II

(Nezakonodajni akti)

PRIPOROČILA

PRIPOROČILO KOMISIJE (EU) 2021/1086

z dne 23. junija 2021

o vzpostavitvi skupne kibernetske enote

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 292 Pogodbe,

ob upoštevanju naslednjega:

(1) Kibernetska varnost je bistvena za uspeh digitalne preobrazbe gospodarstva in družbe. EU se je zavezala za največje naložbe doslej, da bi zagotovila zaupanje ljudi, podjetij in javnih organov digitalnim orodjem.

(2) V pandemiji COVID-19 se sta se povečala pomen povezljivosti in odvisnost Evrope od stabilnih omrežij in informacijskih sistemov, pokazala pa se je tudi potreba po zaščiti celotne dobavne verige. Zanesljivo in varno omrežje in informacijski sistemi so še posebej pomembni za subjekte, ki so na čelu boja proti pandemiji, kot so bolnišnice, zdravstvene agencije in proizvajalci cepiv. Usklajevanje dejavnosti EU za preprečevanje, odkrivanje, oviranje in zmanjševanje najhujših kibernetskih napadov na take subjekte in odzivanje nanje bi lahko preprečilo izgubo človeških življenj in poskuse slabitve sposobnosti EU, da čim prej premaga pandemijo. Poleg tega krepitev sposobnosti EU za učinkovito preprečevanje kibernetskih napadov prispeva k napredku svetovnega, odprtega, stabilnega in varnega kibernetskega prostora.

(3) Spričo čezmejne narave kibernetskih groženj in nenehnega naraščanja bolj zapletenih, razširjenih in ciljno usmerjenih napadov ([1]) bi morali ustrezne institucije in akterji za kibernetsko varnost okrepiti svojo sposobnost odzivanja na take grožnje in napade z izkoriščanjem obstoječih virov in boljšim usklajevanjem dejavnosti. Vsi ustrezni akterji v EU morajo biti pripravljeni na skupen odziv in izmenjavo informacij po načelu „potrebe po izmenjavi“ in ne po načelu „potrebe po seznanitvi“.

(4) Čeprav je bil s sodelovanjem med državami članicami na področju kibernetske varnosti, zlasti preko skupine za sodelovanje (skupina za sodelovanje na področju varnosti omrežij in informacij) in mreže skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT), ustanovljenih na podlagi Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta ([2]), dosežen velik napredek, še vedno ni skupne platforme EU, kjer bi bila možna učinkovita in varna izmenjava informacij, zbranih v različnih skupnostih za kibernetsko varnost, in kjer bi lahko ustrezni akterji usklajevali in mobilizirali operativne zmogljivosti. Zato obstaja nevarnost, da bi se kibernetske grožnje in incidenti reševali v ozkih okvirih, kar bi zmanjšalo učinkovitost in povečalo ranljivost. Poleg tega na ravni EU manjka kanal za tehnično in operativno sodelovanje z zasebnim sektorjem tako v smislu izmenjave informacij kot tudi v smislu podpore pri odzivanju na incidente.

([1]) ENISA, 2020 Threat Landscape; Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020 (Ocena ogroženosti zaradi internetnega organiziranega kriminala (IOCTA), 2020).

([2]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

(5) Obstoječi okviri, strukture, viri in strokovno znanje, ki so na voljo v državah članicah in ustreznih institucijah, organih in agencijah EU, dajejo trdno podlago za skupen odziv na kibernetske grožnje, incidente in krize ([3]). V to obstoječo arhitekturo spadajo na operativni strani načrt za usklajen odziv na obsežne kibernetske incidente in krize (Načrt) ([4]), mreža skupin CSIRT, evropska organizacijska mreža za povezovanje v kibernetski krizi (EU CyCLONe) ([5]), Evropski center za boj proti kibernetski kriminaliteti (EC3), skupna projektna skupina za kibernetski kriminal (J-CAT) pri Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) in protokol EU za odzivanje organov kazenskega pregona na izredne razmere (EU LE ERP). K sodelovanju na področju politik in operativnemu sodelovanju v različnih skupnostih za kibernetsko varnost prispevajo tudi skupina za sodelovanje na področju varnosti omrežij in informacij, Obveščevalni in situacijski center EU (EU INTCEN), zbirka orodij za kibernetsko diplomacijo ([6]) in projekti v zvezi s kibernetsko obrambo v okviru stalnega strukturnega sodelovanja (PESCO) ([7]). Evropska agencija za kibernetsko varnost (ENISA) ima po razširitvi pooblastil nalogo podpirati operativno sodelovanje ([8]) glede kibernetske varnosti omrežij in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje in incidenti. EU lahko z enotnimi ureditvami za politično odzivanje na krize (IPCR) usklajuje svoj politični odziv na večje krize, tudi v primeru velikih kibernetskih napadov.

(6) Toda mehanizem za izkoriščanje obstoječih virov in zagotavljanje vzajemne pomoči med skupnostmi za kibernetsko varnost, odgovornimi za varnost omrežij in informacijskih sistemov, boj proti kibernetski kriminaliteti, izvajanje kibernetske diplomacije in po potrebi kibernetske obrambe v primeru krize še ne obstaja. Prav tako ne obstaja celovit mehanizem na ravni EU za tehnično in operativno sodelovanje med vsemi skupnostmi pri situacijskem zavedanju, pripravljenosti in odzivu. Nadalje bi bilo treba tudi preko Europola oziroma INTCEN doseči sinergije s skupnostmi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter obveščevalnimi skupnostmi.

(7) Komisija, visoki predstavnik Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik), države članice ter ustrezne institucije, organi in agencije EU priznavajo pomen analize prednosti, slabosti, vrzeli in prekrivanj v sedanji arhitekturi kibernetske varnosti EU, ki je nastala v zadnjih letih. Komisija je v posvetovanju z državami članicami in ob sodelovanju visokega predstavnika zasnovala skupno kibernetsko enoto kot odziv na to analizo in pomembno sestavino strategije EU za varnostno unijo ([9]), digitalne strategije ([10]) in strategije za kibernetsko varnost ([11]).

([3]) Evropsko organizacijsko mrežo za povezovanje v kibernetski krizi (EU CyCLONe) so ustanovile države članice kot odziv na priporočilo iz Načrta. To je mreža nacionalnih operativnih strokovnjakov in strokovnjakov za obvladovanje krize, za katero je Komisija predlagala, da se jo kodificira z direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in o razveljavitvi Direktive (EU) 2016/1148, COM(2020) 823 final, 2020/0359 (COD), ki je bila predlagana decembra 2020.

([4]) Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

([5]) V tem priporočilu je upoštevano poročilo po izvedbi načrta na operativni ravni (Blue OLEx) iz leta 2020 in zlasti povzetek predsedujočega o razpravi o strateški politiki glede skupne kibernetske enote.

([6]) Sklepi Sveta o okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“) z dne 19. junija 2017 (9916/17).

([7]) Zlasti projekta PESCO „enote za hitro odzivanje na kibernetske grožnje in medsebojno pomoč na področju kibernetske varnosti“, ki ga usklajuje Litva, in „center za usklajevanje na kibernetskem in informacijskem področju“, ki ga usklajuje Nemčija.

([8]) V skladu s členom 7 Uredbe (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) mora Agencija podpirati operativno sodelovanje med državami članicami ter institucijami, organi, uradi in agencijami Unije ter med deležniki. Sem spada tudi podpora državam članicam glede operativnega sodelovanja v mreži skupin CSIRT, priprave rednega poglobljenega tehničnega poročila o stanju na področju kibernetske varnosti v EU glede incidentov in kibernetskih groženj ter prispevanje k oblikovanju sodelovalnega odziva na velike čezmejne incidente ali krize na ravni Unije in držav članic. Poleg tega agencija ENISA prispeva k dejavnostim usposabljanja skupaj z Evropsko akademijo za varnost in obrambo (ESDC).

