EVROPSKA
KOMISIJA

Bruselj, 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

PRILOGA

k

SPOROČILU KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Kako kar najbolje izkoristiti direktivo o varnosti omrežij in informacij – za učinkovito izvajanje Direktive (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

SL

KAZALO

PRILOGA

1. Uvod

Cilj te priloge je prispevati k učinkoviti uporabi, izvajanju in izvrševanju Direktive (EU) 2016/1148 o ukrepih za visoko raven varnosti omrežij in informacijskih sistemov v Uniji[1] (v nadaljnjem besedilu: direktiva o varnosti omrežij in informacij ali Direktiva) ter državam članicam pomagati, da zagotovijo učinkovito uporabo prava EU. Natančneje ima ta priloga tri cilje: (a) nacionalnim organom zagotoviti večjo jasnost glede obveznosti, ki jim jih nalaga Direktiva, (b) zagotoviti učinkovito izvrševanje obveznosti, ki izhajajo iz Direktive in se navezujejo na subjekte, za katere veljajo obveznosti glede varnostnih zahtev in priglasitve incidentov, ter (c) v splošnem prispevati k ustvarjanju pravne varnosti za vse zadevne akterje.

V ta namen Priloga zagotavlja smernice v zvezi z naslednjimi vidiki, ki so ključni za dosego cilja direktive o varnosti omrežij in informacij, tj. zagotoviti visoko skupno raven varnosti omrežij in informacijskih sistemov v EU ter tako podpreti delovanje naše družbe in gospodarstva:

- obveznostjo držav članic, da sprejmejo nacionalno strategijo za varnost omrežij in informacijskih sistemov (oddelek 2);
- vzpostavitvijo nacionalnih pristojnih organov, enotnih kontaktnih točk in skupin za odzivanje na incidente na področju računalniške varnosti (oddelek 3);
- zahtevami glede varnosti in priglasitve incidentov za izvajalce bistvenih storitev in ponudnike digitalnih storitev (oddelek 4); ter
- razmerjem med direktivo o varnosti omrežij in informacij ter drugo zakonodajo (oddelek 5).

Za pripravo teh smernic je Komisija uporabila prispevke in analize, pridobljene med pripravo Direktive ter prispevke Evropske agencije za varnost omrežij in informacij (v nadaljnjem besedilu: ENISA) in skupine za sodelovanje. Komisija je uporabila tudi izkušnje, ki so jih pridobile nekatere države članice, in ustrezno upoštevala vodilna načela za razlago prava EU: besedilo, kontekst in cilje direktive o varnosti omrežij in informacij. Pri pripravi smernic se ni bilo mogoče nasloniti na sodno prakso, ker Direktiva še ni bila prenesena in zato do zdaj tudi še ni bila izdana nobena sodba Sodišča Evropske unije (v nadaljnjem besedilu: Sodišče EU) oziroma nacionalnih sodišč.

Z združitvijo teh informacij v enem dokumentu bodo države članice dobile dober pregled Direktive in bodo te informacije lahko upoštevale pri pripravi svoje nacionalne zakonodaje. Komisija obenem poudarja, da ta priloga ni zavezujoča in da njen namen ni ustvarjati novih pravil. Končno pristojnost za razlago prava EU ima Sodišče EU.

[1] 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. Direktiva je začela veljati 8. avgusta 2016.

2. Nacionalna strategija za varnost omrežij in informacijskih sistemov

V skladu s členom 7 direktive o varnosti omrežij in informacij morajo države članice sprejeti nacionalne strategije za varnost omrežij in informacijskih sistemov, ki se lahko štejejo za enakovredne terminu „nacionalna strategija za kibernetsko varnost“. V nacionalni strategiji so opredeljeni strateški cilji ter ustrezni ukrepi politike in regulativni ukrepi na področju kibernetske varnosti. Koncept nacionalne strategije za kibernetsko varnost se splošno uporablja tako v Evropi kot tudi na širši mednarodni ravni, zlasti v okviru sodelovanja agencije ENISA z državami članicami pri pripravi nacionalnih strategij, katerega plod je posodobljeni vodnik po dobrih praksah v zvezi z nacionalnimi strategijami za kibernetsko varnost[2].

V tem oddelku Komisija navaja, kako direktiva o varnosti omrežij in informacij izboljšuje pripravljenost držav članic s tem, da od njih zahteva, da imajo vzpostavljene trdne nacionalne strategije za varnost omrežij in informacijskih sistemov (člen 7). V njem sta obravnavana naslednja vidika: (a) področje uporabe strategije ter (b) vsebina in postopek za sprejetje.

Kot je podrobneje opisano v nadaljevanju, je pravilen prenos člena 7 direktive o varnosti omrežij in informacij bistven za dosego ciljev Direktive, prav tako pa tudi zahteva dodelitev ustreznih finančnih in človeških virov za ta namen.

2.1 Področje uporabe nacionalne strategije

V skladu z besedilom člena 7 obveznost za sprejetje nacionalne strategije za kibernetsko varnost velja samo za sektorje iz Priloge II (tj. energija, promet, bančništvo, finančni trg, zdravstvo, oskrba s pitno vodo in njena distribucija ter digitalna infrastruktura) in storitve iz Priloge III (spletna tržnica, spletni iskalnik in storitev računalništva v oblaku).

V členu 3 Direktive je posebej opredeljeno načelo minimalne harmonizacije, v skladu s katerim lahko države članice sprejmejo ali ohranijo določbe za doseganje višje stopnje varnosti omrežij ali informacijskih sistemov. Uporaba tega načela v zvezi z obveznostjo sprejetja nacionalne strategije za kibernetsko varnost državam članicam omogoča, da vključijo več sektorjev in storitev, ki sicer niso zajeti v prilogah II in III k Direktivi.

Po mnenju Komisije in v skladu s ciljem direktive o varnosti omrežij in informacij, tj. doseganje in vzdrževanje visoke ravni varnosti omrežij in informacijskih sistemov v Uniji[3], bi bilo priporočljivo nacionalno strategijo razviti tako, da zajema vse ustrezne družbene in gospodarske razsežnosti ter ne samo sektorje in digitalne storitve, ki so zajeti v prilogah II in III k direktivi o varnosti omrežij in informacij. To je v skladu z dobrimi praksami na mednarodni ravni (gl. smernice Mednarodne telekomunikacijske zveze in analizo OECD, ki so navedeni v nadaljevanju) ter direktivo o varnosti omrežij in informacij.

[2] ENISA, *National Cyber-Security Strategy Good Practice* (Dobre prakse v zvezi z nacionalnimi strategijami za kibernetsko varnost) (2016). Na voljo na https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[3] Glej člen 1(1).

Kot je podrobneje pojasnjeno v nadaljevanju, to zlasti velja za javne uprave, pristojne za sektorje in storitve, ki niso navedeni v prilogah II in III k Direktivi. Javne uprave lahko obdelujejo občutljive informacije, ki jih je upravičeno zajeti v nacionalno strategijo za kibernetsko varnost in načrte upravljanja, da bi se zagotovila zadostna zaščita teh informacij in preprečilo njihovo uhajanje.

2.2 Vsebina nacionalnih strategij in postopek za njihovo sprejetje

V skladu s členom 7 direktive o varnosti omrežij in informacij mora nacionalna strategija o kibernetski varnosti vključevati vsaj:

i) cilje in prednostne naloge nacionalne strategije za varnost omrežij in informacijskih sistemov;
ii) okvir upravljanja za dosego ciljev in prednostnih nalog nacionalne strategije;
iii) opredelitev ukrepov v zvezi s pripravljenostjo, odzivanjem in ponovno vzpostavitvijo, vključno s sodelovanjem med javnim in zasebnim sektorjem;
iv) opredelitev zadevnih programov izobraževanja, ozaveščanja in usposabljanja;
v) opredelitev načrtov raziskav in razvoja;
vi) načrt ocene tveganja za prepoznavanje tveganj; ter
vii) seznam akterjev, vključenih v izvajanje strategije.

Niti v členu 7 niti v ustrezni uvodni izjavi 29 niso navedene zahteve za sprejetje nacionalne strategije za kibernetsko varnost ali podane podrobnejše informacije glede njene vsebine. Kar zadeva postopek in dodatne elemente v zvezi z vsebino nacionalne strategije za kibernetsko varnost, Komisija meni, da je spodnji pristop eden od ustreznih načinov za sprejetje take strategije. Ta pristop temelji na analizi izkušenj držav članic in tretjih držav pri razvoju svojih strategij. Nadaljnji vir informacij je orodje za usposabljanje, ki ga je razvila ENISA in je na voljo v obliki videoposnetkov in prenosljivih datotek, objavljenih na njenem spletišču[4].

2.3 Postopek in vprašanja, ki jih je treba obravnavati

Postopek za pripravo in sprejetje nacionalne strategije je kompleksen in večplasten, za njeno učinkovito in uspešno delovanje pa so potrebna vztrajna prizadevanja strokovnjakov za kibernetsko varnost, civilne družbe in nacionalnih političnih struktur. Predpogoj za to sta višja upravna podpora (vsaj na ravni državnega sekretarja ali enakovredni ravni v vodilnem ministrstvu) ter politična podpora. Za uspešno sprejetje nacionalne strategije za kibernetsko varnost se lahko upošteva naslednji postopek v petih korakih (gl. Sliko 1):

Prvi korak – **Določitev vodilnih načel in strateških ciljev strategije**

Najprej bi pristojni nacionalni organi morali določiti nekaj ključnih elementov za vključitev v nacionalno strategijo za kibernetsko varnost, in sicer: želene rezultate (v skladu z dikcijo člena 7(1)(a) Direktive „cilje in prednostne naloge“), kako bodo rezultati dopolnjevali socialne in gospodarske politike ter združljivost rezultatov s pravicami in dolžnostmi, ki jih države uživajo oziroma so jim naložene kot državam članicam Evropske unije. Cilji bi morali

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool.

biti specifični, merljivi, dosegljivi, realistični in časovno določeni. To se lahko ponazori z naslednjim primerom: „Zagotovili bomo, da bo ta [časovno opredeljena] strategija utemeljena na strogem in celovitem sklopu kazalnikov, na podlagi katerih bomo merili napredek pri doseganju zastavljenih ciljev.“[5]

Navedeno obsega tudi politično presojo, ali je možno zagotoviti zadosten proračun za zagotavljanje virov za izvajanje strategije. Vključuje tudi opis predvidenega področja uporabe strategije in različnih kategorij zainteresiranih strani iz javnega in zasebnega sektorja, ki bi morale biti vključene v pripravo osnutka različnih ciljev in ukrepov.

Prvi korak se lahko izvede v obliki namenskih delavnic z visokimi uradniki ministrstev in politiki, ki bi jih usmerjali strokovnjaki za kibernetsko varnost s ustrezno razvitimi spretnostmi poslovne komunikacije, ki bi znali ponazoriti posledice odsotnosti ali nizke ravni kibernetske varnosti za sodobno digitalno gospodarstvo in družbo.

Drugi korak – **Oblikovanje vsebine strategije**

Strategija bi morala vključevati splošne ukrepe, časovno določene ukrepe in ključne kazalnike uspešnosti za nadaljnje ocenjevanje in izboljševanje po določenem obdobju izvajanja. Ti ukrepi bi morali podpirati cilje, prednostne naloge in rezultate, ki so določeni kot vodilna načela. Vključitev podpornih ukrepov se zahteva v skladu s členom 7(1)(c) direktive o varnosti omrežij in informacij.

Priporočljivo je, da se pod predsedstvom vodilnega ministrstva ustanovi usmerjevalna skupina, ki bo vodila proces priprave strategije in zbirala prispevke. To se lahko doseže s pomočjo več redakcijskih skupin, v katerih sodelujejo zadevni uradniki in strokovnjaki s ključnih splošnih področij, kot so ocenjevanje tveganj, načrtovanje ravnanja v nepredvidljivih razmerah, obvladovanje incidentov, razvoj znanj in spretnosti, ozaveščanje, raziskave in industrijski razvoj itd. Ločeno od tega bi bil vsak sektor (energetski, prometni, itd.) tudi pozvan, naj oceni učinke svoje vključenosti, vključno z zagotavljanjem virov, ter imenovane izvajalce bistvenih storitev in ključne ponudnike digitalnih storitev vključi v postopke določitve prednostnih nalog in podajanja predlogov v procesu priprave. Vključenost zainteresiranih strani iz sektorja je bistvenega pomena tudi z vidika zagotavljanja harmoniziranega izvajanja Direktive v različnih sektorjih ob hkratnem upoštevanju posebnosti vsakega sektorja.

Tretji korak – **Vzpostavitev okvira upravljanja**

Uspešen in učinkovit okvir upravljanja bi moral temeljiti na vključenosti ključnih zainteresiranih strani, prednostnih nalogah, opredeljenih v procesu priprave, ter omejitvah in okviru delovanja nacionalnih upravnih in političnih struktur. Zaželeno je neposredno poročanje na politični ravni, pri čemer ima okvir upravljanja na voljo zmogljivosti za odločanje in dodeljevanje virov, ter pridobivanje prispevkov strokovnjakov za kibernetsko varnost in zainteresiranih strani iz industrije. Člen 7(1)(b) direktive o varnosti omrežij in

[5] Izvleček iz Nacionalne strategije za kibernetsko varnost Združenega kraljestva 2016–2021, str. 67.

informacij se navezuje na okvir upravljanja in izrecno zahteva obravnavo „vlog in odgovornosti vladnih organov in drugih zadevnih akterjev“.

Četrti korak – **Priprava in pregled osnutka strategije**

V tej fazi bi bilo treba pripraviti in pregledati osnutek strategije na podlagi analize prednosti, slabosti, priložnosti in tveganj (SWOT), v skladu s katero bi bilo mogoče ugotoviti, ali bi bilo treba pregledati vsebino. Po notranjem pregledu bi bilo treba opraviti posvetovanje z zainteresiranimi stranmi. Prav tako bi bilo nujno izvesti javno posvetovanje, da se javnosti predstavi, kako pomembna je predlagana strategija, pridobiti prispevke od vseh možnih virov in zagotoviti podporo pri pridobivanju virov, potrebnih za kasnejše izvajanje strategije.

Peti korak – **Uradno sprejetje**

Zadnji korak vključuje uradno sprejetje na politični ravni z zadostnim proračunom, ki odraža resnost, s katero zadevna država članica pristopa k zagotavljanju kibernetske varnosti. Komisija spodbuja države članice, da za dosego ciljev direktive o varnosti omrežij in informacij v okviru priglasitve svojih dokumentov z nacionalno strategijo Komisiji v skladu s členom 7(3) Direktive sporočijo tudi informacije o proračunu. Zaveze glede proračuna in potrebnih človeških virov so neobhodne za učinkovito izvajanje strategije in Direktive. Ker je kibernetska varnost relativno novo in hitro rastoče področje javne politike, so v večini primerov potrebne nove naložbe, tudi kadar splošno stanje javnih financ zapoveduje omejevanje odhodkov in prihranke.

