REPUBLIKA SLOVENIJA

STRATEGIJA KIBERNETSKE VARNOSTI

VZPOSTAVITEV SISTEMA ZAGOTAVLJANJA VISOKEGA NIVOJA KIBERNETSKE VARNOSTI

DIGITALNA SLOVENIJA

Informacije o dokumentu

Naslov dokumenta	Strategija kibernetske varnosti
Datum dokumenta	Februar 2016
Sodelujoči pri pripravi dokumenta	• Agencija za energijo, • Agencija za komunikacijska omrežja in storitve, • Ministrstvo za finance, • Ministrstvo za gospodarski razvoj in tehnologijo, • Ministrstvo za infrastrukturo, • Ministrstvo za izobraževanje, znanost in šport, • Ministrstvo za javno upravo, • Ministrstvo za notranje zadeve – Policija, • Ministrstvo za notranje zadeve, • Ministrstvo za obrambo, • Ministrstvo za zdravje, • Ministrstvo za zunanje zadeve, • Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT), • Slovenska obveščevalno-varnostna agencija, • Svet za nacionalno varnost, • Urad za varovanje tajnih podatkov.

Kazalo

1 Uvod ... 3

2 Analiza obstoječega stanja ... 4

3 Vizija strategije ... 6

4 Tveganja kibernetskega prostora ... 6

4.1 Tehnološki razvoj ... 7

4.2 Internet ... 7

4.3 Kibernetski kriminal ... 7

4.4 Obveščevalna dejavnost ... 8

4.5 Spreminjanje varnostnega okolja ... 8

4.6 Vdori v zasebnost ... 8

5 Opredelitev deležnikov ... 8

6 Vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti in jasne strukture upravljanja ... 9

7 Področja udejanjanja strategije ... 10

7.1 Preprečevanje ... 10

7.2 Odzivanje ... 10

7.3 Ozaveščanje ... 11

8 Cilji strategije in ukrepi za njihovo doseganje ... 11

8.1 Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti ... 12

8.2 Varnost državljanov v kibernetskem prostoru ... 13

8.3 Kibernetska varnost v gospodarstvu ... 14

8.4 Zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore ... 14

8.5 Zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala ... 15

8.6 Razvoj obrambnih kibernetskih zmogljivosti ... 15

8.7 Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah ... 16

8.8 Krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem ... 16

9 Tveganja za udejanjanje strategije ... 17

A Seznam kratic ... 18

Namen in povzetek

S pomočjo strategije kibernetske varnosti bo Slovenija okrepila svoj sistem zagotavljanja kibernetske varnosti, hkrati pa to področje tudi sistemsko uredila. Okrepitev celotnega sistema je nujna zaradi vedno večjega pomena kibernetske varnosti za nemoteno delovanje sistemov, od katerih je odvisno delovanje celotne družbe. Prav tako državo k temu spodbujajo in hkrati zavezujejo nacionalni in mednarodni strateški dokumenti. Učinkovit sistem zagotavljanja kibernetske varnosti ni in ne more biti poceni, vendar je neprimerljivo cenejši, kot bi bilo odpravljanje posledic, ki bi lahko nastale ob varnostnih incidentih, če takega sistema ne bi bilo.

Strategija vsebuje pregled obstoječega stanja na področjih, pomembnih za zagotavljanje kibernetske varnosti, opredeljuje vizijo ter zastavlja cilje. Prav tako opredeljuje področja, na katerih se bo udejanjala, in tveganja, ki nastopajo v kibernetskem prostoru. Strategija predlaga način, kako naj bo sistem zagotavljanja kibernetske varnosti organiziran, in potrebne ukrepe za uresničitev zastavljenih ciljev.

1 Uvod

V sodobnem svetu se uporaba informacijskih sistemov in omrežij vseskozi povečuje, zato se povečuje tudi pomen, ki ga imajo ti sistemi za uspešen razvoj gospodarskih in negospodarskih dejavnosti ter življenje in blaginjo celotne družbe. Varnost omrežij in informacij prispeva h krepitvi pomembnih vrednot in ciljev v družbi, kot so človekove pravice in temeljne svoboščine, demokracija, pravna država ter gospodarska in politična stabilnost.

Vedno hitrejši razvoj informacijsko-komunikacijskih tehnologij po eni strani prinaša koristi za moderno družbo, po drugi strani pa vpliva na pojav vedno novih in tehnološko vse bolj dovršenih kibernetskih groženj. Vse izrazitejši je trend uporabe informacijsko-komunikacijskih tehnologij za politično, gospodarsko in vojaško prevlado. Nedvomno so prav kibernetski napadi ena izmed najpomembnejših varnostnih groženj sodobnemu svetu, kar je pripomoglo k temu, da je kibernetska varnost že pred časom postala pomemben integralni del nacionalne varnosti držav.