([9]) Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o strategiji EU za varnostno unijo (COM/2020/605 final).

([10]) Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij: Oblikovanje digitalne prihodnosti Evrope (COM/2020/67 final).

([11]) Skupno sporočilo Evropskemu parlamentu in Svetu, Strategija EU za kibernetsko varnost v digitalnem desetletju (JOIN/2020/18 final).

(8) Države članice bi morale imeti v primeru krize možnost, da računajo na solidarnost EU v obliki usklajene pomoči, tudi od vseh štirih kibernetskih skupnosti, tj. civilne skupnosti, skupnosti za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ([12]), diplomacije in po potrebi obrambe. Stopnja posredovanja udeležencev iz ene ali več skupnosti je lahko odvisna od narave velikega incidenta ali krize, torej tudi od vrste protiukrepov, ki bodo potrebni za odziv nanjo. Pri soočanju s kibernetskimi grožnjami, incidenti in krizami so dobro usposobljeni strokovnjaki in tehnična oprema bistvena sredstva, ki lahko prispevajo k preprečevanju velike škode in učinkovitemu okrevanju. Zato bodo v skupni kibernetski enoti najpomembnejše jasno določene tehnične in operativne zmogljivosti, predvsem strokovnjaki in oprema, ki jih bo mogoče po potrebi poslati v države članice. V okviru te platforme bodo imeli udeleženci edinstveno možnost za razvoj in usklajevanje takih zmogljivosti preko skupin EU za hiter odziv na področju kibernetske varnosti, hkrati pa bodo zagotavljali ustrezne sinergije z obstoječimi projekti kibernetske varnosti v okviru PESCO.

(9) Skupna kibernetska enota zagotavlja virtualno in fizično platformo, zanjo pa ni potrebna ustanovitev dodatnega samostojnega organa. Njen ustroj ne bi smel vplivati na pristojnosti in pooblastila nacionalnih organov za kibernetsko varnost in ustreznih subjektov Unije. Skupna kibernetska enota bi morala biti določena v memorandumih o soglasju med njenimi udeleženci. Izhajati bi morala iz obstoječih struktur, virov in zmogljivosti in jim dodajati vrednost kot platforma za varno in hitro operativno ter tehnično sodelovanje med subjekti EU in organi držav članic. Poleg tega bi morala povezovati vse skupnosti za kibernetsko varnost, tj. civilno skupnost, skupnost za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, diplomacijo in obrambo. Udeleženci platforme bi morali imeti operativno ali podporno vlogo. Med operativnimi udeleženci bi morali biti agencija ENISA, Europol, skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU), Komisija, Evropska služba za zunanje delovanje (vključno z INTCEN), mreža skupin CSIRT in mreža EU-CyCLONe. Med podpornimi udeleženci bi morali biti Evropska obrambna agencija (EDA), predsedujoči skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov, predsedujoči horizontalne delovne skupine za kibernetska vprašanja Sveta in en predstavnik zadevnih projektov PESCO ([13]). Ker imajo države članice operativne zmogljivosti in pristojnosti za odziv na velike kibernetske grožnje, incidente in krize, bi morali udeleženci platforme za dosego svojih ciljev uporabljati predvsem svoje zmogljivosti, pri čemer bi jim pomagali ustrezni subjekti Unije.

(10) Skupna kibernetska enota bi morala dati nov zagon procesu, ki se je začel leta 2017 z Načrtom. Morala bi nadalje operacionalizirati arhitekturo iz Načrta in narediti odločilen korak v smeri evropskega okvira za krizno upravljanje kibernetske varnosti za usklajeno in pravočasno prepoznavanje in zmanjševanje groženj in tveganj ter odziv nanje. S takim korakom bi morala skupna kibernetska enota pomagati EU pri odzivu na sedanje in preteče grožnje.

(11) Operativni in podporni udeleženci bi morali s sodelovanjem v skupni kibernetski enoti imeti možnost za navezovanje stikov s širšim krogom deležnikov v okviru EU za odzivanje na krize na področju kibernetske varnosti. Udeleženci bi morali pri izvajanju svojih funkcij v mejah pooblastil imeti korist od okrepljene pripravljenosti in širšega situacijskega zavedanja, ki zajema vse vidike kibernetskih groženj in incidentov, ter izkoristiti dodatno strokovno znanje na področju kibernetske varnosti. Npr. udeleženci bi morali redno sodelovati na vajah, na katerih sodeluje več skupnosti, dobiti bi morali jasno opredeljeno vlogo v načrtu EU za odzivanje na kibernetske incidente, povečati bi morali prepoznavnost svojih ukrepov preko skupnega obveščanja javnosti in sklepati sporazume o operativnem sodelovanju z zasebnim sektorjem. Vzporedno s tem bi morali udeleženci s prispevanjem k skupni kibernetski enoti dobiti možnost za krepitev obstoječih mrež, kot sta mreža skupin CSIRT in mreža EU-CyCLONe, dobiti na razpolago varna orodja za izmenjavo informacij in boljše zmogljivosti za odkrivanje (tj. centri za operativno varnost (SOC)) ter dobiti možnost za izkoriščanje razpoložljivih operativnih zmogljivosti EU.

(12) Udeleženci v skupni kibernetski enoti bi se morali osredotočiti na tehnično in operativno sodelovanje, tudi na skupne operacije. Udeleženci bi morali k takemu sodelovanju prispevati v okviru svojih pooblastil. Sodelovanje bi moralo izhajati iz tekočih dejavnosti in jih dopolnjevati. Glede na vrsto zadevnega sodelovanja lahko pri njem sodelujejo tudi dodatni udeleženci.

([12]) Pomembno tudi za pravosodno sodelovanje.

([13]) Glej opombo 5. Evropska služba za zunanje delovanje in EDA se bosta preko svoje vloge kot sekretariat PESCO povezala s koordinatorji ustreznih projektov PESCO.

(13) Platforma bi morala zbirati strokovnjake za tehnično in operativno obvladovanje krize iz držav članic in subjektov EU, da bi usklajevali odziv na kibernetske grožnje, incidente in krize z uporabo obstoječih zmogljivosti in strokovnega znanja. Strokovnjaki, ki bodo sodelovali v skupni kibernetski enoti, bodo lahko spremljali in varovali veliko večjo napadno površino z uporabo fizične in virtualne platforme. V ta namen bi morali udeleženci preko platforme usklajevati svoje dejavnosti v primeru čezmejnih incidentov in kriz ter pomoč državam, ki so jih prizadeli incidenti.

(14) Za nastanek skupne kibernetske enote je potreben postopen proces z izkoriščanjem in utrjevanjem obstoječih okvirov in struktur, navedenih v tem priporočilu, vključno z mehanizmi sodelovanja, ki so jih vzpostavile države članice, vodenih forumov (npr. mreže skupin CSIRT, mreže EU CyCLONe, horizontalne delovne skupine za kibernetska vprašanja Sveta, skupine J-CAT in ustreznih projektov PESCO) ter na strani institucij, organov in agencij EU strukturiranega sodelovanja med agencijo ENISA, skupino CERT-EU in medinstitucionalno skupino za izmenjavo informacij o kibernetski varnosti. Ustrezno bi bilo treba vključiti okvire za hibridne grožnje, civilno zaščito ([14]) in sektorske okvire ([15]). Podobno bi bilo treba ustvariti strukturirano povezavo z ureditvami IPCR ([16]). To bo v primeru krize omogočilo hiter in učinkovit prenos informacij do nosilcev odločanja na politični ravni, zbranih v Svetu.