Nasveti v zvezi s procesom priprave in vsebino nacionalnih strategij so na voljo v različnih javnih in akademskih virih, na primer v dokumentih agencije ENISA[6], Mednarodne telekomunikacijske zveze[7], OECD[8], svetovnega foruma o kibernetskem strokovnem znanju in Univerze v Oxfordu[9].

---

[6] ENISA, *National Cyber-Security Strategy Good Practice* (Dobre prakse v zvezi z nacionalnimi strategijami za kibernetsko varnost) (2016). Na voljo na https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] Mednarodna telekomunikacijska zveza, *National Cybersecurity Strategy Guide* (Priročnik o nacionalnih strategijah za kibernetsko varnost) (2011). Na voljo na http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
Mednarodna telekomunikacijska zveza bo v letu 2017 izdala tudi dokument z naslovom *National Cyber Security Strategy Toolkit* (Zbirka orodij za nacionalne strategije za kibernetsko varnost) (gl. predstavitev na naslovu http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (Oblikovanje politik za kibernetsko varnost na prelomnici: analiza nove generacije nacionalnih strategij za kibernetsko varnost) (2012). Na voljo na: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[9] Svetovni center za zmogljivosti na področju kibernetske varnosti in Univerza v Oxfordu, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (Zrelostni model za nacionalne zmogljivosti na področju kibernetske varnosti (CMM) – revidirana izdaja) (2016). Na voljo na: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

2.4 Konkretni koraki, ki jih morajo države članice narediti pred iztekom roka za prenos

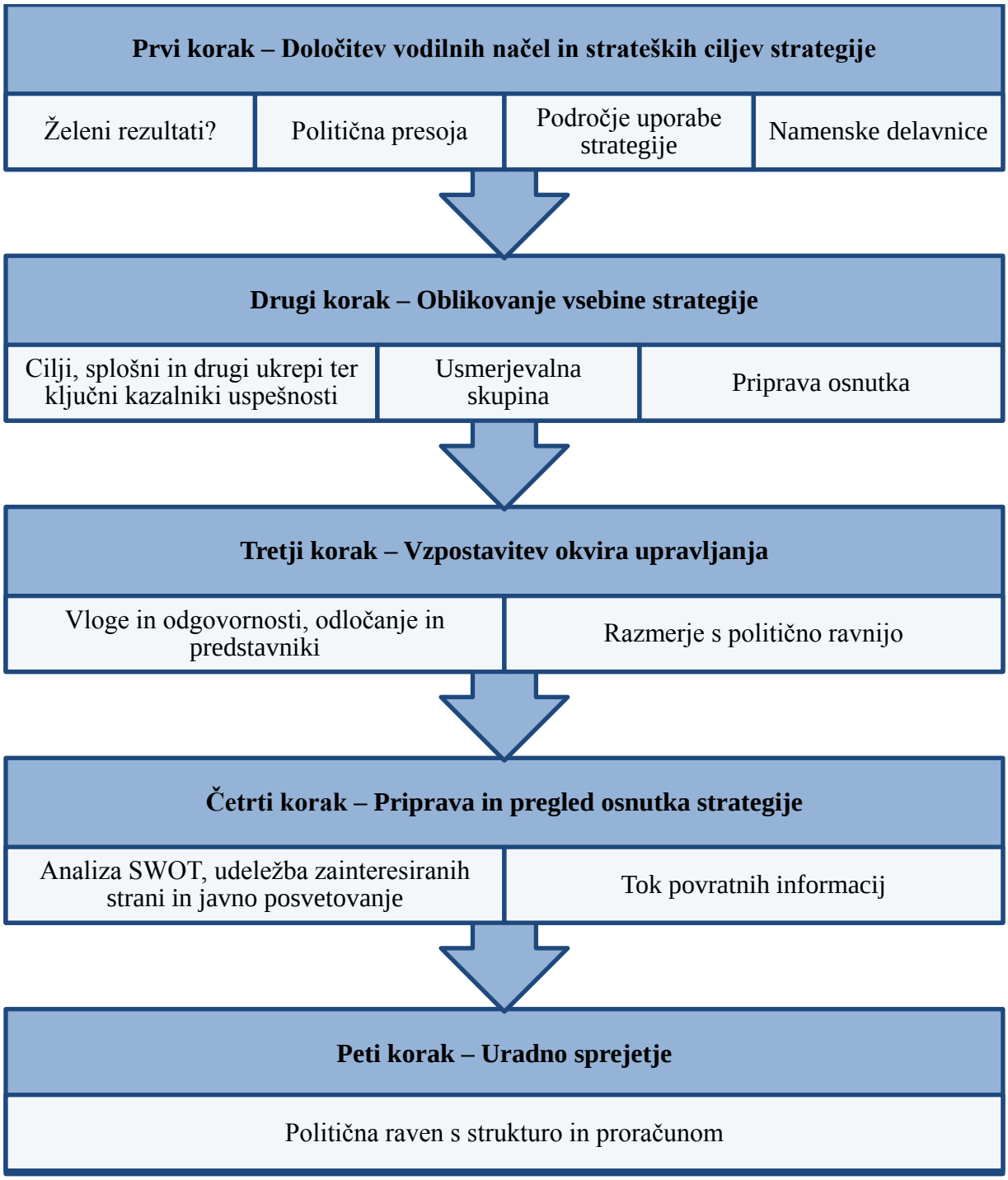
Pred sprejetjem Direktive so skoraj vse države članice[10] že objavile dokumente, ki so se šteli za nacionalno strategijo za kibernetsko varnost. Strategije, ki so trenutno v veljavi v posamezni državi članici[11], so navedene v oddelku 6 te priloge. Običajno vključujejo strateška načela, smernice in cilje ter v nekaterih primerih tudi posebne ukrepe za zmanjševanje tveganj, povezanih s kibernetsko varnostjo.

Glede na to, da so bile nekatere od teh strategij sprejete še pred sprejetjem direktive o varnosti omrežij in informacij, morda ne vsebujejo vseh elementov iz člena 7. Da se zagotovi pravilen prenos, bodo morale države članice opraviti analizo vrzeli, tako da preučijo, ali njihove nacionalne strategije za kibernetsko varnost vsebujejo vseh sedem zahtev iz člena 7 za celotni nabor sektorjev, navedenih v Prilogi II k Direktivi, in storitev, navedenih v Prilogi III. Ugotovljene vrzeli se nato lahko odpravijo z revizijo obstoječe nacionalne strategije za kibernetsko varnost ali s celovito revizijo načel nacionalne strategije za varnost omrežij in informacijskih sistemov. Zgoraj predlagane smernice v zvezi s postopkom sprejetja nacionalne strategije za kibernetsko varnost so primerne tudi za pregled in posodobitev že sprejetih nacionalnih strategij.

[10] Razen Grčije, kjer je nacionalna strategija za kibernetsko varnost v pripravi od leta 2014 (gl. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Te informacije temeljijo na pregledu nacionalnih strategij za kibernetsko varnost, ki ga je pripravila ENISA in je objavljen na https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Slika 1: Postopek sprejetja nacionalne strategije za kibernetsko varnost v petih korakih



3. Direktiva o varnosti omrežij in informacij: pristojni nacionalni organi, enotne kontaktne točke in skupine za odzivanje na incidente na področju računalniške varnosti (CSIRT)

V skladu s členom 8(1) morajo države članice določiti enega ali več pristojnih nacionalnih organov, ki pokrivajo vsaj sektorje iz Priloge II in storitve iz Priloge III k Direktivi in katerih naloga je spremljati uporabo Direktive. Države članice lahko to vlogo dodelijo obstoječemu organu ali organom.

Ta oddelek se osredotoča na to, kako direktiva o varnosti omrežij in informacij izboljšuje pripravljenost držav članic s tem, da od njih zahteva, da imajo vzpostavljene učinkovite pristojne nacionalne organe in skupine za odzivanje na incidente na področju računalniške varnosti (CSIRT). Natančneje ta oddelek zajema obveznost določitve pristojnih nacionalnih organov, vključno z vlogo enotne kontaktne točke. V njem so obravnavane tri teme: (a) možne nacionalne strukture upravljanja (centralizirani ali decentralizirani model itd.) in druge zahteve; (b) vloga enotne kontaktne točke in (c) skupine CSIRT.

3.1 Vrste organov

V skladu s členom 8 direktive o varnosti omrežij in informacij morajo države članice določiti pristojne nacionalne organe za varnost omrežij in informacijskih sistemov, pri tem pa je izrecno dovoljena možnost, da imenujejo „enega ali več pristojnih nacionalnih organov“. Ta politična odločitev je obrazložena v uvodni izjavi 30 Direktive: „Glede na razlike v nacionalnih strukturah upravljanja in zaradi varovanja že obstoječih sektorskih dogovorov ali nadzornih in regulativnih organov Unije ter da bi se izognili podvajanju, bi države članice morale imeti možnost imenovati več kot en pristojni nacionalni organ, odgovoren za izvajanje nalog, povezanih z varnostjo omrežij in informacijskih sistemov izvajalcev bistvenih storitev in ponudnikov digitalnih storitev po tej direktivi.“

V skladu s tem se lahko države članice same odločijo, ali bodo določile en osrednji organ, ki bo pokrival vse sektorje in storitve, zajete v Direktivi, ali pa več organov, na primer glede na vrsto sektorja.

Države članice se pri sprejemanju odločitve o tem lahko naslonijo na izkušnje iz nacionalnih pristopov v okviru obstoječe zakonodaje o zaščiti kritične informacijske infrastrukture. Kot je opisano v preglednici 1, so na področju zaščite kritične informacijske infrastrukture države članice lahko dodeljevale nacionalne pristojnosti s centraliziranim ali decentraliziranim pristopom. Nacionalni primeri v nadaljevanju so navedeni le za ponazoritev in z namenom, da državam članicam predstavijo obstoječe organizacijske okvire. Komisija s tem ne podaja mnenja, da bi bilo treba model, ki ga nekatere države članice uporabljajo za zaščito kritične informacijske infrastrukture, uporabiti tudi za namen prenosa direktive o varnosti omrežij in informacij.

Države članice se lahko odločijo tudi za uporabo različnih kombiniranih ureditev, ki vključujejo tako elemente centraliziranega kot tudi decentraliziranega pristopa. Odločitve o tem se lahko sprejmejo glede na predhodne nacionalne ureditve upravljanja za različne sektorje in storitve, zajete v Direktivi, ali pa jih zadevni organi in zadevne zainteresirane strani, ki se štejejo za izvajalce bistvenih storitev in ponudnike digitalnih storitev, sprejmejo neodvisno od njih. Pomembni dejavniki, ki bi lahko vplivali na odločitve držav članic, so tudi obstoj strokovnega znanja s področja kibernetske varnosti, pomisleki glede zagotavljanja virov ter razmerja med interesi zainteresiranih strani in nacionalnimi interesi (npr. gospodarski razvoj, javna varnost ipd.).

3.2 Obveščanje javnosti in drugi pomembni vidiki

V skladu s členom 8(7) morajo države članice Komisijo obvestiti o določitvi pristojnih nacionalnih organov in njihovih nalogah. To morajo storiti do izteka roka za prenos.

Države članice morajo v skladu s členoma 15 in 17 direktive o varnosti omrežij in informacij zagotoviti, da imajo pristojni organi potrebna pooblastila in sredstva za izvajanje nalog, določenih v ustreznih členih.

Poleg tega je treba določitev subjektov za pristojne nacionalne organe javno objaviti. Direktiva ne določa, na kakšen način bi moralo biti takšno obveščanje javnosti izvedeno. Komisija tudi na podlagi izkušenj iz drugih sektorjev (telekomunikacije, bančništvo, farmacija) meni, da bi bilo cilj te zahteve, tj. visoko raven ozaveščenosti akterjev, vključenih v varnost omrežij in informacijskih sistemov, in splošne javnosti, mogoče doseči na primer s pomočjo dobro oglaševanega portala.

V skladu s členom 8(5) direktive o varnosti omrežij in informacij morajo takšni organi imeti „ustrezne vire“ za izvajanje nalog, dodeljenih na podlagi Direktive.

Preglednica 1: Nacionalni pristopi k zaščiti kritične informacijske infrastrukture

Leta 2016 je ENISA objavila študijo[12] o različnih pristopih držav članic k zaščiti svoje kritične informacijske infrastrukture. V okviru za upravljanje varovanja kritične informacijske infrastrukture v državah članicah sta opisana dva profila, ki ju je mogoče uporabiti v kontekstu prenosa direktive o varnosti omrežij in informacij.

Profil 1: Decentralizirani pristop – več sektorskih organov, pristojnih za določene sektorje in storitve iz prilog II in III k Direktivi

Značilnosti decentraliziranega pristopa so:

(i) načelo subsidiarnosti,
(ii) tesno sodelovanje med javnimi agencijami,
(iii)sektorska zakonodaja.

Načelo subsidiarnosti

V okviru decentraliziranega pristopa ni določena ena sama agencija s splošno pristojnostjo, temveč se sledi načelu subsidiarnosti. To pomeni, da je za izvajanje odgovoren tisti sektorski organ, ki najbolje pozna lokalni sektor in ima že vzpostavljen odnos z zainteresiranimi stranmi. V skladu s tem načelom odločitve sprejema organ, ki je najbližje tistim, na katere bodo te odločitve vplivale.

Tesno sodelovanje med javnimi agencijami

Zaradi raznolikosti javnih agencij, ki se ukvarjajo z zaščito kritične informacijske infrastrukture, so številne države članice razvile programe sodelovanja za usklajevanje dela in prizadevanj različnih organov. Ti programi sodelovanja so lahko zasnovani v obliki neformalnih mrež ali bolj institucionaliziranih forumov ali ureditev. Ne glede na to pa so ti programi namenjeni izključno izmenjavi informacij in usklajevanju med različnimi javnimi agencijami, nimajo pa nad njimi nikakršne avtoritete.

