA vsak mesec predloži zbirno poročilo, vključno z anonimiziranimi in zbirnimi podatki o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih, priglašenih v skladu z odstavkom 1. ***To poročilo je prispevek k dveletnemu poročilu o stanju kibernetske varnosti v Uniji iz člena 18 Direktive***

	[predlog revidirane direktive o varnosti omrežij in informacij].

Predlog spremembe 72

Predlog uredbe
Člen 20 – odstavek 4

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
4. IICB ***lahko*** izda smernice ali priporočila v zvezi z načini in vsebino obvestila. CERT-EU razširi ustrezne tehnične podrobnosti, da se institucijam, organom in agencijam Unije omogočijo proaktivno odkrivanje, odzivanje na incidente ali blažilni ukrepi.	4. IICB izda smernice ali priporočila v zvezi z načini in vsebino obvestila. CERT-EU razširi ustrezne tehnične podrobnosti, da se institucijam, organom***, uradom*** in agencijam Unije omogočijo proaktivno odkrivanje, odzivanje na incidente ali blažilni ukrepi.

Predlog spremembe 73

Predlog uredbe
Člen 20 – odstavek 5

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
5. Obveznosti obveščanja ne veljajo za tajne podatke EU in informacije, ki jih institucija, organ ali agencija Unije prejme od varnostne ali obveščevalne službe ali organa kazenskega pregona države članice pod izrecnim pogojem, da se ne bodo delili s CERT-EU.	***črtano***

Predlog spremembe 74

Predlog uredbe
Člen 24 – odstavek 2

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
2. Komisija poroča Evropskemu parlamentu in Svetu o izvajanju te uredbe najpozneje ***48*** mesecev po začetku veljavnosti te uredbe in nato ***vsaka tri leta***.	2. Komisija poroča Evropskemu parlamentu in Svetu o izvajanju te uredbe najpozneje ***36*** mesecev po začetku veljavnosti te uredbe in nato ***vsaki dve leti***.

Predlog spremembe 75

Predlog uredbe
Člen 24 – odstavek 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
3. Komisija oceni delovanje te uredbe in poroča Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij ***pet let*** po datumu začetka veljavnosti.	3. Komisija oceni delovanje te uredbe in ***o tem*** poroča Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij ***tri leta*** po datumu začetka veljavnosti***, saj se krajina kibernetskih groženj hitro razvija***.

Predlog spremembe 76

Predlog uredbe
Priloga I – odstavek 1 – uvodni del

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
V osnovnih ukrepih za kibernetsko varnost se obravnavajo naslednja področja:	V osnovnih ukrepih za kibernetsko varnost se obravnavajo ***vsaj*** naslednja področja:

Predlog spremembe 77

Predlog uredbe
Priloga I – odstavek 1 – točka 1 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(1a) usposabljanje zaposlenih na področju kibernetske varnosti;

Predlog spremembe 78

Predlog uredbe
Priloga I – odstavek 1 – točka 3

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(3) upravljanje sredstev, vključno s popisom sredstev ***IT*** in kartografijo omrežja ***IT***;	(3) ***nakup in*** upravljanje sredstev, vključno s popisom sredstev ***IKT*** in kartografijo omrežja ***IKT***;

Predlog spremembe 79

Predlog uredbe
Priloga I – odstavek 1 – točka 7

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(7) nakup, razvoj in vzdrževanje sistemov;	(7) nakup, razvoj in vzdrževanje sistemov***, vključno z razvojem interne odprtokodne programske opreme***;

Predlog spremembe 80

Predlog uredbe
Priloga I – odstavek 1 – točka 7 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(7a) revizije kibernetske varnosti;

Predlog spremembe 81

Predlog uredbe
Priloga I – odstavek 1 – točka 9

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(9) obvladovanje incidentov, vključno s pristopi za izboljšanje pripravljenosti na incidente, odzivanje nanje in okrevanje po njih, ter s sodelovanjem s CERT-EU, kot je ohranjanje varnostnega spremljanja in vodenja dnevnikov;	(9) obvladovanje incidentov, vključno s pristopi za izboljšanje pripravljenosti na incidente, odzivanje nanje in okrevanje po njih, ***izpolnjevanjem obveznosti poročanja in skrajšanjem časa za njihovo izpolnitev*** ter s sodelovanjem s CERT-EU, kot je ohranjanje varnostnega spremljanja in vodenja dnevnikov;

Predlog spremembe 82

Predlog uredbe
Priloga II – odstavek 1 – točka 3 a (novo)

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
	(3a) redno usposabljanje zaposlenih na področju kibernetske varnosti;

Predlog spremembe 83

Predlog uredbe
Priloga II – odstavek 1 – točka 4 – točka a

Besedilo, ki ga predlaga Komisija	*Predlog spremembe*
(a) z odpravo pogodbenih ovir, ki omejujejo izmenjavo informacij med ponudniki storitev ***IT*** in CERT-EU o incidentih, ***šibkih točkah*** in kibernetskih grožnjah;	(a) z odpravo pogodbenih ovir, ki omejujejo izmenjavo informacij med ponudniki storitev ***IKT*** in CERT-EU o incidentih, ***ranljivostih*** in kibernetskih grožnjah;

POSTOPEK V ODBORU, ZAPROŠENEM ZA MNENJE

Naslov	Določitev ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije
Referenčni dokumenti	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Pristojni odbor Datum razglasitve na zasedanju	ITRE 4.4.2022
Mnenje pripravil Datum razglasitve na zasedanju	AFCO 4.4.2022
Pripravljavec/-ka mnenja Datum imenovanja	Markéta Gregorová 20.6.2022
Obravnava v odboru	26.10.2022 1.12.2022
Datum sprejetja	25.1.2023
Izid končnega glasovanja	+: 24 –: 0 0: 0
Poslanci, navzoči pri končnem glasovanju	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Namestniki, navzoči pri končnem glasovanju	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Namestniki (člen 209(7)), navzoči pri končnem glasovanju	Leszek Miller

POIMENSKO GLASOVANJE PRI KONČNEM GLASOVANJU V ODBORU, ZAPROŠENEM ZA MNENJE

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Uporabljeni znaki:
+ : za
- : proti
0 : vzdržani