(15) Postopek ustanovitve skupne kibernetske enote bi zato moral biti postopen in pregleden, končati pa bi se moral v naslednjih dveh letih. Iz tega razloga bi bilo treba cilje iz tega priporočila doseči v postopku iz štirih faz, opisanem v Prilogi k temu priporočilu. V prvih dveh fazah bi bilo treba začeti pripravljalni postopek, ki bi ga organizirala in podpirala agencija ENISA, v njem pa bi sodelovali operativni in podporni udeleženci na ravni EU in držav članic; potekati bi moral v delovni skupini, ki bi jo ustanovila Komisija. Priprave bi morale potekati v znamenju obojestranske angažiranosti, vključevanja in doseganja soglasja. Spodbujati bi bilo treba sodelovanje vseh udeležencev, ki bi omogočalo izražanje različnih pogledov in stališč ter prizadevanje za rešitve, ki bi bile deležne čim večje podpore. Glede na potrebe in v upravičenih pogojih se časovnica za različne faze, navedena v tem priporočilu, lahko prilagodi.

(16) V prvi fazi bi se morale začeti priprave z določitvijo ustreznih razpoložljivih operativnih zmogljivosti EU ter začetkom ocene vlog in odgovornosti udeležencev v okviru platforme. Druga faza bi morala vključevati pripravo načrta odzivanja EU na incidente in krize v skladu z Načrtom ([17]) in protokolom EU za odzivanje organov kazenskega pregona na izredne razmere, začetek izvajanja dejavnosti v zvezi s pripravljenostjo in situacijskim zavedanjem v skladu z aktom o kibernetski varnosti in uredbo o Europolu ([18]) ter zaključek ocenjevanja vlog in odgovornosti udeležencev v okviru platforme. Delovna skupina bi morala rezultate tega ocenjevanja predstaviti Komisiji in visokemu predstavniku, ki jih bosta posredovala Svetu. Komisija in visoki predstavnik bi morala v skladu s svojimi pristojnostmi na podlagi te ocene ob medsebojnem sodelovanju pripraviti skupno poročilo in pozvati Svet, da ga podpre s svojimi sklepi.

(17) Po tem izrazu podpore bo skupna kibernetska enota pripravljena za delovanje, da bi bili dokončani še preostali dve fazi postopka. V tretji fazi bi morali imeti udeleženci možnost, da uporabijo skupine EU za hiter odziv v skupni kibernetski enoti po postopkih, ki bodo opredeljeni v načrtu odzivanja EU na incidente in krize ter bodo izkoriščali tako fizično kot virtualno platformo in prispevali k različnim vidikom odziva na incidente (od obveščanja javnosti do okrevanja po incidentu). V četrti fazi bodo k prispevanju k platformi pozvani deležniki iz zasebnega sektorja, tudi uporabniki in ponudniki rešitev in storitev kibernetske varnosti, kar bo udeležencem omogočilo, da izboljšajo izmenjavo informacij in okrepijo usklajeni odziv EU na kibernetske grožnje in incidente.

([14]) V tej zvezi bi morala skupna kibernetska enota doseči sinergije z mehanizmom Unije na področju civilne zaščite (UCPM) za boljšo evropsko pripravljenost in odzivnost v primeru večvrstnih nesreč in izrednih razmer s kibernetskimi elementi.

([15]) Kot je predvideno za finančni sektor v Uredbi (EU) 2021/xx Evropskega parlamenta in Sveta* [DORA].

([16]) Glej uvodno izjavo 5.

([17]) Glej opombo 3.

([18]) Uredba (EU) 2016/794 Evropskega parlamenta in Sveta z dne 11. maja 2016 o Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) ter nadomestitvi in razveljavitvi sklepov Sveta 2009/371/PNZ, 2009/934/PNZ, 2009/935/PNZ, 2009/936/PNZ in 2009/968/PNZ (UL L 135, 24.5.2016, str. 53).

(18) Ob koncu postopka v štirih fazah bi morali udeleženci pripraviti poročilo o dejavnosti s predstavitvijo napredka pri izvajanju štirih faz, določenih v priporočilu, in opisom dosežkov in izzivov ter ga predložiti Komisiji in visokemu predstavniku. Komisija in visoki predstavnik bi morala na podlagi tega poročila opraviti oceno teh rezultatov in podati ugotovitve glede prihodnosti skupne kibernetske enote.

(19) Komisija, agencija ENISA, Europol in skupina CERT-EU bi morali skupni kibernetski enoti nuditi upravno, finančno in tehnično pomoč v skladu z oddelkom IV tega priporočila, če bodo na voljo proračunska sredstva in človeški viri. Okrepitev ustreznih operativnih zmogljivosti za kibernetsko varnost institucij, organov in agencij EU bo ključnega pomena za zagotovitev učinkovite priprave in trajnostnosti skupne kibernetske enote. Komisija namerava zagotoviti, da bo uredba o skupnih zavezujočih pravilih za kibernetsko varnost institucij, organov in agencij EU, ki je v postopku (oktober 2021), vsebovala pravno podlago za ta prispevek v primeru skupine CERT-EU.

(20) Agencija ENISA ima glede na svoja okrepljena pooblastila na podlagi Uredbe (EU) 2019/881 (akt o kibernetski varnosti) edinstvene možnosti za organiziranje in pripravo skupne kibernetske enote ter za prispevek k njeni operacionalizaciji. V skladu z določbami akta o kibernetski varnosti trenutno ustanavlja urad v Bruslju za podporo strukturiranemu sodelovanju s skupino CERT-EU. Strukturirano sodelovanje, vključno s sosednjimi pisarnami, zagotavlja koristen okvir za lažji nastanek skupne kibernetske enote, tudi z vzpostavitvijo njenega fizičnega prostora, ki bi moral biti po potrebi na voljo udeležencem ter osebju drugih ustreznih institucij, organov in agencij EU. Fizično platformo bi bilo treba kombinirati z virtualno platformo, sestavljeno iz orodij za sodelovanje in varno izmenjavo informacij. Ta orodja bodo izkoristila bogastvo informacij, zbranih preko evropskega kibernetskega ščita ([19]), vključno s centri za varnostne operacije (SOC) ter centri za izmenjavo in analizo informacij (ISAC).

(21) V protokolu EU za odzivanje organov kazenskega pregona na izredne razmere za večji čezmejni kibernetski napad, ki ga je Svet sprejel leta 2018, ima osrednjo vlogo Europolov Evropski center za boj proti kibernetski kriminaliteti (EC3) ([20]) kot del okvira Načrta. Ta protokol organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v EU omogoča odziv na velike čezmejne napade domnevno zlonamerne narave po načelu 24/7 s hitrim odzivom in oceno ter varno in pravočasno izmenjavo kritičnih informacij za učinkovito usklajevanje odzivov na čezmejne incidente. V protokolu je nadalje razčlenjeno sodelovanje z drugimi institucijami EU in kriznimi protokoli povsod po EU ter krizno sodelovanje z zasebnim sektorjem. Skupnost za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj bi morala, po potrebi s podporo Europola, prispevati k skupni kibernetski enoti s sprejetjem ustreznih ukrepov v celotnem preiskovalnem ciklu v skladu z zahtevami okvira za kazensko pravosodje in postopkih za elektronsko obravnavo dokazov, ki se uporabljajo. Europol nudi operativno podporo in omogoča lažje operativno sodelovanje v boju proti kibernetskim grožnjam od začetka delovanja Evropskega centra za boj proti kibernetski kriminaliteti leta 2013. Platformo bi moral podpirati skladno s svojimi pooblastili in pristopom obveščevalno vodene policijske dejavnosti, hkrati pa izkoriščati vse vrste svojega internega strokovnega znanja, proizvodov, orodij in storitev, ki so pomembne za odziv na incidente ali krize.