Sektorska zakonodaja

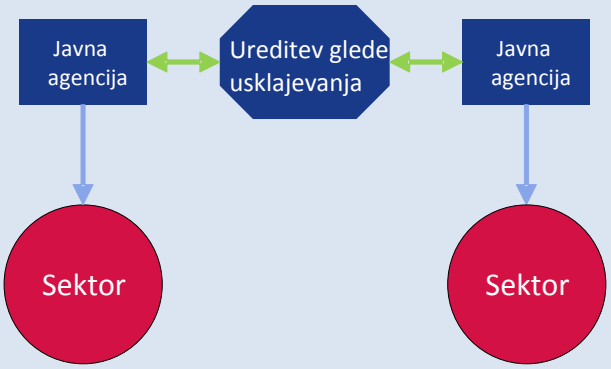
Države, ki v ključnih sektorjih uporabljajo decentralizirani pristop, področja zaščite kritične informacijske infrastrukture pogosto ne urejajo zakonodajno, temveč se zakoni in predpisi sprejemajo sektorsko in se zato lahko od sektorja do sektorja zelo razlikujejo. Prednost tega pristopa je, da so ukrepi, povezani z varnostjo omrežij in informacij, prilagojeni obstoječim sektorskim predpisom, s čimer se izboljša tako njihovo sprejemanje s strani sektorja kot tudi učinkovitost njihovega izvrševanja s strani pristojnega organa.

Pri popolnoma decentraliziranem pristopu obstaja precejšnje tveganje za nedosledno izvajanje Direktive v različnih sektorjih in za različne storitve. V tem primeru Direktiva določa enotno

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (Ocena stanja, analiza in priporočila o zaščiti kritične informacijske infrastrukture) (2016). Na voljo na: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis.

nacionalno kontaktno točko za povezovanje v čezmejnih zadevah, ta subjekt pa bi zadevna država članica lahko zadolžila tudi za notranje usklajevanje in sodelovanje med različnimi pristojnimi nacionalnimi organi v skladu s členom 10 Direktive.

Slika 2: Decentralizirani pristop



Primeri decentraliziranega pristopa

Lep primer države, ki uporablja decentralizirani pristop k zaščiti kritične informacijske infrastrukture, je Švedska. Švedska uporablja „sistemski vidik“, kar pomeni, da so za glavne naloge na področju zaščite kritične informacijske infrastrukture, kot so opredelitev bistvenih storitev in kritične infrastrukture, usklajevanje izvajalcev in podpora zanje, regulativne naloge ter ukrepi za pripravljenost na izredne razmere, odgovorne različne agencije in občine. Omenjene agencije vključujejo Švedsko agencijo za civilno ukrepanje v izrednih razmerah (MSB), Švedsko agencijo za pošto in telekomunikacije (PTS) in več drugih agencij s področja obrambe, vojske ter preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

Za usklajevanje ukrepov med različnimi agencijami in javnimi subjekti je švedska vlada razvila sodelovalno mrežo, ki jo sestavljajo organi „s posebnimi družbenimi pristojnostmi na področju varnosti informacij“. Ta sodelovalna skupina za varnost informacij (SAMFI) vključuje predstavnike različnih organov in se sestane večkrat letno, da razpravlja o vprašanjih, povezanih z nacionalno varnostjo informacij. SAMFI obravnava predvsem politično-strateška področja, zlasti teme, kot so tehnična vprašanja in standardizacija, razvoj na področju varnosti informacij na nacionalni in mednarodni ravni ter obvladovanje in preprečevanje incidentov na področju IT (MSB, 2015).

Švedska nima centralne zakonodaje s področja zaščite kritične informacijske infrastrukture, ki bi veljala za upravljavce take infrastrukture v vseh sektorjih, temveč so za sprejemanje zakonodaje, ki nalaga obveznosti podjetjem iz posameznih sektorjev, odgovorni zadevni javni organi. Tako ima na primer MSB pravico, da vladnim organom s področja varnosti informacij izdaja uredbe, PTS pa lahko od upravljavcev zahteva, da izvedejo določene tehnične ali organizacijske varnostne ukrepe, ki temeljijo na sekundarni zakonodaji.

Primer države, ki uporablja decentralizirani pristop, je tudi Irska. Irska sledi načelu subsidiarnosti, pri čemer je vsako ministrstvo odgovorno za opredelitev kritične informacijske infrastrukture in oceno tveganj v sektorju, za katerega je pristojno. Poleg tega na nacionalni ravni niso bili sprejeti nobeni posebni predpisi glede zaščite kritične informacijske infrastrukture. Obstoječa zakonodaja je sektorska in velja predvsem za področje energetike in telekomunikacijski sektor (2015). Decentralizirani pristop uporabljajo tudi Avstrija, Ciper in Finska.

Profil 2: Centralizirani pristop – en osrednji organ, pristojen za vse sektorje in storitve iz prilog II in III k Direktivi

Značilnosti centraliziranega pristopa sta:

i) en osrednji organ za vse sektorje,
ii) celovita zakonodaja.

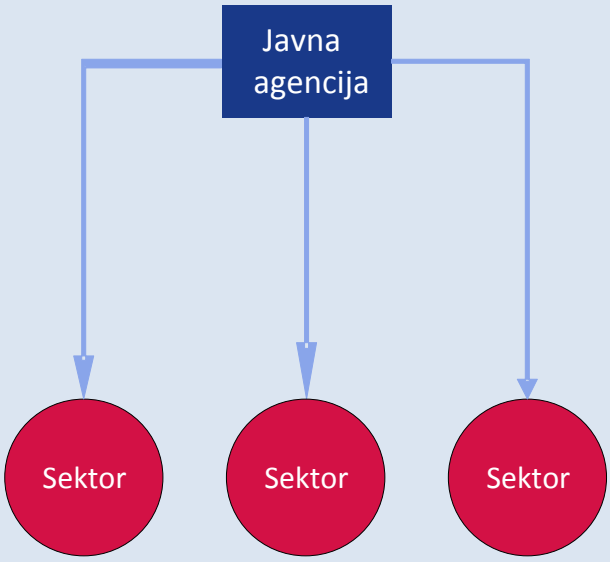
En osrednji organ za vse sektorje

Države članice, ki uporabljajo centralizirani pristop, so vzpostavile organe z odgovornostmi in širokimi pristojnostmi za več ali vse ključne sektorje ali pa so razširile pooblastila obstoječim organom. Ti glavni organi za zaščito kritične informacijske infrastrukture združujejo več zadolžitev, kot so načrtovanje ravnanja v nepredvidljivih razmerah, obvladovanje izrednih razmer, regulativne naloge in podpora zasebnim upravljavcem. V več primerih je nacionalna ali vladna skupina CSIRT del glavnega organa za zaščito kritične informacijske infrastrukture. Glede na splošno pomanjkanje znanj in spretnosti s področja kibernetske varnosti bo osrednjemu organu verjetno na voljo več združenega strokovnega znanja s tega področja kot več posameznim sektorskim organom.

Celovita zakonodaja

Celovita zakonodaja določa obveznosti in zahteve za vse upravljavce kritične informacijske strukture v vseh sektorjih. To je mogoče doseči z novimi celovitimi zakoni ali z dopolnitvijo obstoječih sektorskih predpisov. Ta pristop lahko zagotovi dosledno uporabo direktive o varnosti omrežij in informacij v vseh zadevnih sektorjih in storitvah. S tem bi se izničilo tveganje za vrzeli v izvajanju, do katerih bi lahko prišlo, če bi bile posebne pristojnosti podeljene več organom.

Slika 3: Centralizirani pristop



Primeri centraliziranega pristopa

Lep primer države članice EU, ki uporablja centralizirani pristop, je Francija. Francoska agencija za varnost informacijskih sistemov (ANSSI) je bila leta 2011 razglašena za glavni nacionalni organ na področju zaščite informacijskih sistemov. ANSSI ima pomembno vlogo pri nadzoru „ključnih upravljavcev“, od katerih lahko zahteva skladnost z varnostnimi ukrepi, in je pooblaščena, da pri njih izvede varnostni nadzor. Ima tudi vlogo osrednje enotne kontaktne točke za ključne upravljavce, ki morajo agenciji poročati o varnostnih incidentih.

V primeru varnostnih incidentov ANSSI deluje kot agencija za ukrepanje v izrednih razmerah na področju zaščite kritične informacijske infrastrukture in sprejema odločitve o ukrepih, ki jih morajo v odziv na krize izvesti upravljavci. Vladni ukrepi se usklajujejo v operativnem centru ANSSI. Odkrivanje groženj in odziv na incidente na operativni ravni kot del ANSSI izvaja CERT-FR.

Francija ima vzpostavljen celovit pravni okvir za zaščito kritične informacijske infrastrukture. Leta 2006 je predsednik vlade odredil pripravo seznama sektorjev s kritično infrastrukturo. Vlada je na podlagi tega seznama opredelila dvanajst ključnih sektorjev s približno 250 ključnimi upravljavci. Leta 2013 je bil razglašen Zakon o načrtovanju vojaških zmogljivostih[13], ki določa različne obveznosti za ključne upravljavce, med drugim poročanje o incidentih in izvajanje varnostnih ukrepov. Te zahteve so obvezne za vse ključne upravljavce v vseh

[13] *La loi de programmation militaire*.

sektorjih (francoski senat, 2013).

3.3 Člen 9 direktive o varnosti omrežij in informacij: Skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT)

Države članice morajo v skladu s členom 9 določiti eno ali več skupin CSIRT, ki jih zadolžijo za obvladovanje incidentov in tveganj v sektorjih, navedenih v Prilogi II k Direktivi, in storitvah, navedenih v Prilogi III. Ob upoštevanju zahteve po minimalni harmonizaciji iz člena 3 Direktive lahko države članice po svoji presoji skupine CSIRT uporabijo tudi v drugih sektorjih, ki niso zajeti v Direktivi, na primer v javni upravi.

Države članice lahko skupine CSIRT ustanovijo v okviru pristojnega nacionalnega organa[14].

3.4 Naloge in zahteve

Naloge določenih skupin CSIRT so navedene v Prilogi I k direktivi o varnosti omrežij in informacij ter vključujejo:

- spremljanje incidentov na nacionalni ravni;
- zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o tveganjih in incidentih deležnikom;
- odzivanje na incidente;
- opravljanje dinamičnih analiz tveganja in incidentov ter spremljanje razmer; ter
- sodelovanje v mreži nacionalnih skupin CSIRT (mreži skupin CSIRT), ustanovljeni v skladu s členom 12.

Posebne dodatne naloge v zvezi s priglasitvijo incidentov, kadar se države članice odločijo, da lahko poleg ali namesto pristojnih nacionalnih organov takšne vloge prevzamejo skupine CSIRT, so določene v členih 14(3), 14(5), 14(6), 16(3), 16(6) in 16(7) Direktive.

Države članice imajo pri prenosu Direktive različne možnosti glede vloge skupin CSIRT v zvezi s priglasitvijo incidentov. Možno je neposredno obvezno poročanje skupinam CSIRT, s čimer se poveča upravna učinkovitost, sicer pa države članice lahko odločijo za možnost, pri kateri se neposredno poroča pristojnim nacionalnim organom, skupine CSIRT pa imajo pravico dostopa do sporočenih informacij. Skupine CSIRT so pri reševanju problemov skupaj

[14] Gl. zadnji stavek člena 9(1).

z zainteresiranimi stranmi osredotočene na preprečevanje kibernetskih incidentov (vključno s tistimi, ki niso tako kritični, da bi zanje veljala obveznost poročanja) ter odzivanje nanje in blaženje njihovih učinkov, preverjanje skladnosti s predpisi pa je v domeni pristojnih nacionalnih organov.

V skladu s členom 9(3) Direktive morajo države članice tudi zagotoviti, da imajo skupine CSIRT dostop do varne in odporne komunikacijske in informacijske infrastrukture.

Člen 9(4) Direktive od držav članic zahteva, da Komisijo obvestijo o pristojnostih skupin CSIRT, ki so jih določile, in o glavnih elementih njihovega postopka za obvladovanje incidentov.

Zahteve za skupine CSIRT, ki so jih določile države članice, so navedene v Prilogi I k direktivi o varnosti omrežij in informacij. Skupine CSIRT morajo zagotoviti visoko stopnjo razpoložljivosti svojih komunikacijskih storitev. Njihovi uradi in podporni informacijski sistemi se morajo nahajati na varnih krajih in morajo omogočati neprekinjeno poslovanje. Poleg tega morajo skupine CSIRT imeti možnost, da so delujejo v mednarodnih mrežah za sodelovanje.

3.5 Pomoč pri oblikovanju skupin CSIRT

Program infrastrukture digitalnih storitev za kibernetsko varnost instrumenta za povezovanje Evrope lahko zagotovi znatna sredstva EU za pomoč skupinam CSIRT držav članic pri izboljšanju njihovih zmogljivosti in njihovega medsebojnega sodelovanja prek mehanizma za sodelovanje z izmenjavo informacij. Namen mehanizma za sodelovanje, ki je v pripravi v okviru projekta SMART 2015/1089, je poenostaviti hitro in učinkovito prostovoljno operativno sodelovanje med skupinami CSIRT držav članic, zlasti za podpiranje nalog, ki so mreži skupin CSIRT dodeljene v členu 12 Direktive.

Podrobnosti o zadevnih razpisih za zbiranje predlogov za krepitev zmogljivosti skupin CSIRT držav članic so na voljo na spletišču Izvajalske agencije za inovacije in omrežja (INEA) Evropske komisije[15].

Upravljalni odbor programa infrastrukture digitalnih storitev za kibernetsko varnost instrumenta za povezovanje Evrope zagotavlja neformalno strukturo za smernice in pomoč skupinam CSIRT držav članic na ravni politike, da se okrepi njihova zmogljivost, ter za izvajanje prostovoljnega mehanizma za sodelovanje.

Skupina CSIRT, ki je ustanovljena na novo ali imenovana za izpolnjevanje nalog iz Priloge I k direktivi o varnosti omrežij in informacij, se lahko za izboljšanje delovanja in učinkovito izvajanje nalog opira na nasvete in strokovno znanje agencije ENISA[16]. V zvezi s tem je treba opozoriti, da se lahko skupine CSIRT držav članic oprejo na nedavno opravljeno delo agencije ENISA. Agencija je, kot je navedeno v oddelku 7 te priloge, objavila več dokumentov in študij, ki opisujejo dobre prakse, ter tehničnih priporočil, ki zajemajo oceno

[15] Na voljo na: https://ec.europa.eu/inea/en/connecting-europe-facility.
[16] Glej člen 9(5) direktive o varnosti omrežij in informacij.

zrelosti skupin CSIRT, za različne zmogljivosti in storitve skupin CSIRT. Poleg tega so smernice in najboljše prakse delile tudi mreže skupin CSIRT, in sicer tako na svetovni (FIRST[17]) kot evropski ravni (Trusted Introducer, TI[18]).