H krepitvi sistema za zagotavljanje kibernetske varnosti državo spodbujajo in hkrati zavezujejo sprejeti strateški dokumenti na nacionalni in mednarodni ravni. O tem govorijo Resolucija o strategiji nacionalne varnosti Republike Slovenije[1], Strategija kibernetske varnosti Evropske unije »Odprt, varen in zavarovan kibernetski prostor«[2] ter predlog Direktive o ukrepih za zagotovitev visoke skupne stopnje varnosti omrežij in informacij v Uniji[3].

S to strategijo bo Slovenija opredelila ukrepe za vzpostavitev nacionalnega sistema kibernetske varnosti, ki bo sposoben hitrega odzivanja na varnostne grožnje in bo predstavljal učinkovito zaščito informacijsko-komunikacijske infrastrukture in informacijskih sistemov, s čimer se bo zagotavljalo neprekinjeno delovanje tako javnega kot zasebnega sektorja, predvsem pa ključnih funkcij države in družbe v vseh varnostnih razmerah. Zagotavljanje varnosti kibernetskega prostora[4] bo uravnoteženo med interesi zagotavljanja varnosti in ekonomske upravičenosti ter človekovimi pravicami in temeljnimi svoboščinami.

[1] Resolucija o strategiji nacionalne varnosti Republike Slovenije. V: Uradni list RS [online], 2010, št. 27/2010, točka 5.3.5 Odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov. Dostopno na: https://www.uradni-list.si/1/content? id=97018.

[2] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Digital Agenda for Europe - A Europe 2020 Initiative [online], 2013. Dostopno na: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[3] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. Digital Agenda for Europe - A Europe 2020 Initiative [online], 2013. Dostopno na: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[4] Izraz kibernetski prostor (ang. Cyberspace) predstavlja globalno omrežje informacijske tehnologije, telekomunikacijskih omrežij in sistemov za računalniško obdelavo.

DEFINICIJA KIBERNETSKE VARNOSTI[5]

Kibernetska varnost je v splošnem smislu opredeljena kot:

- skupek aktivnosti in drugih ukrepov, tehničnih in ne-tehničnih, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih le-ta vsebuje in obravnava, kar vključuje programsko opremo in podatke kot tudi druge elemente kibernetskega prostora, pred vsemi grožnjami, vključno z grožnjami nacionalni varnosti;
- stopnja zaščite, ki jo aktivnosti in ukrepi lahko zagotovijo;
- združena področja profesionalnih naporov, vključno z raziskavami in razvojem na področju implementiranja in izboljševanja ukrepov ter dvigovanja kakovosti le-teh.

2 Analiza obstoječega stanja

V Sloveniji je bilo v preteklosti že pripravljenih nekaj predlogov sistemske ureditve področja kibernetske varnosti, vendar do izvedbe nikoli ni prišlo. Kljub temu je prevladalo spoznanje, da država potrebuje strategijo kibernetske varnosti, ki bo združila in usmerila prizadevanja vseh deležnikov za okrepitev in sistemsko ureditev tega pomembnega področja.

Trenutno so operativne zmogljivosti za odzivanje na kibernetske grožnje porazdeljene v SI-CERT[6] kot nacionalnem odzivnem centru za omrežne incidente, v Sektorju za informacijsko varnost v okviru Direktorata za informatiko na Ministrstvu za javno upravo, na Ministrstvu za obrambo za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami, v SOVA na področju protiobveščevalnega delovanja ter na Policiji, v Uradu za informatiko in telekomunikacije in Upravi kriminalistične policije, predvsem v Centru za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala. Razen Policije, ki je v zadnjih petih letih izboljšala svoje kapacitete za preiskovanje in preprečevanje kibernetske kriminalitete, so drugi organi podhranjeni na kadrovskem, materialno-tehničnem in organizacijskem področju. Kljub pomanjkljivostim, zmogljivosti na operativni ravni obstajajo, ne obstaja pa koordinacijsko telo, ki bi na strateški ravni povezovalo navedene deležnike.

[5]Dunn, M. A Comparative Analysis of Cybersecurity Initiatives Worldwide. V: ITU WSIS Thematic Meeting on Cybersecurity [online], 2005, str. 4. Dostopno na: https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.