(22) Tudi v skladu z Direktivo 2013/40/EU o napadih na informacijske sisteme morajo države članice zagotoviti, da imajo operativno nacionalno kontaktno točko, ki je dosegljiva 24 ur na dan vse dni v tednu, za izmenjavo informacij v zvezi s kaznivimi dejanji, opredeljenimi v navedeni direktivi. Tudi omrežje operativnih nacionalnih kontaktnih točk bi moralo prispevati k skupni kibernetski enoti, in sicer tako, da bi po potrebi zagotovilo sodelovanje organov držav članic za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

(23) Kibernetska diplomacija EU prispeva k spodbujanju in zaščiti svetovnega, odprtega, stabilnega in varnega kibernetskega prostora ter k preprečevanju in odvračanju zlonamernih kibernetskih dejavnosti in odzivanju nanje. EU je leta 2017 vzpostavila okvir za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“). Ta okvir je sestavni del širše politike kibernetske diplomacije EU. Prispeva k preprečevanju konfliktov in večji stabilnosti v mednarodnih odnosih. EU in državam članicam omogoča, da, po potrebi v sodelovanju z mednarodnimi partnerji, uporabijo vse ukrepe skupne zunanje in varnostne politike (CFSP) v skladu z ustreznimi postopki za njihovo doseganje ter z njimi spodbujajo sodelovanje, zmanjšujejo grožnje ter vplivajo na sedanje in morebitno prihodnje zlonamerno ravnanje v kibernetskem prostoru. Skupnost kibernetske diplomacije bi morala sodelovati v skupni kibernetski enoti z uporabo in zagotavljanjem pomoči pri uporabi celotnega nabora diplomatskih ukrepov, zlasti glede obveščanja javnosti, ter tako podpirati skupno situacijsko zavedanje in navezavo stikov s tretjimi državami v primeru krize.

([19]) JOIN/2020/18 final, oddelek 1.2.
([20]) Ustanovljen z Uredbo (EU) 2016/794.

(24) Visoki predstavnik bi moral v skladu z okvirom iz Načrta prispevati k skupni kibernetski enoti tako, da bi, tudi preko INTCEN, na podlagi obveščevalnih podatkov zagotavljal stalno skupno situacijsko zavedanje o obstoječih in nastajajočih grožnjah, vključno s potrebnim strateškim situacijskim zavedanjem za kateri koli dogodek.

(25) V skupnosti za kibernetsko obrambo je namen EU in držav članic okrepiti zmogljivosti za kibernetsko obrambo in še okrepiti sinergije, usklajevanje in sodelovanje med ustreznimi institucijami, organi in agencijami EU ter med državami članicami, tudi glede misij in operacij v okviru skupne varnostne in obrambne politike. Funkcije skupnosti temeljijo na medvladnem upravljanju na ravni EU, nacionalnih vojaških strukturah poveljevanja ter vojaških zmogljivostih in sredstvih ali zmogljivostih in sredstvih z dvojno rabo. Zaradi njene posebne narave bi bilo treba vzpostaviti posebne stične točke s skupno kibernetsko enoto, da bi omogočili souporabo informacij s skupnostjo za kibernetsko obrambo ([21]).

(26) Stalno strukturno sodelovanje je pravni okvir, ki je bil uveden z Lizbonsko pogodbo ([22]) in vzpostavljen leta 2017 z okvirom Unije. Strukturno sodelovanje je omogočilo izvedbo več projektov PESCO na kibernetskem področju in tako prispevalo k izpolnitvi zaveze št. 11 ([23]), da bo „zagotovljena okrepitev dejavnosti pri sodelovanju na področju kibernetske obrambe, kot so souporaba informacij, usposabljanje in operativna podpora“. Evropska služba za zunanje delovanje skupaj z Vojaškim štabom EU in EDA tvori sekretariat PESCO, ki zagotavlja enotno kontaktno točko v okviru Unije za vse zadeve v zvezi s PESCO, vključno s podpiranjem in usklajevanjem funkcij v zvezi s projekti PESCO (npr. ocena predlogov novih projektov, priprava poročil o napredku projektov itd.). Predstavniki zadevnih projektov PESCO bi morali skupno kibernetsko enoto podpirati predvsem glede situacijskega zavedanja in pripravljenosti.

(27) Udeleženci bi morali preko skupne kibernetske enote ustrezno vključiti deležnike iz zasebnega sektorja, vključno s ponudniki in uporabniki rešitev in storitev kibernetske varnosti, in tako podpreti evropski okvir za obvladovanje kriz na področju kibernetske varnosti ob upoštevanju pravnega okvira za izmenjavo podatkov in varnosti informacij. Ponudniki kibernetske varnosti bi morali k pobudi prispevati z omogočanjem souporabe obveščevalnih podatkov o grožnjah in zagotavljanjem osebja za odziv na incidente, s katerim bi hitro okrepili zmogljivost enote za odziv na velike napade in krize. Uporabnikom blaga in storitev na področju kibernetske varnosti, zlasti tistim s področja uporabe direktive o varnosti omrežij in informacijskih sistemov, bi moralo biti omogočeno, da zaprosijo za pomoč in svetovanje preko strukturiranih kanalov (ki jih zdaj še ni), povezanih s centri za izmenjavo in analizo informacij na ravni EU ([24]). Platforma bi lahko prispevala tudi h krepitvi sodelovanja z mednarodnimi partnerji.

(28) Za krepitev in ohranitev situacijskega zavedanja so potrebne najsodobnejše zmogljivosti za odkrivanje in preprečevanje vdorov. Skupna kibernetska enota bi morala imeti na razpolago najsodobnejše omrežje, ki bo lahko analiziralo zlonamerne grožnje in incidente, ki bi lahko vplivali na ključne komunikacijske in informacijske sisteme povsod po Uniji. To pomeni, da bi bilo treba skupni kibernetski enoti posredovati podatke o grožnjah, pridobljene med drugim iz komunikacijskih omrežij, ki jih spremljajo nacionalni, sektorski in čezmejni centri za varnostne operacije, da bi tako izboljšali oceno udeležencev o okolju groženj v EU.

(29) Za podporo izmenjavi operativnih informacij, ki bodo morda vsebovale tudi zaupno gradivo, bi morala platforma uporabljati primerno varne komunikacijske kanale. Taki kanali bi lahko izhajali iz obstoječe infrastrukture, kot je mrežna aplikacija za varno izmenjavo informacij (SIENA), ki jo uporabljata Europol in skupnost za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Kot je napovedano v strategiji za kibernetsko varnost, bi morala orodja, ki jih uporabljajo institucije, organi in agencije EU, spoštovati pravila o varovanju tajnosti podatkov, ki jih bo kmalu predlagala Komisija.

([21]) Predvsem preko predstavništva Evropske službe za zunanje delovanje, da bi omogočili ustrezno sodelovanje skupnosti za kibernetsko obrambo, ki bo temeljilo na prostovoljnih nacionalnih prispevkih.

([22]) Člen 42(6), člen 46 in Protokol 10 PEU.