3.6 Vloga enotne kontaktne točke

V skladu s členom 8(3) direktive o varnosti omrežij in informacij mora vsaka država članica določiti enotno kontaktno točko, ki ima povezovalno vlogo in zagotavlja čezmejno sodelovanje z ustreznimi organi drugih držav članic ter s skupino za sodelovanje in mrežo skupin CSIRT[19], ki sta ustanovljeni z navedeno direktivo. Uvodna izjava 31 in člen 8(4) vsebujeta utemeljitev te zahteve, in sicer zagotavljanje lažjega čezmejnega sodelovanja in komunikacije. To je zlasti potrebno glede na to, da se države članice lahko odločijo, da imenujejo več kot en nacionalni organ. Enotna kontaktna točka bi zato olajšala iskanje organov iz različnih držav članic in sodelovanje med njimi.

Povezovalna vloga enotne kontaktne točke bo verjetno vključevala sodelovanje s sekretariati skupine za sodelovanje in mreže skupin CSIRT v primerih, ko nacionalna enotna kontaktna točka ni niti skupina CSIRT niti članica skupine za sodelovanje. Poleg tega morajo države članice zagotoviti, da je enotna kontaktna točka obveščena o prejetih priglasitvah izvajalcev bistvenih storitev in ponudnikov digitalnih storitev[20].

Člen 8(3) Direktive določa, da je v primeru, da se država članica odloči za centraliziran pristop, tj. da določi le en pristojni organ, ta organ tudi enotna kontaktna točka. Če se država članica odloči za decentraliziran pristop, lahko določi, da eden od različnih pristojnih organov deluje kot enotna kontaktna točka. Ne glede na izbrani institucionalni model velja, da morajo države članice v primeru, da so pristojni organ, skupina CSIRT in enotna kontaktna točka ločeni subjekti, zagotoviti učinkovito sodelovanje med njimi, da izpolnijo obveznosti, ki jih določa Direktiva[21].

Enotna kontaktna točka mora do 9. avgusta 2018 in nato vsako leto skupini za sodelovanje predložiti zbirno poročilo o prejetih priglasitvah, vključno s številom priglasitev, vrsto incidentov in ukrepi, ki so jih organi sprejeli, na primer obveščanje drugih prizadetih držav članic o incidentu ali zagotavljanje pomembnih informacij priglasitelju za obvladovanje incidentov[22]. Enotna kontaktna točka mora na zahtevo pristojnega organa ali skupine CSIRT priglasitve izvajalcev bistvenih storitev posredovati enotnim kontaktnim točkam drugih prizadetih držav članic[23].

[17] Forum skupin za odzivanje na incidente in računalniško varnost (Forum of Incident Response and Security Teams) (https://www.first.org/).
[18] https://www.trusted-introducer.org/.
[19] Mreža nacionalnih skupin CSIRT za operativno sodelovanje med državami članicami iz člena 12.
[20] Glej člen 10(3).
[21] Glej člen 10(1).
[22] Glej prejšnjo opombo.
[23] Glej člen 14(5).

Države članice morajo Komisijo do roka za prenos obvestiti o določitvi enotne kontaktne točke in njenih nalogah. Določitev enotne kontaktne točke je treba javno objaviti, enako kot pristojne nacionalne organe. Komisija objavi seznam določenih enotnih kontaktnih točk.

3.7 Kazni

Člen 21 državam članicam daje pravico, da same določijo vrsto in naravo kazni, pod pogojem, da so te učinkovite, sorazmerne in odvračilne. Države članice lahko tako načeloma same določijo najvišji znesek kazni, ki se zapiše v nacionalno zakonodajo, vendar bi moral določeni znesek ali odstotek nacionalnim organom omogočiti, da v vsakem posameznem primeru naložijo učinkovite, sorazmerne in odvračilne kazni ob upoštevanju različnih dejavnikov, kot so resnost in pogostost kršitve.

4. Subjekti, za katere veljajo obveznosti glede varnostnih zahtev in priglasitve incidentov

Subjekti, ki imajo pomembno vlogo v družbi in gospodarstvu ter so v členu 4(4) in 4(5) Direktive opredeljeni kot izvajalci bistvenih storitev in ponudniki digitalnih storitev, morajo sprejeti ustrezne varnostne ukrepe in resne incidente priglasiti zadevnim nacionalnim organom. Razlog za to je, da lahko varnostni incidenti v teh subjektih močno ogrozijo delovanje takih storitev, kar lahko povzroči večje motnje v gospodarskih dejavnostih in v družbi kot celoti, to pa lahko oslabi zaupanje uporabnikov in povzroči veliko škodo gospodarstvu Unije[24].

Ta oddelek vsebuje pregled subjektov iz področja uporabe prilog II in III k direktivi o varnosti omrežij in informacij ter seznam njihovih obveznosti. Obširno je obravnavana določitev izvajalcev bistvenih storitev, saj je ta postopek pomemben za harmonizirano izvajanje direktive o varnosti omrežij in informacij po vsej EU. Prav tako sta obširno pojasnjeni opredelitvi digitalne infrastrukture in ponudnikov digitalnih storitev. Preučena je tudi možnost vključitve dodatnih sektorjev in pojasnjen posebni pristop v zvezi s ponudniki digitalnih storitev.

4.1 Izvajalci bistvenih storitev

Direktiva o varnosti omrežij in informacij ne določa izrecno, kateri subjekti se bodo v njenem področju uporabe obravnavali kot izvajalci bistvenih storitev. Določa pa merila, ki jih bodo morale države članice uporabljati pri izvajanju postopka določitve, na podlagi katerega se bo določilo, katera posamezna podjetja, ki spadajo med vrste subjektov iz Priloge II, se bodo obravnavala kot izvajalci bistvenih storitev in bodo zato zanje veljale obveznosti iz Direktive.

4.1.1 Vrste subjektov iz Priloge II k direktivi o varnosti omrežij in informacij

Člen 4(4) izvajalca bistvenih storitev opredeljuje kot javni ali zasebni subjekt, ki spada med vrste iz Priloge II k Direktivi in izpolnjuje merila, določena v členu 5(2). V Prilogi II so

[24] Glej uvodno izjavo 2.

navedeni sektorji, podsektorji in vrste subjektov, za katere mora vsaka država članica opraviti postopek določitve v skladu s členom 5(2)[25]. Vključeni sektorji so energija, promet, bančništvo, infrastruktura finančnega trga, zdravstvo, voda in digitalna infrastruktura.

Za večino subjektov iz „tradicionalnih sektorjev“ so v zakonodaji EU določene natančne opredelitve, na katere se sklicuje Priloga II. To pa ne velja za sektor digitalne infrastrukture iz točke 7 Priloge II, vključno s stičišči omrežij, sistemi domenskih imen in registri domenskih imen najvišje ravni. Za pojasnitev so te opredelitve podrobneje razložene v nadaljevanju.

1) Stičišče omrežij

Pojem stičišče omrežij, ki je opredeljen v členu 4(13) in dodatno pojasnjen v uvodni izjavi 18, je mogoče opisati kot omrežno zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih tehnološko avtonomnih sistemov, predvsem zaradi lažje izmenjave internetnega prometa. Stičišče omrežij je mogoče opisati tudi kot fizično lokacijo, na kateri si lahko več omrežij med seboj izmenjuje internetni promet prek omrežnega stikala. Glavni namen stičišča omrežij je omogočanje neposredne medsebojne povezave omrežij prek omrežnega stikala brez prehoda prek enega ali več tretjih omrežij. Ponudnik stičišča omrežij običajno ni odgovoren za usmerjanje internetnega prometa. Za to so pristojni ponudniki omrežnih storitev. Prednosti neposredne medsebojne povezave so številne, med glavnimi pa so stroški, latenca in pasovna širina. Prometa prek stičišča omrežja običajno nobena stran ne zaračunava, kar pa ne velja za promet do ponudnika internetnih storitev višje v omrežju. Pri neposredni medsebojni povezavi, ki se pogosto nahaja v istem mestu kot obe omrežji, podatkom ni treba prepotovati dolgih razdalj, da pridejo od enega omrežja do drugega, s čimer se zmanjša latenca.

Treba je opozoriti, da opredelitev stičišča omrežij ne zajema fizične točke, kjer se medsebojno povežeta samo dve fizični omrežji (na primer ponudnika omrežnih storitev, kot sta BASE in PROXIMUS). Zato morajo države članice pri prenosu Direktive razlikovati med izvajalci, ki olajšujejo izmenjavo skupnega internetnega prometa med več omrežnimi operaterji, in tistimi, ki so operaterji enega omrežja in svoja omrežja fizično povezujejo na podlagi sporazuma o povezovanju. V drugem primeru ponudniki omrežnih storitev niso zajeti v opredelitvi iz člena 4(13). Pojasnilo v zvezi s tem je v uvodni izjavi 18, ki navaja, da stičišče omrežij ne zagotavlja dostopa do omrežja oziroma ni ponudnik ali nosilec prenosa. Zadnja kategorija ponudnikov so podjetja, ki zagotavljajo javna komunikacijska omrežja in/ali storitve, za katera veljajo obveznosti glede varnosti in priglasitve iz členov 13a in 13b Direktive 2002/21/ES in ki so zato izvzeta iz področja uporabe direktive o varnosti omrežij in informacij[26].

2) Sistem domenskih imen

[25] Za podrobnosti o postopku določitve glej oddelek 4.1.6.
[26] Za podrobnosti o povezavi med direktivo o varnosti omrežij in informacij ter Direktivo 2002/21/ES glej oddelek 5.2.

Pojem sistem domenskih imen je v členu 4(14) opredeljen kot „hierarhičen porazdeljen sistem dodeljevanja imen v omrežju, ki posreduje poizvedbe za domenska imena“. Natančneje je sistem domenskih imen mogoče opisati kot hierarhičen porazdeljen sistem dodeljevanja imen za računalnike, storitve ali katere koli druge vire, povezane z internetom, ki omogoča kodiranje domenskih imen v naslove IP. Glavna vloga sistema je pretvorba dodeljenih domenskih imen v naslove IP. V ta namen sistem domenskih imen upravlja podatkovno zbirko ter uporablja imenske strežnike in razreševalnik, da omogoči pretvorbo domenskih imen v delujoče naslove IP. Kodiranje domenskih ni edina odgovornost sistema domenskih imen, je pa njegova osrednja naloga. Pravna opredelitev iz člena 4(14) se osredotoča na glavno vlogo sistema z vidika uporabnika, ne spušča pa se v bolj tehnične podrobnosti, kot je na primer delovanje prostora domenskih imen, imenskih strežnikov, razreševalnikov itd. Nazadnje člen 4(15) pojasnjuje, kdo se šteje za ponudnika storitev sistema domenskih imen.

3) Register domenskih imen najvišje ravni

Register domenskih imen najvišje ravni je v členu 4(16) opredeljen kot subjekt, ki upravlja in izvaja registracijo imen internetnih domen v okviru določene domene najvišje ravni. Tako upravljanje in vodenje domenskih imen vključuje kodiranje domenskih imen najvišje ravni v naslove IP.

IANA (organ za dodeljevanje internetnih naslovov) je odgovoren za svetovno usklajevanje korena DNS, naslavljanje internetnega protokola in druge vire internetnega protokola. Zlasti je odgovoren za dodeljevanje generičnih domen najvišje ravni, npr. „.com“, in državnih domen najvišje ravni, npr. „.be“, operaterjem (registrom) ter za hranjenje njihovih tehničnih in administrativnih podatkov. IANA upravlja svetovni register dodeljenih domen najvišje ravni, poleg tega pa sodeluje pri razširjanju tega seznama uporabnikom interneta po vsem svetu ter uvajanju novih domen najvišje ravni.

Pomembna naloga registrov je dodeljevanje imen druge ravni t. i. registrantom v okviru ustreznih domen najvišje ravni. Če želijo, lahko ti registranti tudi sami dodelijo domenska imena tretje ravni. Državne domene najvišjih ravni predstavljajo državo ali ozemlje na podlagi standarda ISO 3166-1. „Generične“ domene najvišje ravni običajno nimajo geografske ali državne oznake.

Opozoriti je treba, da upravljanje registra domenskih imen najvišje ravni lahko vključuje zagotavljanje sistema domenskih imen. V skladu s pravili IANA glede prenosa pooblastil imenovani subjekt, ki se ukvarja s potrebami glede državnih domen najvišje ravni, med drugim nadzoruje domenska imena in upravlja sistem domenskih imen zadevne države[27]. Države članice morajo pri izvajanju postopka določitve izvajalcev bistvenih storitev iz člena 5(2) upoštevati take okoliščine.

[27] Informacije so na voljo na naslovu: https://www.icann.org/resources/pages/delegation-2012-02-25-en.

4.1.2 Določitev izvajalcev bistvenih storitev

V skladu z zahtevami iz člena 5 Direktive mora vsaka država članica izvesti postopek določitve za vse subjekte, ki spadajo med vrste iz Priloge II in imajo zakoniti sedež na ozemlju zadevne države članice. Na podlagi te ocene se vsi subjekti, ki izpolnjujejo merila iz člena 5(2), opredelijo kot izvajalci bistvenih storitev, za katere veljajo obveznosti glede varnosti in priglasitve iz člena 14.

Države članice izvajalce za vsak sektor in podsektor določijo do 9. novembra 2018. Za podporo državam članicam pri tem postopku skupina za sodelovanje trenutno pripravlja smernice z vsemi pomembnimi informacijami o potrebnih korakih in najboljših praksah v zvezi z določitvijo izvajalcev bistvenih storitev.

Poleg tega bo v skladu s členom 24(2) skupina za sodelovanje obravnavala postopek, vsebino in vrsto nacionalnih ukrepov, ki omogočajo določitev izvajalcev bistvenih storitev v posameznih sektorjih. Države članice lahko pred 9. novembrom 2018 za razpravo v skupini za sodelovanje predložijo osnutek nacionalnih ukrepov, ki omogočajo določitev izvajalcev bistvenih storitev.

4.1.3 Vključitev dodatnih sektorjev

Ob upoštevanju zahteve glede minimalne harmonizacije iz člena 3 lahko države članice sprejmejo ali ohranijo določbe za doseganje višje stopnje varnosti omrežij in informacijskih sistemov. V zvezi s tem imajo države članice načeloma pravico, da razširijo obveznosti glede varnosti in priglasitve iz člena 14 na subjekte, ki spadajo v sektorje in podsektorje, ki niso navedeni v Prilogi II k direktivi o varnosti omrežij in informacij. Različne države članice so že vključile nekatere od naslednjih dodatnih sektorjev ali pa o tem razmišljajo:

i) Javne uprave

Javne uprave lahko ponujajo bistvene storitve iz Priloge II k Direktivi, ki izpolnjujejo zahteve iz člena 5(2). V takih primerih bi za javne uprave, ki ponujajo take storitve, veljale ustrezne varnostne zahteve in obveznosti priglasitve. Nasprotno pa v primerih, ko javne uprave ponujajo storitve, ki ne spadajo v navedeno področje uporabe, za take storitve navedene obveznosti ne bi veljale.

Javne uprave so odgovorne za pravilno izvajanje javnih storitev, ki jih zagotavljajo vladni, regionalni in lokalni organi, agencije in povezana podjetja. Te storitve pogosto vključujejo ustvarjanje in obdelavo osebnih in poslovnih podatkov o posameznikih in organizacijah, ki se lahko delijo ali dajo na voljo več javnim subjektom. V širšem smislu je visoka raven varnosti omrežij in informacijskih sistemov, ki jih uporabljajo javne uprave, velikega pomena za družbo in gospodarstvo kot celoto. Komisija zato meni, da bi bilo primerno, da države članice razmislijo o vključitvi javnih uprav v področje uporabe nacionalne zakonodaje, ki prenaša Direktivo, in sicer v obsegu, ki presega zagotavljanje bistvenih storitev, kot so določene v Prilogi II in členu 5(2).

ii) Poštni sektor

Poštni sektor zajema zagotavljanje poštnih storitev, kot so zbiranje, razvrščanje, prevoz in dostavljanje poštnih pošiljk.

iii) Prehrambeni sektor

Prehrambeni sektor zadeva proizvodnjo kmetijskih in drugih prehrambenih izdelkov in bi lahko vključeval bistvene storitve, kot so zagotavljanje prehranske varnosti ter kakovosti in varnosti hrane.

iv) Kemična in jedrska industrija

Kemična in jedrska industrija zadevata zlasti skladiščenje, proizvodnjo in obdelavo kemičnih in petrokemičnih izdelkov ali jedrskih snovi.

v) Okoljski sektor

Okoljske aktivnosti zajemajo zagotavljanje blaga in storitev, potrebnih za varstvo okolja in upravljanje virov. Aktivnosti so zato usmerjene na preprečevanje, zmanjševanje in odpravljanje onesnaževanja ter ohranjanje zalog razpoložljivih naravnih virov. V tem sektorju bi bistvene storitve lahko zajemale spremljanje in nadziranje onesnaževanja (npr. zraka in vode) ter meteoroloških pojavov.

vi) Civilna zaščita

Cilj sektorja civilne zaščite je preprečevanje naravnih nesreč in nesreč, ki jih povzroči človek, ter priprava in odzivanje nanje. Storitve za ta namen bi bile lahko aktivacija številk za klic v sili ter izvajanje ukrepov informiranja in obvladovanja nujnih primerov ter odzivanja nanje.

4.1.4 Pristojnost

V skladu s členom 5(1) mora vsaka država članica določiti izvajalce bistvenih storitev s sedežem na svojem ozemlju. Določba ne opredeljuje natančneje vrste zakonitega sedeža, vendar uvodna izjava 21 pojasnjuje, da takšen sedež pomeni učinkovito in dejansko izvajanje dejavnosti na podlagi stabilnih ureditev, pri čemer pravna oblika takih ureditev ne bi smela biti odločilni dejavnik. To pomeni, da ima lahko država članica pristojnost nad izvajalci bistvenih storitev ne le v primerih, ko imajo ti glavni sedež na njenem ozemlju, temveč tudi takrat, ko ima izvajalec na njenem ozemlju podružnico ali drugo vrsto zakonitega sedeža.

Posledično ima lahko več držav članic hkrati pristojnost nad istim subjektom.

4.1.5 Informacije, ki se predložijo Komisiji

Za namene pregleda, ki ga mora Komisija opraviti v skladu s členom 23(1) direktive o varnosti omrežij in informacij, morajo države članice do 9. novembra 2018, nato pa vsaki dve leti, Komisiji predložiti naslednje informacije:

- nacionalne ukrepe, ki omogočajo določitev izvajalcev bistvenih storitev;
- seznam bistvenih storitev;
- število izvajalcev bistvenih storitev, določenih za vsak sektor iz Priloge II, in njihov pomen za ta sektor ter

- prage, kadar obstajajo, za določitev ustrezne ravni opravljanja storitev glede na število uporabnikov, ki so odvisni od te storitve, kot je določeno v členu 6(1)(a), ali glede na pomen zadevnega subjekta, kot je določeno v členu 6(1)(f).

Pregled iz člena 23(1), ki se opravi pred celovitim pregledom Direktive, odraža pomen, ki ga sozakonodajalca pripisujeta pravilnemu prenosu Direktive v zvezi z določitvijo izvajalcev bistvenih storitev, da se prepreči razdrobljenost trgov.

Da bi se ta postopek izvedel kar najbolj učinkovito, Komisija države članice spodbuja k razpravi o tem vprašanju ter k izmenjavi pomembnih izkušenj v skupini za sodelovanje. Poleg tega Komisija države članice spodbuja, da ji poleg vseh informacij, ki jih morajo države članice na podlagi Direktive predložiti, sporočijo tudi seznam (po potrebni zaupno) določenih izvajalcev bistvenih storitev, ki so bili na koncu izbrani. Takšni seznami bi Komisiji olajšali oceno doslednosti postopka določitve in izboljšali kakovost te ocene, prav tako pa bi omogočili primerjavo pristopov različnih držav članic, kar bi vodilo k boljšemu uresničevanju ciljev Direktive.

4.1.6 Kako izvesti postopek določitve?

Kot je prikazano na sliki 4, bi morali nacionalni organi pri izvajanju postopka določitve za posamezen subjekt obravnavati šest ključnih vprašanj. V nadaljevanju vsako vprašanje ustreza koraku, ki ga je treba narediti v skladu s členom 5 v povezavi s členom 6 ter ob upoštevanju uporabe člena 1(7).

Korak 1 – **Ali subjekt spada v sektor/podsektor in ustreza vrstam, določenim v Prilogi II k Direktivi?**

Nacionalni organ bi moral oceniti, ali subjekt s sedežem na njegovem ozemlju spada v sektorje in podsektorje iz Priloge II k Direktivi. Priloga II zajema različne gospodarske sektorje, za katere se šteje, da so ključnega pomena za zagotavljanje pravilnega delovanja notranjega trga. Natančneje, Priloga II navaja naslednje sektorje in podsektorje:

- energija: elektrika, nafta in plin;
- promet: zračni, železniški, vodni in cestni;
- bančništvo: kreditne institucije;
- infrastruktura finančnega trga: mesta trgovanja, centralne nasprotne stranke;
- zdravstvo: zdravstvene ustanove (vključno z bolnišnicami in zasebnimi klinikami);
- voda: oskrba s pitno vodo in njena distribucija;
- digitalna infrastruktura: stičišča omrežij, sistemi domenskih imen in registri domenskih imen najvišje ravni[28].

Korak 2 – **Ali se uporablja *lex specialis*?**

[28]Ti subjekti so podrobneje pojasnjeni v oddelku 4.1.1.

V naslednjem koraku mora nacionalni organ oceniti, ali se uporablja določba o *lex specialis*, kot določa člen 1(7). Natančneje, ta določba navaja, da se, kadar pravni akt EU ponudnikom digitalnih storitev ali izvajalcem bistvenih storitev nalaga varnostne zahteve in/ali zahteve glede priglasitve, ki so vsaj enakovredne ustreznim zahtevam iz direktive o varnosti omrežij in informacij, uporabljajo zahteve iz posebnega pravnega akta. Poleg tega uvodna izjava 9 pojasnjuje, da bi morale države članice v primeru, da so izpolnjene zahteve iz člena 1(7), uporabljati določbe iz sektorskih pravnih aktov EU, tudi tiste, ki se nanašajo na pristojnost. Ustrezne določbe direktive o varnosti omrežij in informacij pa se ne bi uporabljale. V tem primeru pristojni organi ne bi smeli nadaljevati postopka določitve iz člena 5(2)[29].

Korak 3 – **Ali izvajalec zagotavlja bistveno storitev v smislu Direktive?**

V skladu s členom 5(2)(a) mora subjekt, ki je predmet postopka določitve, zagotavljati storitev, ki je bistvena za ohranitev ključnih družbenih in/ali gospodarskih dejavnosti. Pri ocenjevanju tega merila bi morale države članice upoštevati, da en subjekt lahko zagotavlja tako bistvene kot nebistvene storitve. To pomeni, da se bodo varnostne zahteve in zahteve glede priglasitve iz direktive o varnosti omrežij in informacij za nekatere izvajalce uporabljale samo v obsegu, v katerem ta izvajalec zagotavlja bistvene storitve.

V skladu s členom 5(3) bi morale države članice pripraviti seznam vseh bistvenih storitev, ki jih izvajalec bistvenih storitev zagotavlja na njihovem ozemlju. Ta seznam morajo predložiti Komisiji do 9. novembra 2018, nato pa vsaki dve leti[30].

Korak 4 – **Ali je storitev odvisna od omrežja ali informacijskega sistema?**

Treba bi bilo tudi pojasniti, ali ta storitev izpolnjuje drugo merilo iz člena 5(2)(b), in zlasti, ali je zagotavljanje bistvene storitve odvisno od omrežij in informacijskih sistemov, kot so določeni v členu 4(1).

Člen 5 – **Ali bi imel varnostni incident pomemben negativen vpliv?**

Člen 5(2)(c) od nacionalnih organov zahteva, da ocenijo, ali bi imel incident pomemben negativen vpliv na zagotavljanje storitve. V tem smislu člen 6(1) določa več medsektorskih dejavnikov, ki jih je treba pri tej oceni upoštevati. Poleg tega člen 6(2) določa, da se pri oceni po potrebi upoštevajo tudi dejavniki, značilni za posamezni sektor.

Medsektorski dejavniki iz člena 6(1) so:

- število uporabnikov, ki so odvisni od storitve zadevnega subjekta;
- odvisnost drugih sektorjev iz Priloge II od storitve tega subjekta;
- stopnja in trajanje vpliva, ki bi ga incidenti lahko imeli na gospodarske in družbene dejavnosti ali javno varnost;
- tržni delež tega subjekta;

[29] Več podrobnosti o uporabi *lex specialis* je navedenih v oddelku 5.1.
[30] Glej člen 5(7)(b).

- geografska razširjenost, kar zadeva območje, ki bi ga incident lahko prizadel;
- pomen subjekta za ohranitev zadostne ravni storitve ob upoštevanju razpoložljivosti alternativnih načinov za zagotavljanje zadevne storitve.

V zvezi z **dejavniki, značilnimi za posamezni sektor**, uvodna izjava 28 navaja nekaj primerov (glej preglednico 4), ki bi bili lahko uporabno vodilo nacionalnim organom.

Preglednica 4: Primeri dejavnikov, značilnih za posamezni sektor, ki bi jih bilo treba upoštevati pri določanju, kako pomemben je negativni vpliv incidenta

Sektor	Primeri dejavnikov, značilnih za posamezni sektor
Dobavitelji energije	količina ali delež nacionalno proizvedene energije
Dobavitelji nafte	količina dobave nafte na dan
Zračni promet (vključno z letališči in letalskimi prevozniki) **Železniški prevoz** **Morska pristanišča**	delež nacionalnega prometa; število potnikov ali tovornih operacij na leto
Bančništvo in infrastruktura finančnega trga	sistemski pomen glede na skupna sredstva; razmerje med skupnimi sredstvi in BDP
Zdravstveni sektor	število bolnikov v oskrbi ponudnika na leto
Pridobivanje in čiščenje vode ter preskrba z njo	obseg, število in vrste uporabnikov, ki se oskrbujejo z vodo (vključno na primer z bolnišnicami, javnimi službami, organizacijami ali posamezniki); obstoj nadomestnih virov vode, ki oskrbujejo isto geografsko območje

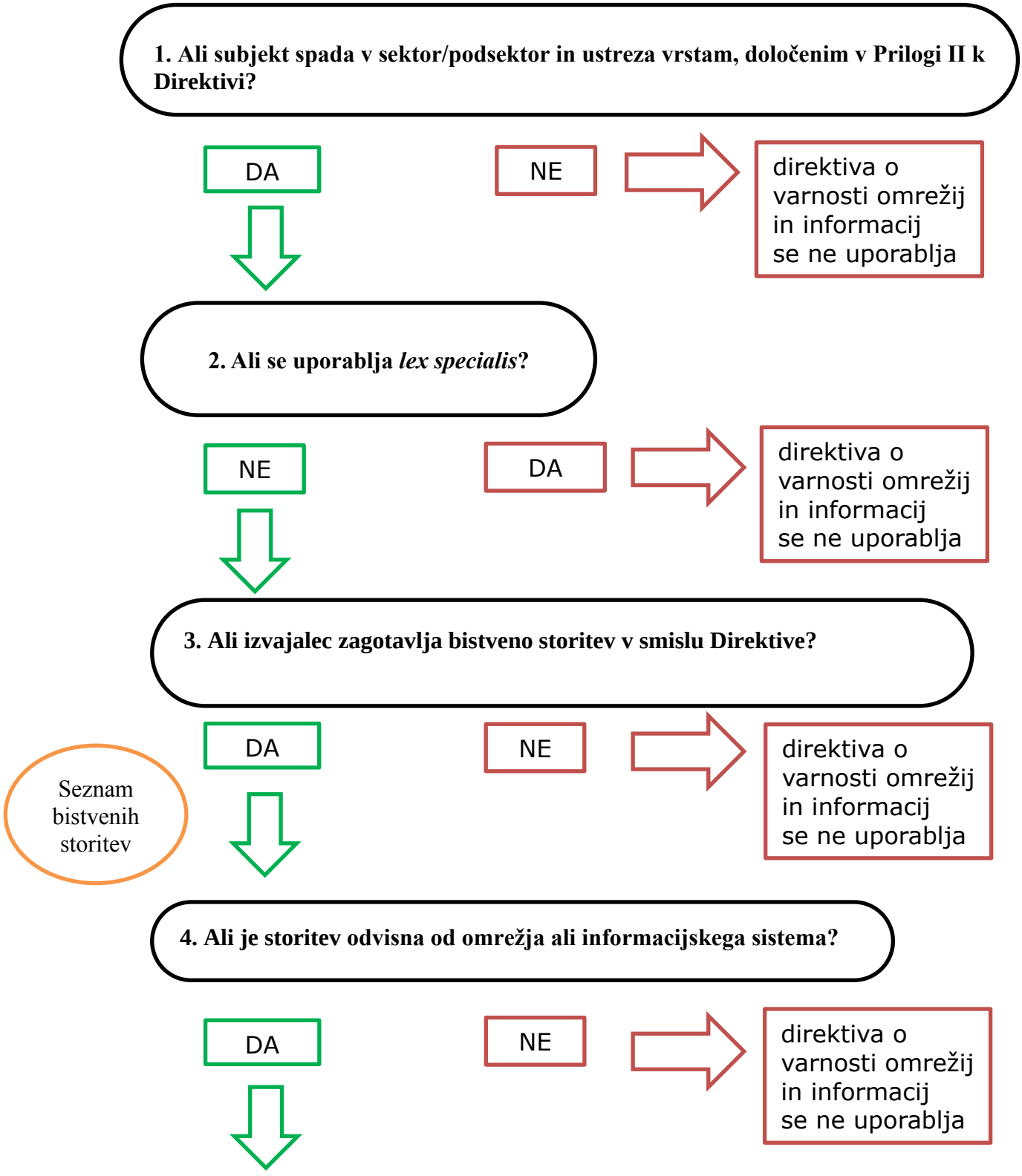
Treba je poudariti, da države članice pri izvajanju ocene iz člena 5(2) merilom iz navedenega člena ne bi smele dodajati dodatnih meril, saj bi to lahko zmanjšalo število določenih izvajalcev bistvenih storitev in ogrozilo minimalno harmonizacijo za izvajalce bistvenih storitev iz člena 3 Direktive.