([23]) Vsaka država članica, ki sodeluje v PESCO, poda 20 posamičnih zavez, razdeljenih na pet ključnih področij v skladu s členom 2 Protokola št. 10 o PESCO, ki je priloga k Pogodbi o Evropski uniji.

([24]) Pomembna primera obstoječih centrov za izmenjavo in analizo informacij, ki bi lahko sodelovali pri taki souporabi, sta med drugim center za izmenjavo in analizo informacij na področju evropske energetike (EE-ISAC) ali center za izmenjavo in analizo informacij evropskih finančnih institutov.

(30) Komisija bo predvsem preko programa za digitalno Evropo podpirala potrebne naložbe za vzpostavitev fizične in virtualne platforme, vzpostavitev in vzdrževanje varnih komunikacijskih kanalov in zmogljivosti za usposabljanje ter za razvoj in uvajanje zmogljivosti za odkrivanje. Poleg tega bi lahko Evropski obrambni sklad pomagal pri financiranju ključnih tehnologij in zmogljivosti kibernetske obrambe, ki bi okrepile nacionalno pripravljenost za kibernetsko obrambo –

SPREJELA NASLEDNJE PRIPOROČILO:

I. **NAMEN PRIPOROČILA**

(1) Namen tega priporočila je določiti potrebne ukrepe za usklajevanje dejavnosti EU za preprečevanje, odkrivanje, oviranje in zmanjševanje velikih kibernetskih incidentov in kriz s pomočjo skupne kibernetske enote. V ta namen so v tem priporočilu opredeljeni tudi postopek, mejniki in časovnica, ki bi se jih morale držati države članice in ustrezne institucije, organi in agencije EU v zvezi z nastankom in razvojem navedene platforme.

(2) Države članice in ustrezne institucije, organi in agencije EU bi morale zagotoviti, da bodo v primeru velikih kibernetskih incidentov in kriz usklajevale svoje dejavnosti preko skupne kibernetske enote, ki omogoča vzajemno pomoč ([25]) s strokovnim znanjem organov držav članic in ustreznih institucij, organov in agencij EU. Skupna kibernetska enota bi morala udeležencem omogočati tudi vzpostavitev sodelovanja z zasebnim sektorjem.

II. **OPREDELITEV POJMOV**

(3) V tem priporočilu se uporabljajo naslednje opredelitve pojmov:

(a) „načrt odzivanja EU na kibernetske incidente in krize“ pomeni zbirko vlog, načinov in postopkov za dokončanje okvira EU za odzivanje na krize na področju kibernetske varnosti iz točke 1 Priporočila komisije z dne 13. septembra 2017 o načrtu za usklajen odziv na obsežne kibernetske incidente in krize (v nadaljnjem besedilu: Načrt);

(b) „skupnosti za kibernetsko varnost“ pomeni sodelovalne civilne skupnosti, skupnosti za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, diplomatske in obrambne skupnosti, ki predstavljajo države članice in ustrezne institucije, organe in agencije EU, ki si izmenjujejo informacije za dosego skupnih ciljev, interesov in nalog v zvezi s kibernetsko varnostjo;

(c) „udeleženci iz zasebnega sektorja“ pomeni predstavnike zasebnega sektorja, ki dajejo na voljo ali uporabljajo rešitve ([26]) in storitve ([27]) kibernetske varnosti;

(d) „velik incident“ pomeni incident, kakor je opredeljen v členu 4(7) Direktive (EU) 2016/1148, ki občutno prizadene najmanj dve državi članici;

(e) „poročilo o stanju v EU na področju kibernetske varnosti“ pomeni poročilo, v katerem so zbrani prispevki udeležencev v skupni kibernetski enoti in ki izhaja iz tehničnega poročila o stanju na področju kibernetske varnosti v EU, opredeljenega v členu 7(6) Uredbe (EU) 2019/881;

(f) „skupina EU za hiter odziv na področju kibernetske varnosti“ pomeni skupino, sestavljeno iz priznanih strokovnjakov za kibernetsko varnost, zbranih predvsem iz skupin CSIRT držav članic, ob podpori agencije ENISA, skupine CERT-EU in Europola, ki je pripravljena nuditi pomoč na daljavo udeležencem, ki so jih prizadeli veliki incidenti in krize;

(g) „memorandumi o soglasju“ pomeni sporazume med udeleženci, v katerih so določeni potrebni načini sodelovanja vključno z opredelitvijo sredstev in postopkov, potrebnih za vzpostavitev in mobilizacijo skupin EU za hiter odziv na področju kibernetske varnosti, ter za omogočanje vzajemne pomoči.

([25]) Skladno s pristopom in načeli iz Direktive (EU) 2016/1148 in člena 222 PDEU. Brez poseganja v člen 42(7) Pogodbe o Evropski uniji.
([26]) Vključno s ponudniki programske opreme.
([27]) Vključno z obveščevalnimi podatki o grožnjah.

III. **CILJ SKUPNE KIBERNETSKE ENOTE**

(4) Države članice in ustrezne institucije, organi in agencije EU bi morale zagotoviti **usklajen odziv na ravni EU** na velike kibernetske incidente in krize in okrevanje po njih. Tak odziv bi bilo treba zagotoviti zlasti med operativnimi udeleženci (predvsem agencija ENISA, Europol, skupina CERT-EU, Komisija, Evropska službo za zunanje delovanje (vključno z INTCEN), mreža skupin CSIRT, mreža EU-CyCLONe) in podpornimi udeleženci (predvsem predsedujoči skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov, predsedujoči horizontalne delovne skupine za kibernetska vprašanja Sveta, Evropska obrambna agencija in po en predstavnik zadevnih projektov PESCO) ([28]). Operativni udeleženci bi morali imeti možnost hitre in učinkovite mobilizacije operativnih virov za vzajemno pomoč v okviru skupne kibernetske enote. V ta namen bi bilo treba v skupni kibernetski enoti na zahtevo ene ali več držav članic usklajevati mehanizme vzajemne pomoči.

(5) Za zagotovitev učinkovitega usklajenega odziva bi morali imeti operativni in podporni udeleženci iz točke 4 možnost, da si v okviru svojih pooblastil izmenjujejo dobre prakse, izkoriščajo stalno **skupno situacijsko zavedanje** in zagotavljajo potrebno **pripravljenost**. Ti udeleženci bi morali upoštevati obstoječe postopke in strokovno znanje različnih skupnosti za kibernetsko varnost.

IV. **OPREDELITEV DELOVANJA SKUPNE KIBERNETSKE ENOTE**

(6) Države članice in ustrezne institucije, organi in agencije EU bi morale izhajajoč iz prispevka agencije ENISA v skladu s členom 7(7) Uredbe (EU) 2019/881 zagotoviti **usklajen odziv** na velike incidente in krize ter okrevanje po njih:

(a) z vzpostavitvijo, usposabljanjem, preizkušanjem in usklajeno uporabo **skupin EU za hiter odziv na področju kibernetske varnosti** z upoštevanjem člena 7(4) Uredbe (EU) 2019/881 ter členov 3 in 4 Uredbe (EU) 2016/794;

(b) z usklajenim odzivom **virtualne in fizične platforme** z uporabo strukturiranega sodelovanja agencije ENISA in skupine CERT-EU iz člena 7(4) Uredbe (EU) 2019/881, ki bi morala delovati kot podporna infrastruktura za tehnično in operativno sodelovanje med udeleženci ter zbirati ustrezno osebje in druge vire od udeležencev;

(c) z vzpostavitvijo in vzdrževanjem popisa razpoložljivih **operativnih in tehničnih zmogljivosti v EU** v vseh skupnostih za kibernetsko varnost ([29]) v Uniji, ki so pripravljene za posredovanje v primeru velikih kibernetskih incidentov ali kriz;

(d) s poročanjem Komisiji in visokemu predstavniku o izkušnjah z **dejavnostmi operativnega sodelovanja na področju kibernetske varnosti** znotraj skupnosti za kibernetsko varnost in med njimi.