Korak 6 **– Ali zadevni izvajalec zagotavlja bistvene storitve v drugi državi članici?**

Korak 6 se nanaša na primere, ko izvajalec zagotavlja bistvene storitve v dveh ali več državah članicah. Člen 5(4) zahteva, da se zadevne države članice pred zaključkom postopka določitve med seboj posvetujejo[31].

[31] Za več podrobnosti o postopku posvetovanja glej oddelek 4.1.7.

Slika 4: Postopek določitve v 6 korakih



5. Ali bi imel varnostni incident pomemben negativen vpliv?

Medsektorski dejavniki (člen 6(1))

- **število uporabnikov**, ki so odvisni od storitve
- **odvisnost** drugih bistvenih sektorjev od storitve
- vpliv, ki bi ga incidenti lahko imeli na **gospodarske in družbene dejavnosti** ali **javno varnost**
- potencialna **geografska razširjenost**
- pomen subjekta za ohranitev zadostne **ravni**

Dejavniki, značilni za posamezni sektor (primeri v uvodni izjavi 28)

- **energija**: količina ali delež nacionalno proizvedene energije
- **promet**: delež nacionalnega prometa in število operacij na leto
- **zdravstvo**: število bolnikov v oskrbi ponudnika na leto

DA

NE → direktiva o varnosti omrežij in informacij se ne uporablja

6. Ali zadevni izvajalec zagotavlja bistvene storitve v drugi državi članici?

DA

NE → direktiva o varnosti omrežij in informacij se ne uporablja

Obvezno posvetovanje z zadevnimi državami

Sprejetje nacionalnih ukrepov (npr. seznam izvajalcev bistvenih storitev, ukrepi politike in pravni ukrepi).

4.1.7 Čezmejni postopek posvetovanja

Kadar izvajalec zagotavlja bistveno storitev v dveh ali več državah članicah, člen 5(4) zahteva, da se te države članice med seboj posvetujejo pred zaključkom postopka o določitvi. Namen tega posvetovanja je olajšati oceno kritične narave izvajalca z vidika čezmejnega učinka.

Želeni izid posvetovanja je, da si zadevni organi izmenjajo argumente in stališča ter v najboljšem primeru pridejo do enakih sklepov glede določitve zadevnega izvajalca. Vendar direktiva o varnosti omrežij in informacij državam članicam ne preprečuje, da sprejmejo različne sklepe glede tega, ali se subjekt določi kot izvajalec bistvene dejavnosti ali ne. Uvodna izjava 24 navaja možnost, da države članice v zvezi s tem zaprosijo za pomoč skupine za sodelovanje.

Po mnenju Komisije bi si morale države članice prizadevati doseči soglasje o teh vprašanjih, da se izognejo primerom, da ima isto podjetje drugačen pravni status v različnih državah članicah. Razlikovanje bi moralo biti dopuščeno le v zares izjemnih primerih, ko na primer subjekt, ki je v eni državi članici določen kot izvajalec bistvenih storitev, v drugi državi članici opravlja le obstransko in manj pomembno dejavnost.

4.2 Varnostne zahteve

V skladu s členom 14(1) morajo države članice zagotoviti, da izvajalci bistvenih storitev ob upoštevanju stanja tehnike sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih organizacije uporabljajo pri svojih dejavnostih. V skladu s členom 14(2) ustrezni ukrepi preprečujejo in zmanjšujejo vpliv incidentov.

Namensko delovno telo skupine za sodelovanje trenutno pripravlja nezavezujoče smernice glede varnostnih ukrepov za izvajalce bistvenih storitev[32]. Smernice bodo pripravljene v zadnjem četrtletju 2017. Komisija spodbuja države članice, da se pozorno držijo smernic, ki jih bo pripravila skupina za sodelovanje, da bodo nacionalne določbe glede varnostnih zahtev čim bolj skladne. Harmonizacija takih zahtev bi izvajalcem bistvenih storitev zelo olajšala izpolnjevanje zahtev, saj pogosto zagotavljajo bistvene storitve v več kot eni državi članici, prav tako pa bi poenostavila nadzorne naloge pristojnih nacionalnih organov in skupin CSIRT.

4.3 Zahteve glede priglasitve

V skladu s členom 14(3) morajo države članice zagotoviti, da izvajalci bistvenih storitev priglasijo „incidente s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev“. Zato izvajalcem bistvenih storitev ni treba priglasiti manjših incidentov, ampak samo resnejše,

[32] Za namene tega delovnega telesa so bili razposlani seznami mednarodnih standardov, dobrih praks ter metodologij za oceno/obvladovanje tveganja za vse sektorje, ki jih zajema direktiva o varnosti omrežij in informacij, in se uporabili za predlagane varnostne domene in ukrepe.

ki vplivajo na neprekinjeno izvajanje bistvenih storitev. Člen 4(7) incident opredeljuje kot „vsak dogodek, ki ima dejanski negativen učinek na varnost omrežij in informacijskih sistemov“. Pojem varnost omrežij in informacijskih sistemov je v členu 4(2) opredeljen kot „zmožnost omrežij in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vse dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali pripadajočih storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopne“. Potencialno tako lahko za vsak dogodek, ki ima negativen učinek na razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov ali pripadajočih storitev, velja obveznost priglasitve. Neprekinjeno izvajanje storitve iz člena 14(3) je lahko ogroženo tako v primerih, ko gre za fizično razpoložljivost, kot tudi v primerih, ko kateri koli drug varnostni incident vpliva na pravilno zagotavljanje storitve[33].

Namensko delovno telo znotraj skupine za sodelovanje trenutno pripravlja nezavezujoče smernice za priglasitev v zvezi z okoliščinami, v katerih morajo izvajalci bistvenih storitev priglasiti incidente v skladu s členom 14(7), ter obliko in postopek nacionalnih priglasitev. Smernice bodo predvidoma pripravljene v zadnjem četrtletju leta 2017.

Različne nacionalne zahteve glede priglasitve lahko povzročijo pravno negotovost, bolj zapletene in dolgotrajne postopke ter visoke upravne stroške izvajalcev, ki poslujejo v več državah članicah. Zato Komisija pozdravlja delo skupine za sodelovanje. Kot pri varnostnih zahtevah Komisija tudi pri zahtevah glede priglasitve spodbuja države članice, da se pozorno držijo smernic, ki jih bo pripravila skupina za sodelovanje, da bodo nacionalne določbe glede priglasitve incidentov čim bolj skladne.

4.4 Direktiva o varnosti omrežij in informacij, Priloga III: ponudniki digitalnih storitev

Ponudniki digitalnih storitev so druga kategorija subjektov, vključenih v področje uporabe direktive o varnosti omrežij in informacij. Ti subjekti se štejejo za pomembne gospodarske akterje, saj jih številna podjetja uporabljajo za zagotavljanje svojih storitev, prekinitev digitalnih storitev pa bi lahko vplivala na ključne ekonomske in družbene dejavnosti.

4.4.1 Kategorije ponudnikov digitalnih storitev

Člen 4(5), ki opredeljuje digitalno storitev, se sklicuje na pravno opredelitev iz točke (b) člena 1(1) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta in področje uporabe zožuje na vrste storitev iz Priloge III. Natančneje, točka (b) člena 1(1) Direktive (EU) 2015/1535 te storitve opredeljuje kot „katero koli storitev, ki se običajno opravi odplačno, na daljavo, elektronsko in na posamezno zahtevo prejemnika storitev“, Priloga III k Direktivi pa navaja tri posebne vrste storitev: spletna tržnica, spletni iskalnik in storitev računalništva v oblaku. V nasprotju z izvajalci bistvenih storitev Direktiva od držav članic ne zahteva, da določijo ponudnike digitalnih storitev, za katere bi nato veljale zadevne obveznosti. Zato se bodo zadevne obveznosti iz Direktive, tj. varnostne zahteve in zahteve glede priglasitve iz člena 16, uporabljale za vse ponudnike digitalnih storitev iz področja uporabe Direktive.

[33] Enako velja za ponudnike digitalnih storitev.

Naslednji oddelki vsebujejo dodatna pojasnila v zvezi s tremi vrstami digitalnih storitev iz področja uporabe Direktive.

1. Ponudniki spletnih tržnic

Spletne tržnice številnim različnim podjetjem omogočajo trgovanje s potrošniki in interakcijo med podjetji. Podjetjem nudijo osnovno infrastrukturo za trgovanje na spletu in prek meja. Imajo pomembno vlogo v gospodarstvu, saj zlasti malim in srednjim podjetjem zagotavljajo dostop do širšega enotnega digitalnega trga EU. Med dejavnosti ponudnika spletne tržnice lahko sodijo tudi zagotavljanje storitev računalništva na daljavo, ki olajšujejo gospodarsko dejavnost stranke, vključno z obdelavo transakcij ter združevanjem informacij o kupcih, dobaviteljih in izdelkih, pa tudi omogočanje iskanja ustreznih izdelkov, njihova dobava, strokovno znanje na področju transakcij ter usklajevanje kupcev in prodajalcev.

Pojem „spletna tržnica“ je opredeljen v členu 4(17) in nadalje pojasnjen v uvodni izjavi (15). Opisan je kot storitev, ki potrošnikom in trgovcem omogoča sklepanje pogodb o spletni prodaji in pogodb o spletnih storitvah s trgovci, ki so v okviru nje tudi dokončno sklenjene. Ponudnik kot je na primer *eBay* se lahko šteje za spletno tržnico, saj na svoji platformi drugim omogoča ustanavljanje trgovin, v katerih lahko svoje izdelke in storitve na spletu dajo na voljo potrošnikom ali podjetjem. Tudi za spletne trgovine z aplikacijami za distribucijo aplikacij in programske opreme se šteje, da so opredeljene kot spletne tržnice, saj razvijalcem aplikacij omogočajo prodajo ali distribucijo storitev potrošnikom ali drugim podjetjem. Nasprotno posredniki do storitev tretjih strani, kot je *Skyscanner,* in storitve za primerjavo cen, ki uporabnika preusmerijo na spletišče trgovca, kjer se dejansko sklene pogodba za storitev ali izdelek, ne sodijo v opredelitev iz člena 4(17).

2. Ponudniki spletnega iskanja

Pojem „spletni iskalnik“ je opredeljen v členu 4(18) in nadalje pojasnjen v uvodni izjavi (16). Opisan je kot digitalna storitev, ki uporabnikom na podlagi poizvedbe na katero koli temo omogoča iskanje načeloma po vseh spletiščih ali spletiščih v določenem jeziku. Pojem ne zajema iskalnih funkcij, omejenih na iskanje po enem spletišču, in spletišč za primerjavo cen. Na primer iskalnik, kot je iskalnik na spletišču EUR-Lex[34], se ne more šteti za iskalnik v smislu Direktive, saj je njegova iskalna funkcija omejena na vsebino navedene konkretne spletne strani.

3. Ponudniki storitev računalništva v oblaku

V členu 4(19) je „storitev računalništva v oblaku“ opredeljena kot „digitalna storitev, ki omogoča dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov“, v uvodni izjavi (17) pa so nadalje pojasnjeni pojmi „računalniški viri“, „prožen“ in „prilagodljiv nabor“.

Skratka, računalništvo v oblaku lahko opišemo kot posebno vrsto računalniških storitev, ki uporablja skupne vire za obdelavo podatkov na zahtevo, pri čemer se skupni viri nanašajo na katero koli vrsto komponent strojne ali programske opreme (npr. omrežja, strežniki ali druga

[34] Na voljo na: http://eur-lex.europa.eu/homepage.html?locale=sl.

infrastruktura, pomnilniške naprave, aplikacije in storitve), ki so na zahtevo uporabnikom na voljo za obdelavo podatkov. Pojem „deljiv“ opredeljuje računalniške vire, pri katerih več uporabnikov uporablja isto fizično infrastrukturo za obdelavo podatkov. Računalniški vir se lahko opredeli kot deljiv, če se nabor virov, ki jih ponudnik uporablja, lahko razširi ali zmanjša kadar koli glede na uporabniške zahteve. Zato bi bilo možno dodati ali odvzeti podatkovne centre ali posamezne komponente znotraj enega podatkovnega centra, če bi skupna količina računalniških zmogljivosti ali zmogljivosti shranjevanja potrebovala posodobitev. Pojem „prožen nabor“ je mogoče opisati kot spremembe delovne obremenitve s samodejnim dodajanjem ali odvzemanjem virov, tako da so razpoložljivi viri v vsakem trenutku karseda skladni s trenutnim povpraševanjem.[35]

Trenutno obstajajo tri glavne vrste modelov storitev v oblaku, ki jih ponudnik lahko nudi:

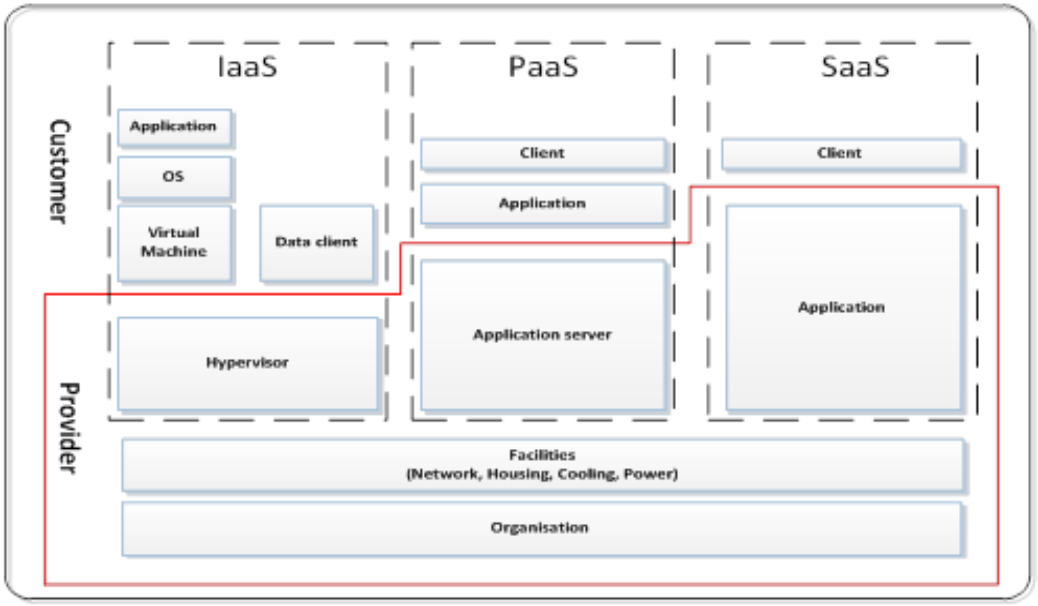
- infrastruktura kot storitev (IaaS): Kategorija storitev v oblaku, pri kateri se stranki kot zmogljivost v oblaku zagotavlja infrastruktura. Vključuje virtualno dobavo računalniških virov v obliki strojnih in mrežnih storitev ter storitev shranjevanja. Na infrastrukturo kot storitev se zanašajo strežniki, pomnilniške naprave, omrežja in operacijski sistemi. Nudi podjetniško infrastrukturo, ki jo lahko podjetja uporabljajo za shranjevanje svojih podatkov in programe, ki jih potrebujejo za vsakodnevno delovanje.

- platforma kot storitev (PaaS): Kategorija storitev v oblaku, pri kateri se stranki kot zmogljivost v oblaku zagotavlja platforma. Vključuje spletne računalniške platforme, ki podjetjem omogočajo, da uporabljajo obstoječe aplikacije ali razvijajo in preskušajo nove.

- programje kot storitev (SaaS): Kategorija storitev v oblaku, pri kateri se stranki kot zmogljivost v oblaku zagotavlja aplikacija ali programska oprema, ki se uporablja prek interneta. Ta vrsta storitev v oblaku odpravlja potrebo končnega uporabnika po nakupu, namestitvi in upravljanju programske opreme. Njena prednost je, da je programska oprema z internetno povezavo dostopna od koder koli.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, „Elasticity in Cloud Computing: What It Is, and What It Is Not“ (Prožnost računalništva v oblaku: kaj to je in kaj to ni), na voljo na: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Glej tudi COM(2012) 529, str. 2–5.

Slika 5: Modeli storitev in sredstva pri računalništvu v oblaku



Agencija ENISA je pripravila celovite smernice o posameznih temah na področju računalništva v oblaku[36] ter smernice o osnovah računalništva v oblaku[37].

4.4.2 Varnostne zahteve

V skladu s členom 16(1) morajo države članice zagotoviti, da ponudniki digitalnih storitev sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih podjetja uporabljajo pri opravljanju svojih storitev. Navedeni varnostni ukrepi bi morali upoštevati najnovejši tehnični razvoj in naslednjih pet elementov: i) varnost sistemov in infrastrukture, ii) obvladovanje incidentov, iii) upravljanje neprekinjenega poslovanja, iv) spremljanje, revidiranje in preskušanje, v) skladnost z mednarodnimi standardi.

V zvezi s tem je Komisija na podlagi člena 16(8) pooblaščena za sprejetje izvedbenih aktov, ki natančneje določajo navedene elemente in zagotavljajo visoko stopnjo harmonizacije za te ponudnike storitev. Komisija naj bi zadevni izvedbeni akt sprejela jeseni 2017. Poleg tega morajo države članice zagotoviti, da ponudniki digitalnih storitev sprejmejo potrebne ukrepe za preprečitev in zmanjšanje vpliva incidentov, in sicer z namenom neprekinjenega zagotavljanja storitev.

4.4.3 Zahteve glede priglasitve

Od ponudnikov digitalnih storitev bi bilo treba zahtevati, da resne incidente priglasijo pristojnim organom ali skupinam CSIRT. V skladu s členom 16(3) direktive o varnosti omrežij in informacij zahteva glede priglasitve za ponudnike digitalnih storitev velja, kadar

[36] Na voljo na: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security.
[37] ENISA, *Cloud Security Guide for SMEs* (Vodnik o varnosti storitev v oblaku za mala in srednja podjetja) (2015). Na voljo na: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

ima varnostni incident znaten vpliv na zagotavljanje storitve. V členu 16(4) je za določanje stopnje vpliva incidenta navedenih pet parametrov, ki jih morajo upoštevati ponudniki digitalnih storitev. V zvezi s tem je Komisija v skladu s členom 16(8) pooblaščena za sprejetje izvedbenih aktov s podrobnejšimi opisi parametrov. Natančnejša določitev navedenih parametrov bo del izvedbenega akta, ki bo določal varnostne elemente iz točke 4.4.2 in ki ga Komisija namerava sprejeti jeseni.

4.4.4 Regulativni pristop na podlagi tveganja

V členu 17 je določeno, da pristojni nacionalni organi pri ponudnikih digitalnih storitev izvajajo naknadno nadzorno kontrolo. Države članice morajo zagotoviti, da pristojni organi ukrepajo, kadar se jim predložijo dokazi, da ponudnik digitalnih storitev ne izpolnjuje zahtev iz člena 16 Direktive.

Poleg tega je Komisija na podlagi člena 16(8) in (9) pooblaščena za sprejetje izvedbenih aktov v zvezi z zahtevami glede priglasitve in varnostnimi zahtevami, ki bodo povečali harmonizacijo za ponudnike digitalnih storitev. Države članice na podlagi člena 16(10) za ponudnike digitalnih storitev ne smejo uvesti nikakršnih nadaljnjih varnostnih zahtev ali zahtev glede priglasitve poleg tistih, ki so določene v Direktivi, razen kadar so taki ukrepi potrebni za zaščito njihovih temeljnih državnih funkcij, zlasti za zaščito nacionalne varnosti, ter za omogočanje preiskovanja, odkrivanja in pregona kaznivih dejanj.

In končno Direktiva ob upoštevanju čezmejne narave ponudnikov digitalnih storitev ne sledi modelu več vzporednih pristojnosti, ampak pristopu, ki temelji na kriteriju glavnega sedeža podjetja v EU[38]. Ta pristop omogoča, da se za ponudnike digitalnih storitev uporablja le en sklop pravil, za nadzor pa je odgovoren le en pristojni organ; to je zlasti pomembno, ker veliko ponudnikov digitalnih storitev svoje storitve hkrati ponuja v številnih državah članicah. Z uporabo tega pristopa se čim bolj zmanjšuje breme zagotavljanja skladnosti za ponudnike digitalnih storitev in zagotavlja pravilno delovanje enotnega digitalnega trga.

4.4.5 Pristojnost

Kot je razloženo zgoraj, ima na podlagi člena 18(1) direktive o varnosti omrežij in informacij pristojnost nad ponudnikom digitalnih storitev država članica, v kateri ima podjetje glavni sedež. Ponudnik digitalnih storitev, ki v EU zagotavlja storitve, vendar na ozemlju EU nima sedeža, mora v skladu s členom 18(2) določiti predstavnika v Uniji. V tem primeru je za podjetje pristojna država članica, v kateri ima sedež predstavnik. Kadar ponudnik digitalnih storitev zagotavlja storitve v državi članici, vendar v EU ni določil predstavnika, lahko država članica načeloma sproži postopek proti ponudniku digitalnih storitev, saj ponudnik krši svoje obveznosti, ki izhajajo iz Direktive.

[38] Glej zlasti člen 18 Direktive.

4.4.6 Izvzetje ponudnikov digitalnih storitev omejenega obsega s področja uporabe varnostnih zahtev in zahtev glede priglasitve

Ponudniki digitalnih storitev, ki so mikropodjetja ali mala podjetja v smislu Priporočila Komisije 2003/361/ES39, so v skladu s členom 16(11) izvzeti s področja uporabe varnostnih zahtev in zahtev glede priglasitve iz člena 16. To pomeni, da podjetij z manj kot 50 zaposlenimi ter z letnim prometom in/ali letno bilančno vsoto, ki ne presega 10 milijonov EUR, take zahteve ne zavezujejo. Pri ugotavljanju velikosti podjetja ni pomembno, ali zadevno podjetje zagotavlja le digitalne storitve v smislu direktive o varnosti omrežij in informacij ali tudi druge storitve.

5. Razmerje med direktivo o varnosti omrežij in informacij ter drugo zakonodajo

Ta oddelek se osredotoča na določbe o *lex specialis* iz člena 1(7) direktive o varnosti omrežij in informacij ter orisuje tri primere *lex specialis*, ki jih je Komisija ocenila doslej, in pojasnjuje varnostne zahteve in zahteve glede priglasitve, ki veljajo za ponudnike telekomunikacijskih storitev in storitev zaupanja.

5.1 Člen 1(7) direktive o varnosti omrežij in informacij: določbe o *lex specialis*

V skladu s členom 1(7) direktive o varnosti omrežij in informacij se določbe o varnostnih zahtevah in/ali zahtevah glede priglasitve za ponudnike digitalnih storitev ali izvajalce bistvenih storitev v okviru Direktive ne uporabljajo, kadar sektorska zakonodaja EU določa varnostne zahteve in/ali zahteve glede priglasitve, ki so po učinku vsaj enakovredne ustreznim obveznostim iz direktive o varnosti omrežij in informacij. Države članice morajo člen 1(7) upoštevati pri celotnem prenosu Direktive in Komisiji predložiti informacije o uporabi določb o *lex specialis*.

Metodologija

Pri ocenjevanju enakovrednosti sektorskega zakonodajnega akta EU z ustreznimi določbami direktive o varnosti omrežij in informacij bi bilo treba posebno pozornost nameniti vprašanju, ali varnostne obveznosti v sektorski zakonodaji vsebujejo ukrepe, ki zagotavljajo varnost omrežij in informacijskih sistemov, kot je opredeljena v členu 4(2) Direktive.

V zvezi z zahtevo glede priglasitve člen 14(3) in člen 16(3) direktive o varnosti omrežij in informacij določata, da morajo izvajalci bistvenih storitev in ponudniki digitalnih storitev pristojnemu organu ali skupini CSIRT brez nepotrebnega odlašanja priglasiti incidente z bistvenim/znatnim vplivom na zagotavljanje storitve. Tu je treba posebno pozornost nameniti obveznostim izvajalca/ponudnika digitalnih storitev, da v priglasitev vključi informacije, ki pristojnemu organu ali skupini CSIRT omogočajo, da ugotovijo čezmejni vpliv varnostnega incidenta.

[39] UL L 24, 20.5.2003, str. 36.

Trenutno ni sektorske zakonodaje za kategorijo ponudnikov digitalnih storitev, ki bi določala varnostne zahteve in zahteve glede priglasitve, ki bi bile primerljive s tistimi iz člena 16 direktive o varnosti omrežij in informacij in bi jih bilo treba upoštevati pri uporabi člena 1(7) direktive o varnosti omrežij in informacij[40].

Kar zadeva izvajalce bistvenih storitev varnostne zahteve in/ali zahteve glede priglasitve iz sektorske zakonodaje EU veljajo za finančni sektor ter zlasti sektorja bančništva in infrastrukture finančnega trga iz točk 3 in 4 Priloge II. Razlog za to je, da sta varnost in solidnost informacijskih tehnologij ter omrežij in informacijskih sistemov, ki jih uporabljajo finančne institucije, bistveni del zahtev za operativno tveganje, ki jih zakonodaja EU nalaga finančnim institucijam.

Primeri

i) Direktiva o plačilnih storitvah 2

V zvezi z bančnim sektorjem in zlasti kar zadeva zagotavljanje plačilnih storitev s strani kreditnih institucij, kot so opredeljene v členu 4(1) Uredbe (EU) št. 575/2013, t. i. direktiva o plačilnih storitvah 2[41] v členu 95 oz. členu 96 določa varnostne zahteve in zahteve glede priglasitve.

Natančneje, člen 95(1) od ponudnikov plačilnih storitev zahteva, da sprejmejo ustrezne ukrepe za zmanjšanje tveganj in nadzorne mehanizme za obvladovanje operativnih in varnostnih tveganj, povezanih s plačilnimi storitvami, ki jih opravljajo. Ti ukrepi naj bi vključevali vzpostavitev in vzdrževanje učinkovitih postopkov za obvladovanje incidentov, tudi za odkrivanje in razvrstitev večjih operativnih in varnostnih incidentov. V uvodnih izjavah 95 in 96 direktive o plačilnih storitvah 2 je narava teh varnostnih ukrepov nadalje pojasnjena. Iz teh določb je razvidno, da si predpisani ukrepi prizadevajo za obvladovanje varnostnih tveganj v zvezi z omrežji in informacijskimi sistemi, ki se uporabljajo pri zagotavljanju plačilnih storitev. Zato se lahko navedene varnostne zahteve štejejo po učinku za vsaj enakovredne ustrezni določbi iz člena 14(1) in (2) direktive o varnosti omrežij in informacij.

V zvezi z zahtevami glede priglasitve člen 96(1) direktive o plačilnih storitvah 2 določa obveznost ponudnikov plačilnih storitev, da pristojni organ brez nepotrebnega odlašanja obvestijo o resnih varnostnih incidentih. Poleg tega člen 96(2) direktive o plačilnih storitvah 2 podobno kot člen 14(5) direktive o varnosti omrežij in informacij od pristojnega organa zahteva, da obvesti pristojne organe drugih držav članic, če je incident pomemben za njih. Ta obveznost hkrati pomeni, da mora poročilo o varnostnih incidentih vključevati informacije, ki organom omogočajo oceno čezmejnega vpliva incidenta. Člen 96(3)(a) direktive o plačilnih

[40] To ne posega v priglasitev kršitve varstva osebnih podatkov nadzornemu organu iz člena 33 Splošne uredbe o varstvu podatkov.
[41] Direktiva (EU) 2015/2366, UL L 337, 23.12.2015, str. 35.

storitvah 2 v zvezi s tem pooblašča EBA, da v sodelovanju z ECB pripravi smernice o natančni vsebini in obliki priglasitev.