(7) Države članice in ustrezne institucije, organi in agencije EU bi morale zagotoviti, da bo skupna kibernetska enota zagotavljala stalno **situacijsko zavedanje** in **pripravljenost** na kibernetske krize med skupnostmi za kibernetsko varnost in znotraj njih, ob izpolnjevanju ciljev iz člena 7 Uredbe (EU) 2019/881 in člena 3 Uredbe (EU) 2016/794. Države članice in ustrezne institucije, organi in agencije EU bi morale v ta namen in v skladu z Uredbo (EU) 2019/881 in Uredbo (EU) 2016/794 omogočiti izvajanje naslednjih **podpornih** operacij:

(a) priprava **skupnega poročila o stanju v EU na področju kibernetske varnosti** z zbiranjem in analizo vseh pomembnih informacij in obveščevalnih podatkov o grožnjah;

(b) uporaba ustreznih in varnih **orodij** v skladu s členom 7(1) Uredbe (EU) 2019/881 za hitro izmenjavo informacij med udeleženci in drugimi subjekti;

(c) **izmenjava informacij in strokovnega znanja**, potrebnih za pripravo Unije na obvladovanje velikih kibernetskih incidentov in kriz, ob podpori agencije ENISA v skladu s členom 7(2) Uredbe (EU) 2019/881;

(d) sprejetje in preizkus nacionalnih **načrtov odzivanja na kibernetske incidente in krize** ([30]) v skladu s členom 7(2), (5) in (7) Uredbe (EU) 2019/881;

([28]) „Center za usklajevanje na kibernetskem in informacijskem področju“ (CIDCC) in „Enote za hitro odzivanje na kibernetske grožnje in medsebojna pomoč na področju kibernetske varnosti“ (CRRT).

([29]) Če je ustrezno, vključno s skupnostjo za kibernetsko obrambo.

([30]) Predlaganih v skladu s členom 7(3) Direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148, COM(2020) 823 final, 2020/0359 (COD).

(e) razvoj, upravljanje in preizkušanje **načrta odzivanja EU na kibernetske incidente in krize**, tudi z vajami in usposabljanji med skupnostmi, v skladu s priporočili iz Načrta in izhajajoč iz člena 7(3) predloga Komisije za revizijo Direktive (EU) 2016/1148 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji ([31]);

(f) pomoč udeležencev pri sklepanju sporazumov o izmenjavi informacij ter sporazumov o operativnem sodelovanju s **subjekti iz zasebnega sektorja**, ki zagotavljajo med drugim storitve obveščanja o grožnjah in storitve odziva na incidente, ob podpori agencije ENISA v skladu s členom 7(1) Uredbe (EU) 2019/881;

(g) doseganje strukturiranih sinergij z nacionalnimi, sektorskimi in čezmejnimi **zmogljivostmi spremljanja in odkrivanja**, zlasti s centri za varnostne operacije;

(h) pomoč udeležencev pri **obvladovanju** velikih incidentov in kriz v skladu s podporno vlogo agencije ENISA v skladu s členom 7 Uredbe (EU) 2019/881. Sem spada med drugim prispevanje k skupnemu situacijskemu zavedanju, podpora diplomatskim ukrepom, politični prispevek in prispevek v zvezi s kazenskimi preiskavami, tudi preko Europola ([32]), usklajevanje obveščanja javnosti in omogočanje lažjega okrevanja po incidentih.

(8) Za izvedbo točk 6 in 7 bi morale države članice in ustrezne institucije, organi in agencije EU zagotoviti:

(a) opredelitev organizacijskih vidikov skupne kibernetske enote ter **vlog in odgovornosti** operativnih in podpornih udeležencev znotraj platforme, ki bi omogočila učinkovito delovanje platforme v skladu z vidiki in načeli iz Priloge k temu priporočilu;

(b) sklenitev **memorandumov o soglasju**, v katerih bodo določeni potrebni načini sodelovanja med udeleženci iz točke 4.

(9) Agencija ENISA bi morala v skladu s členom 7 Uredbe (EU) 2019/881 zagotoviti usklajevanje in podporo držav članic in ustreznih institucij, organov in agencij EU v skupni kibernetski enoti, tudi v vlogi sekretariata, z organizacijo sestankov ter s prispevanjem k izvajanju ukrepov tako na ravni držav članic kot na ravni EU. Vzpostaviti bi morala tako varno virtualno platformo kot tudi fizični prostor za prirejanje sestankov ter omogočati lažji potek potrebnih izvedbenih ukrepov.

V. **VZPOSTAVITEV SKUPNE KIBERNETSKE ENOTE**

(10) Države članice in ustrezne institucije, organi in agencije EU bi morale zagotoviti, da skupna kibernetska enota operativno fazo doseže s **30. junijem 2022**. Do takrat bi morali operativni udeleženci dati na razpolago operativne zmogljivosti in strokovnjake, ki bodo lahko podlaga za skupine EU za hiter odziv na področju kibernetske varnosti. Načrti za fizično in virtualno platformo bi morali biti že v zreli fazi.

(11) Države članice in ustrezne institucije, organi in agencije EU bi morale prispevati k delovanju skupne kibernetske enote in zagotoviti, da bo njena operacionalizacija v celoti dokončana do **30. junija 2023**. To bi bilo treba izvesti v štirih zaporednih fazah, katerih cilj bo dokončanje naslednjih dejavnosti:

(a) prva faza: ocena organizacijskih vidikov skupne kibernetske enote in ugotovitev, katere operativne zmogljivosti so na voljo v EU, do **31. decembra 2021**;

(b) druga faza: priprava načrtov odzivanja na kibernetske incidente in krize ter začetek izvajanja dejavnosti pripravljenosti do **30. junija 2022**;

(c) tretja faza: operacionalizacija skupne kibernetske enote do **31. decembra 2022**;

(d) četrta faza: razširitev sodelovanja znotraj skupne kibernetske enote na zasebne subjekte in poročilo o napredku do **30. junija 2023**.

Podrobnejši ukrepi v okviru teh štirih zaporednih faz so navedeni v Prilogi k temu priporočilu.

([31]) COM(2020) 823 final.
([32]) V skladu z Uredbo (EU) 2016/794.

(12) V prvih dveh fazah bi morala agencija ENISA organizirati in podpirati pripravo skupne kibernetske enote. Službe Komisije bi morale organizirati sestanek delovne skupine, v kateri bodo zbrani operativni in podporni udeleženci, da bodo dokončali take priprave. Službe Komisije bi morale imenovati predstavnika kot sopredsedujočega delovne skupine in pozvati k sopredsedovanju predstavnika, ki ga imenuje visoki predstavnik, od katerih vsak prispeva točke dnevnega reda v skladu s svojimi pristojnostmi, ter predstavnika, ki ga izberejo države članice.

(13) Do konca druge faze bi morala delovna skupina dokončati svojo oceno organizacijskih vidikov skupne kibernetske enote ter vlog in odgovornosti operativnih udeležencev v tej platformi. Delovna skupina bi morala rezultate tega ocenjevanja predstaviti Komisiji in visokemu predstavniku. Komisija in visoki predstavnik bi morala tako oceno nato posredovati Svetu. Komisija in visoki predstavnik bi morala na podlagi te ocene pripraviti skupno poročilo in pozvati Svet, da ga podpre v sklepih Sveta.

(14) Skupna kibernetska enota bi morala začeti delovati od tretje faze.

(15) Agencija ENISA in Komisija bi morali zagotoviti uporabo obstoječih virov v okviru programov financiranja s strani EU, zlasti programa za digitalno Evropo, v skladu z veljavnimi pravili za vzpostavitev ustreznih delovnih programov, za zagotovitev dodatnih zmogljivosti za usposabljanje udeležencev v skupni kibernetski enoti, komunikacije in varne infrastrukture za izmenjavo informacij, ki bo omogočala izmenjavo zaupnih podatkov, tudi med skupnostmi.

VI. **PREGLED**

(16) Države članice bi morale v sodelovanju s Komisijo in visokim predstavnikom v skladu z njunimi pristojnostmi do **30. junija 2025** oceniti učinkovitost in uspešnost skupne kibernetske enote, da bi podale ugotovitve glede prihodnosti skupne kibernetske enote. Pri oceni je treba upoštevati izvajanje navedenih štirih faz.

V Bruslju, 23. junija 2021

Za Komisijo
Thierry BRETON
član Komisije

PRILOGA

Faze vzpostavitve skupne kibernetske enote

V tej prilogi so podrobneje opisani osrednji in podporni ukrepi, ki so potrebni za vzpostavitev skupne kibernetske enote in njeno usposobitev za delovanje.

1. *Faza 1 – ocena organizacijskih vidikov skupne kibernetske enote in ugotovitev, katere operativne zmogljivosti so na voljo v EU*

OSREDNJI UKREPI

Operativni udeleženci skupne kibernetske enote, zbrani v delovni skupini, ki jo ustanovi Komisija in jo podpira agencija ENISA, bi morali zbirati informacije o obstoječih operativnih zmogljivostih, vključno s pripravo seznama razpoložljivih priznanih strokovnjakov z navedbo njihovega zadevnega strokovnega znanja, o razpoložljivih orodjih, funkcijah in sredstvih za obvladovanje incidentov, razpoložljivih portfeljih za usposabljanje in vaje ter obstoječih proizvodih za analizo obveščevalnih informacij. Na podlagi teh vhodnih podatkov bi morali udeleženci pripraviti **seznam razpoložljivih operativnih zmogljivosti v EU**, ki jih je mogoče uporabiti v primeru kibernetskih incidentov ali kriz, predvsem preko skupin EU za hiter odziv na področju kibernetske varnosti.

Delovna skupina bi morala začeti ocenjevanje **organizacijskih vidikov** skupne kibernetske enote ter **vlog in odgovornosti operativnih udeležencev znotraj te platforme**.

Da bi si ustvarili pregled nad zmogljivostmi in se sporazumeli o postopkih ter osrednjih in po možnosti podpornih ukrepih v okviru prve faze, bi bilo treba to fazo dokončati do **31. decembra 2021 [6 mesecev od sprejetja]**.

2. *Faza 2 – priprava načrtov odzivanja na kibernetske incidente in krize ter začetek izvajanja dejavnosti pripravljenosti*

OSREDNJI UKREPI

Operativni udeleženci v delovni skupini bi morali v posvetovanju s podpornimi udeleženci pripraviti **načrt odzivanja EU na kibernetske incidente in krize** na podlagi nacionalnih načrtov odzivanja na kibernetske incidente in krize. Načrt odzivanja EU na kibernetske incidente in krize bi moral zajemati cilje pripravljenosti EU, ugotovljene postopke in kanale za varno izmenjavo informacij, vključno z načini za ravnanje z informacijami, ter merila za aktivacijo mehanizma vzajemne pomoči na podlagi dogovorjene taksonomije za razvrščanje incidentov in seznama razpoložljivih zmogljivosti v EU.

Do konca druge faze bi morala delovna skupina končati ocenjevanje organizacijskih vidikov skupne kibernetske enote ter vlog in odgovornosti operativnih udeležencev znotraj te platforme. Delovna skupina bi morala rezultate te ocene predstaviti Komisiji in visokemu predstavniku. Komisija in visoki predstavnik bi morala tako oceno posredovati Svetu. Komisija in visoki predstavnik bi morala na podlagi te ocene v skladu s svojimi pristojnostmi skupaj pripraviti skupno poročilo in pozvati Svet, da ga podpre v svojih sklepih.

PODPORNI UKREPI

Načrt odzivanja EU na kibernetske incidente in krize bi moral izhajati iz glavnih elementov nacionalnih načrtov odzivanja na kibernetske incidente in krize. V skladu s predlogom Komisije za direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 ([1]) bi morale države članice sprejeti nacionalne načrte odzivanja na kibernetske incidente in krize. V nacionalnih načrtih, za katere bi se morda opravil medsebojni strokovni pregled, bi morali biti opredeljeni cilji in načini obvladovanja velikih kibernetskih incidentov in kriz. V nacionalnih načrtih bi morala biti obravnavana predvsem naslednja vprašanja:

(a) cilji nacionalnih ukrepov in dejavnosti pripravljenosti;

(b) vloge in odgovornosti pristojnih nacionalnih organov na nacionalni ravni;

(c) nacionalni postopki obvladovanja krize in kanali za izmenjavo informacij;

(d) določitev ukrepov pripravljenosti, tudi vaj in dejavnosti usposabljanja;

(e) določitev ustreznih sodelujočih javnih in zasebnih deležnikov in infrastrukture;

(f) nacionalni postopki in dogovori med ustreznimi nacionalnimi organi, tudi tistimi, ki so odgovorni za vse kibernetske skupnosti, za zagotovitev učinkovitega sodelovanja države članice pri usklajenem obvladovanju velikih kibernetskih incidentov in kriz na ravni EU ter njegove podpore.

Operativni udeleženci bi morali na podlagi vhodnih podatkov držav članic in institucij, organov in agencij EU v okviru skupne kibernetske enote izvesti naslednje podporne ukrepe:

(a) pripraviti prvo skupno poročilo o stanju v EU na podlagi nacionalnih načrtov odzivanja na kibernetske incidente in krize;

([1]) COM(2020) 823 final 2020/0359 (COD), Bruselj, 16. decembra 2020.

(b) vzpostaviti komunikacijske zmogljivosti in orodja za varno izmenjavo informacij;

(c) omogočiti lažje sprejemanje protokolov za vzajemno pomoč med udeleženci;

(d) organizirati vaje in usposabljanja, pri katerih bo sodelovalo več skupnosti, za strokovnjake s seznama razpoložljivih operativnih zmogljivosti EU;

(e) pripraviti večletni načrt za usklajevanje vaj.

Operativni udeleženci se po potrebi posvetujejo s podpornimi udeleženci. Agencija ENISA bi morala ob podpori Komisije, Europola in skupine CERT-EU omogočiti izmenjavo informacij z vzpostavitvijo komunikacijskih zmogljivosti in orodij za varno izmenjavo informacij.

Da bi zagotovili, da bodo potrebni načrti pripravljeni in da se bodo lahko začele izvajati skupne dejavnosti, bi bilo treba osrednje, po možnosti pa tudi podporne ukrepe iz druge faze dokončati do **30. junija 2022 [6 mesecev od konca faze 1]**.