Na podlagi tega se lahko zaključi, da bi se morale na podlagi člena 1(7) direktive o varnosti omrežij in informacij pri zagotavljanju plačilnih storitev s strani kreditnih institucij uporabljati varnostne zahteve in zahteve glede priglasitve iz člena 95 oziroma člena 96 direktive o plačilnih storitvah 2 in ne ustrezne določbe iz člena 14 direktive o varnosti omrežij in informacij.

ii) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov

V zvezi z infrastrukturo finančnega trga Uredba (EU) št. 648/2012 v povezavi z Izvedbeno uredbo Komisije (EU) št. 153/2013 vsebuje določbe o varnostnih zahtevah za centralne nasprotne stranke, kar se lahko šteje za *lex specialis.* Zlasti zakonodajna akta določata tehnične in organizacijske ukrepe v zvezi z varnostjo omrežij in informacijskih sistemov, ki so še podrobnejši, kot to zahteva člen 14(1) in (2) direktive o varnosti omrežij in informacij, zato se lahko šteje, da izpolnjujeta zahteve iz člena 1(7) direktive o varnosti omrežij in informacij, kar zadeva varnostne zahteve.

Natančneje, člen 26(1) Uredbe (EU) št. 648/2012 določa, da bi moral imeti subjekt „zanesljivo ureditev upravljanja, ki vključuje jasno organizacijsko strukturo z natančno opredeljenimi, preglednimi in doslednimi odgovornostmi, učinkovitimi postopki za ugotavljanje, upravljanje in spremljanje tveganj, ki jim je ali bi jim lahko bila izpostavljena, in poročanje o njih ter primerne mehanizme za notranjo kontrolo, vključno z zanesljivimi upravnimi in računovodskimi postopki.“ Člen 26(3) zahteva, da mora organizacijska struktura z uporabo ustreznih in sorazmernih sistemov, virov in postopkov zagotavljati neprekinjeno in pravilno delovanje storitev in dejavnosti.

Poleg tega je člen 26(6) pojasnjuje, da mora centralna nasprotna stranka vzdrževati „sisteme informacijske tehnologije, ki ustrezajo zapletenosti, raznolikosti ter vrsti storitev in dejavnosti, ki jih opravlja, da se zagotovijo visoki standardi varnosti, celovitosti in zaupnosti informacij“. Člen 34(1) določa sprejetje, uveljavitev in vzdrževanje ustrezne politike neprekinjenega poslovanja in načrta ponovne vzpostavitve delovanja, s katerim bo zagotovljena pravočasna ponovna vzpostavitev delovanja.

Te obveznosti nadalje določa Delegirana uredba Komisije (EU) št. 153/2013 z dne 19. decembra 2012 o dopolnitvi Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi glede zahtev za centralne nasprotne stranke[42]. Zlasti člen 4 navedene delegirane uredbe določa obveznost, da se razvijejo ustrezna orodja za upravljanje tveganj, ki bi omogočila upravljanje in poročanje o vseh pomembnih tveganjih, ter podrobneje določa vrsto ukrepov (npr.: uporabo zanesljivih informacij in sistemov nadzora tveganj, razpoložljivost sredstev, strokovnega znanja in dostop do vseh ustreznih informacij

[42] UL L 52, 23.2.2013, str. 41.

za funkcijo upravljanja tveganj, razpoložljivost ustreznih mehanizmov notranjega nadzora, kot so zanesljivi upravni in računovodski postopki, ki pomagajo organu upravljanja centralnih nasprotnih strank pri spremljanju in ocenjevanju ustreznosti in učinkovitosti njihovih politik, postopkov in sistemov za upravljanje tveganj.

Poleg tega se člen 9 izrecno sklicuje na varnost sistemov informacijske tehnologije in določa konkretne tehnične in organizacijske ukrepe v zvezi z vzdrževanjem zanesljivega okvira za informacijsko varnost, s katerim upravlja tveganja na področju varnosti informacijskih tehnologij. Taki ukrepi bi morali vključevati mehanizme in postopke, ki bi zagotavljali razpoložljivost storitev in zaščito avtentičnosti, celovitosti in zaupnosti podatkov.

iii) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU[43].

V zvezi z mesti trgovanja člen 48(1) Direktive 2014/65/EU od upravljavcev zahteva, da zagotovijo neprekinjenost storitev, če pride do okvare sistemov trgovanja. Ta splošna obveznost je bila nedavno podrobneje določena in dopolnjena z Delegirano uredbo Komisije (EU) 2017/584[44] z dne 14. julija 2016 o dopolnitvi Direktive 2014/65/EU Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo organizacijske zahteve za mesta trgovanja[45]. Zlasti člen 23(1) navedene uredbe določa, da mesta trgovanja vzpostavijo postopke in ureditve za fizično in elektronsko varnost, zasnovane za zaščito njihovih sistemov pred zlorabo ali nepooblaščenim dostopom ter za zagotavljanje integritete podatkov. Ti ukrepi bi morali omogočiti preprečevanje ali zmanjševanje tveganj napadov na informacijske sisteme.

Člen 23(2) nadalje zahteva, da ukrepi in ureditve, ki jih sprejmejo upravljavci, omogočajo hitro odkritje in upravljanje tveganj, ki se nanašajo na kakršen koli nepooblaščen dostop, motnje sistema, ki resno ovirajo ali prekinejo delovanje informacijskih sistemov, in motnje podatkov, ki ogrozijo razpoložljivost, integriteto ali avtentičnost podatkov. Poleg tega člen 15 Uredbe mestom trgovanja nalaga obveznost, da razpolagajo z učinkovitimi ureditvami neprekinjenega poslovanja, namenjenimi zagotavljanju zadostne stabilnosti sistema in odpravljanju motenj. Ti ukrepi bi zlasti morali omogočiti upravljavcu, da lahko trgovanje ponovno vzpostavi v dveh urah ali približno dveh urah in zagotovi, da je količina izgubljenih podatkov blizu nič.

Člen 16 nadalje določa, da bi morali biti opredeljeni ukrepi za odpravljanje in upravljanje motenj del načrta neprekinjenega poslovanja mest trgovanja, in posamezne elemente, ki jih mora pri sprejemanju načrta neprekinjenega poslovanja upoštevati upravljavec (npr. ustanovitev posebne skupine za varnostne operacije, izvajanje redno pregledane ocene učinka, ki opredeljuje tveganja).

[43] UL L 173, 12.6.2014, str. 349.
[44] UL L 87, 31.3.2017, str. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf.

Glede na vsebino teh varnostnih ukrepov se zdi, da so namenjeni upravljanju in odpravljanju tveganj v zvezi z razpoložljivostjo, avtentičnostjo, celovitostjo in zaupnostjo podatkov ali zagotovljenih storitev, in posledično se lahko zaključi, da navedena sektorska zakonodaja EU vsebuje varnostne obveznosti, ki so po učinku vsaj enakovredne ustreznim obveznostim iz člena 14(1) in (2) direktive o varnosti omrežij in informacij.

5.2 Člen 1(3) direktive o varnosti omrežij in informacij: ponudniki telekomunikacijskih storitev in ponudniki storitev zaupanja

V skladu s členom 1(3) se varnostne zahteve in zahteve glede priglasitve iz Direktive ne uporabljajo za izvajalce, za katera veljajo zahteve iz členov 13a in 13b Direktive 2002/21/ES. Člena 13a in 13b Direktive 2002/21/ES se uporabljata za podjetja, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve. Zato mora podjetje, kar zadeva zagotavljanje javnih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, spoštovati varnostne zahteve in zahteve glede priglasitve iz Direktive 2002/21/ES.

Vendar če isto podjetje zagotavlja tudi druge storitve, kot so digitalne storitve (npr. računalništvo v oblaku ali spletne tržnice) iz Priloge III k direktivi o varnosti omrežij in informacij, ali storitve, kot so sistemi domenskih imen ali stičišče omrežij iz točke 7 Priloge II k direktivi o varnosti omrežij in informacij, bodo za podjetje pri zagotavljanju teh storitev veljale varnostne zahteve in zahteve glede priglasitve iz direktive o varnosti omrežij in informacij. Treba je opozoriti, da ponudniki storitev iz točke 7 Priloge II sodijo v kategorijo izvajalcev bistvenih storitev in zato morajo države članice izvesti postopek določitve v skladu s členom 5(2) in določiti, kateri posamezni ponudniki storitev sistema domenskih imen, stičišča omrežij ali domenskih imen najvišje ravni bi morali izpolnjevati zahteve iz direktive o varnosti omrežij in informacij. To pomeni, da bo po taki oceni obveznost izpolnjevanja zahtev iz direktive o varnosti omrežij in informacij veljala samo za tiste ponudnike sistema domenskih imen, stičišča omrežij ali domenskih imen najvišje ravni, ki izpolnjujejo merila iz člena 5(2) direktive o varnosti omrežij in informacij.

Člen 1(3) nadalje določa, da se varnostne zahteve in zahteve glede priglasitve iz Direktive ne uporabljajo niti za ponudnike storitev zaupanja, za katere se uporabljajo podobne zahteve iz člena 19 Uredbe (EU) št. 910/2014.

6. Objavljeni dokumenti z nacionalnimi strategijami za kibernetsko varnost

	Država članica	Naslov strategije in razpoložljive povezave
1	Avstrija	*Austrian Cybersecurity Strategy* (Avstrijska strategija za kibernetsko varnost) (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgija	*Securing Cyberspace* (Zavarovanje kibernetskega prostora) (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bolgarija	*Cyber Resilient Bulgaria 2020* (Na kibernetske grožnje odporna Bolgarija 2020) (2016) http://www.cyberbg.eu/ (BG)
4	Hrvaška	*The national cyber security strategy of the republic of Croatia* (Nacionalna strategija Republike Hrvaške za kibernetsko varnost) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Češka	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (Nacionalna strategija Češke republike za kibernetsko varnost za obdobje 2015–2020) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Ciper	*Cybersecurity Strategy of the Republic of Cyprus* (Strategija Republike Ciper za kibernetsko varnost) (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Danska	*The Danish Cyber and Information Security Strategy* (Danska strategija za kibernetsko in informacijsko varnost) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estonija	*Cyber Security Strategy* (Strategija za kibernetsko varnost) (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finska	*Finland´s Cyber security Strategy* (Strategija Finske za kibernetsko varnost) (2013)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Francija	*French national digital security strategy* (Francoska nacionalna strategija za digitalno varnost) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irska	*National Cyber Security Strategy 2015-2017* (Nacionalna strategija za kibernetsko varnost za obdobje 2015–2017) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italija	*National Strategic Framework for Cyberspace Security* (Nacionalni strateški okvir za varnost v kibernetskem prostoru) (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Nemčija	*Cyber-Sicherheitsstrategie für Deutschland* (Strategija za kibernetsko varnost za Nemčijo) (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Madžarska	*National Cyber Security Strategy of Hungary* (Nacionalna strategija Madžarske za kibernetsko varnost) (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Latvija	*Cyber Security Strategy of Latvia 2014–2018* (Strategija Latvije za kibernetsko varnost za obdobje 2014–2018) (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Litva	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (Program za razvoj varnosti elektronskih informacij (kibernetske varnosti) za obdobje 2011–2019) (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luksemburg	*National Cybersecurity Strategy II* (Nacionalna strategija za kibernetsko varnost II) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (Zelena knjiga o nacionalni strategiji za kibernetsko varnost) (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Nizozemska	*National Cyber Security Strategy 2* (Nacionalna strategija za kibernetsko varnost 2) (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Poljska	*Cyberspace Protection Policy of the Republic of Poland* (Politika Republike Poljske za zaščito kibernetskega prostora) (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Romunija	*Strategia de securitate cibernetică a României* (Strategija Romunije za kibernetsko varnost) (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugalska	*National Cyberspace Security Strategy* (Nacionalna strategija za varnost v kibernetskem prostoru) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Slovaška republika	*Cyber Security Concept of the Slovak Republic for 2015–2020* (Zasnova Slovaške republike za kibernetsko varnost za obdobje 2015–2020) (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovenija	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (Strategija za kibernetsko varnost, ki vzpostavlja sistem za zagotavljanje visoke ravni kibernetske varnosti) (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Španija	*National Cyber Security Strategy* (Nacionalna strategija za kibernetsko varnost) (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Švedska	*The Swedish National Cybersecurity Strategy* (Švedska nacionalna strategija za kibernetsko varnost) (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Združeno	*National Cyber Security Strategy (2016-2021)* (Nacionalna strategija

kraljestvo	za kibernetsko varnost (2016–2021)) (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Seznam dobrih praks in priporočil agencije ENISA

Za odzivanje na incidente

- ✓ Strategije za odzivanje na incidente in sodelovanje pri kibernetskih krizah[46]

Za obvladovanje incidentov

- ✓ Projekt avtomatizacije obvladovanja incidentov[47]
- ✓ Vodnik po dobrih praksah za upravljanje incidentov[48]

Za razvrščanje incidentov in njihova taksonomija

- ✓ Pregled obstoječih taksonomij[49]
- ✓ Vodnik po dobrih praksah uporabe taksonomij pri preprečevanju in odkrivanju incidentov[50]

Za zrelost skupin CSIRT

- ✓ Izzivi za nacionalne skupine CSIRT v Evropi leta 2016: študija o zrelosti skupin CSIRT[51]
- ✓ Študija o zrelosti skupin CSIRT – postopek ocenjevanja[52]
- ✓ Smernice za nacionalne in vladne skupine CSIRT o načinu ocenjevanja zrelosti[53]

Za krepitev zmogljivosti in usposabljanje skupin CSIRT

- ✓ Vodnik po dobrih praksah pri metodologijah usposabljanja[54]

Za več informacij o obstoječih skupinah CSIRT v Evropi – Pregled skupin CSIRT po državah[55]

---

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (Strategije za odzivanje na incidente in sodelovanje pri kibernetskih krizah) (2016). Na voljo na:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation.

[47] Več informacij je na voljo na: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation.

[48] ENISA, *Good Practice Guide for Incident Management* (Vodnik po dobrih praksah za upravljanje incidentov) (2010). Na voljo na:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[49] Več informacij je na voljo na: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies.

[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (Vodnik po dobrih praksah uporabe taksonomij pri preprečevanju in odkrivanju incidentov) (2017). Na voljo na:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection.

[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (Izzivi za nacionalne skupine CSIRT v Evropi leta 2016: študija o zrelosti skupin CSIRT) (2017). Na voljo na:https://www.enisa.europa.eu/publications/study-on-csirt-maturity.

[52] *Study on CSIRT Maturity – Evaluation Process* (Študija o zrelosti skupin CSIRT – postopek ocenjevanja) (2017). Na voljo na:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process.

[53] ENISA, *CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs* (Zmogljivosti skupin CSIRT. Kako ocenjevati zrelost? Smernice za nacionalne in vladne skupine CSIRT) (2016). Na voljo na: https://www.enisa.europa.eu/publications/csirt-capabilities.

[54] ENISA, *Good Practice Guide on Training Methodologies* (Vodnik po dobrih praksah pri metodologijah usposabljanja) (2014). Na voljo na:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.

[55] Več informacij je na voljo na: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.