3. *Faza 3 – operacionalizacija skupne kibernetske enote*

OSREDNJI UKREPI

Potem ko bo Svet podprl sklepe Komisije o poročilu iz druge faze, bi morali operativni udeleženci uskladiti začetek uporabe **skupin EU za hiter odziv na področju kibernetske varnosti** v okviru skupne kibernetske enote in vzpostaviti **fizično platformo**, ki bo skupinam omogočala izvajanje tehničnih in operativnih dejavnosti. Udeleženci bi morali na podlagi pripravljalnega dela, opravljenega v drugi fazi, dokončati načrt odzivanja EU na kibernetske incidente in krize. Operativni udeleženci bi morali zagotoviti, da bodo strokovnjaki in zmogljivosti s seznama razpoložljivih operativnih zmogljivosti EU na voljo in da bodo lahko prispevali k delovanju skupin EU za hiter odziv na področju kibernetske varnosti.

Da bi bilo mogoče izvesti načrt odzivanja EU na kibernetske incidente in krize, bi morali udeleženci opredeliti letni delovni program.

PODPORNI UKREPI

Skupnost za kibernetsko diplomacijo lahko uporabi skupno kibernetsko enoto za usklajevanje obveščanja javnosti. Platforma lahko udeležencem omogoča prispevanje k političnemu pripisovanju in pripisovanju v kazenskopravnem okviru, ki se uporablja na ravni policije in pravosodja. Poleg tega lahko omogoča lažje okrevanje in strukturirane sinergije z nacionalnimi in čezmejnimi zmogljivostmi za spremljanje in odkrivanje.

Da bi zagotovili, da bo skupna kibernetska enota pripravljena za delovanje, bi bilo treba osrednje, po možnosti pa tudi podporne ukrepe iz tretje faze končati do **31. decembra 2022 [6 mesecev od konca faze 2]**.

4. *Faza 4 – razširitev sodelovanja znotraj skupne kibernetske enote na zasebne subjekte in poročanje o napredku*

OSREDNJI UKREPI

Udeleženci skupne kibernetske enote bi morali pripraviti **poročilo o dejavnosti o napredku pri izvajanju štirih faz iz tega priporočila z opisom dosežkov in izzivov**. Poročilo bi moralo vsebovati tudi statistične informacije o dejavnostih operativnega sodelovanja, izvedenih v teh štirih fazah. Poročilo bi bilo treba predložiti Komisiji in visokemu predstavniku.

PODPORNI UKREPI

Da bi razširili zmogljivosti in podatke, ki so na razpolago skupinam EU za hiter odziv na področju kibernetske varnosti, bi morali udeleženci zagotoviti, da bo skupna kibernetska enota pomagala pri sklenitvi **sporazumov o izmenjavi informacij in operativnem sodelovanju med udeleženci in subjekti iz zasebnega sektorja**, ki med drugim opravljajo storitve zagotavljanja obveščevalnih podatkov in odzivanja na incidente. Zagotoviti bi morali tudi, da bi skupna kibernetska enota med drugimi dejavnostmi redno podpirala dejavnosti dialoga in izmenjave informacij o grožnjah in šibkih točkah z uporabniki rešitev na področju kibernetske varnosti, predvsem tistimi, ki spadajo na področje uporabe direktive o varnosti omrežij in informacijskih sistemov ali ki so zbrani v **centrih za izmenjavo in analizo informacij (ISAC) na ravni EU**.

Države članice bi morale subjekte, ki delujejo na njihovem ozemlju, zlasti tiste s področja direktive o varnosti omrežij in informacijskih sistemov, podpirati pri omogočanju dostopa do dialogov med javnim in zasebnim sektorjem in prispevanju k tem dialogom s centri ISAC na ravni EU.

Da bi zagotovili ustrezno sodelovanje zasebnega sektorja, bi bilo treba osrednje, po možnosti pa tudi podporne ukrepe iz četrte faze končati do **30. junija 2023** [6 mesecev od konca faze 3].

KAKO HITRO MOBILIZIRATI OPERATIVNE ZMOGLJIVOSTI EU

KDO ZAGOTAVLJA ZMOGLJIVOSTI: operativni udeleženci

KDO UPRAVLJA ZMOGLJIVOSTI: udeleženci v skupni kibernetski enoti v skladu z dogovorjenimi vlogami in odgovornostmi

Faza	Cilj	Naloga	Osrednji ukrep	Podporni ukrep
Faza 1 – opredelitev do **31. decembra 2021 [6 mesecev od sprejetja]**	PRIPRAVLJENOST	**Ugotovitev zmogljivosti**	**Operativni udeleženci pripravijo seznam razpoložljivih operativnih zmogljivosti v EU.**	
Faza 2 – priprava do **30. junija 2022 [6 mesecev od konca faze 1]**	PRIPRAVLJENOST	**Opredelitev ustreznih postopkov in dogovorov za aktivacijo zmogljivosti v primeru potrebe**	**Operativni udeleženci na podlagi sprejetih nacionalnih načrtov pripravijo načrt odzivanja EU na kibernetske incidente in krize (v Načrtu: okvir EU za odzivanje na krize na področju kibernetske varnosti).**	**Operativni udeleženci na podlagi tehničnega poročila o stanju na področju kibernetske varnosti v EU pripravijo skupna poročila o stanju v EU.**
	PRIPRAVLJENOST	**Zmogljivosti za vaje**		**Udeleženci organizirajo skupno vajo in usposabljanje (pri katerih sodeluje več skupnosti).** **Udeleženci pripravljajo večletni načrt za usklajevanje vaj.**
	SITUACIJSKO ZAVEDANJE	**Vzpostavitev orodij za izmenjavo informacij in zahtevkov za podporo**		**Udeleženci vzpostavijo varno in hitro izmenjavo informacij.**
SKUPNA KIBERNETSKA ENOTA JE PRIPRAVLJENA ZA DELOVANJE Na podlagi priprav, ki jih udeleženci izvedejo v delovni skupini, ki jo vzpostavi Komisija				
Faza 3 – uporaba do **31. decembra 2022 [6 mesecev od konca faze 2]**	PRIPRAVLJENOST	**Sprejetje ustreznih postopkov, dogovorov in memorandumov o soglasju za aktivacijo zmogljivosti v primeru potrebe**	**Operativni udeleženci dokončajo načrt odzivanja EU na kibernetske incidente in krize ter opredelijo njegovo izvajanje v letnih delovnih programih.**	**Udeleženci podpirajo vzpostavitev nacionalnih in čezmejnih zmogljivosti za spremljanje in odkrivanje, vključno z vzpostavitvijo centrov za varnostne operacije (SOC).**
	USKLAJEN ODZIV	**Uporaba zmogljivosti v primeru potrebe**	**Operativni udeleženci usklajujejo operativne skupine EU za hiter odziv na področju kibernetske varnosti preko virtualne in fizične platforme skupne kibernetske enote v Bruslju.**	**Udeleženci usklajujejo obveščanje javnosti ter prispevajo k političnemu pripisovanju in pripisovanju v kazenskopravnem okviru.**

Faza 4 – širjenje in poročanje do **30. junija 2023 [6 mesecev od konca faze 3]**	SITUACIJSKO ZAVEDANJE USKLAJEN ODZIV	**Zagotovitev možnosti povečanja obsega z vključitvijo zasebnega sektorja za pomoč pri nastajajočih potrebah**	**Udeleženci predložijo poročilo o dejavnosti o doseženem napredku, v katerem s pomočjo statističnih podatkov opišejo dosežke in izzive.**	**Udeleženci s ponudniki storitev kibernetske varnosti sklenejo sporazume o izmenjavi informacij ter sporazume o operativnem sodelovanju.** **Udeleženci sklenejo sporazume o izmenjavi informacij z uporabniki storitev kibernetske varnosti, predvsem subjekti s področja uporabe direktive o varnosti omrežij in informacijskih sistemov in s centri EU za izmenjavo in analizo informacij (ISAC).**