[6]SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij, ki od leta 1995 deluje v okviru javnega zavoda Arnes. Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah v elektronskih omrežjih. Trenutno opravlja tudi naloge vladnega centra za odzivanje na omrežne incidente (SIGOV-CERT) in pomaga pri vzpostavitvi samostojnega centra, ki bo skrbel za zaščito informacijske infrastrukture državne uprave. SI-CERT je član svetovnega združenja odzivnih in varnostnih centrov FIRST (Forum of Incident Response and Security Teams), član skupine nacionalnih odzivnih centrov pri CERT/CC, član delovne skupine evropskih odzivnih centrov TF-CSIRT in je akreditiran v programu Trusted Introducer. SI-CERT je slovenska kontaktna točka za Varnostni organ Generalnega sekretariata Sveta EU in nacionalna informacijska točka za program IMPACT mednarodne telekomunikacijske zveze ITU.

Po podatkih SI-CERT[7] je bilo leta 2014 v Sloveniji obravnavanih 2060 incidentov, kar je skoraj 6,4-kratno povečanje glede na leto 2008. Naraščajoči trend glede na zgoraj omenjeno podhranjenost sistema zagotavljanja kibernetske varnosti vzbuja skrb.

Sodelovanje deležnikov pri zagotavljanju kibernetske varnosti ni formalizirano, ampak predvsem med odzivnimi centri poteka neformalno, razen kadar za to obstaja pravna podlaga[8]. Pri tem gre za obveščanje o incidentih in pomoč pri njihovem reševanju, izmenjavo izkušenj ali pa uporabo obstoječih zmogljivosti. Priložnost za vzpostavitev sodelovanja so med drugim skupna sodelovanja pri izvedbi mednarodnih vaj iz kibernetske varnosti, ki jih organizira Agencija EU za varnost omrežij in informacij (ENISA)[9]. Tako je bilo v preteklosti sodelovanje že vzpostavljeno z nekaterimi bankami, telekomunikacijskimi ponudniki in distributerji električne energije.

Na področju ozaveščanja potekata dva projekta. SI-CERT od leta 2011 izvaja nacionalni program ozaveščanja in izobraževanja Varni na internetu[10]. Projekt, ki je namenjen najširši slovenski javnosti, poseben sklop vsebin pa tudi malim podjetjem, obrtnikom in samostojnim podjetnikom, si za ključen cilj zastavlja dvig stopnje informiranosti o varni rabi interneta. Projekt, ki ga financira Ministrstvo za izobraževanje, znanost in šport, sodeluje tudi v kampanjah evropskega meseca kibernetske varnosti.

V okviru Centra za varnejši internet, ki ga vodi konzorcij, sestavljen iz Fakultete za družbene vede Univerze v Ljubljani, Arnes, Zveze prijateljev mladine Slovenije in Zavoda MISSS[11], financirata pa ga Generalni direktorat Connect pri Evropski komisiji in Ministrstvo za izobraževanje, znanost in šport, se izvajajo programi SAFE.SI[12], TOM telefon in Spletno oko. Program SAFE.SI deluje kot nacionalna točka ozaveščanja otrok in najstnikov o varni rabi interneta in mobilnih naprav. Program TOM telefon otrokom in mladostnikom med drugim svetuje tudi o varni rabi interneta in mobilnih naprav. Spletno oko pa je spletna prijavna točka, ki v partnerstvu s policijo, tožilstvom, Uradom varuha za človekove pravice, ponudniki internetnih storitev, javnimi ter drugimi zainteresiranimi vladnimi in nevladnimi organizacijami omogoča anonimno prijavo domnevno nezakonitega gradiva s spolnimi zlorabami otrok in sovražnega govora na spletu ter ozavešča o problematiki nezakonitih spletnih vsebin.

Na izobraževalnem področju je informacijska oziroma kibernetska varnost vključena v visokošolski študijski program »Informacijska varnost« na Fakulteti za varnostne vede Univerze v Mariboru, kot predmet je vključena v predmetnike študijskih programov na Fakulteti za računalništvo in informatiko ter Fakulteti za družbene vede Univerze v Ljubljani, Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, Fakulteti za vede o zdravju Univerze na Primorskem, Fakulteti za informacijske študije v Novem mestu in samostojnem visokošolskem zavodu GEA College, kot del predmeta korporativna varnost pa tudi na nekaterih drugih visokošolskih izobraževalnih ustanovah. Na osnovnošolski in srednješolski ravni predmet s tega področja ne obstaja.

---

[7]Podatki za leto 2014 in poročila za pretekla leta so dostopni na https://www.cert.si.

[8]Npr. Zakon o elektronskih komunikacijah v 81. členu določa postopek izmenjave informacij med AKOS in SI-CERT ob kršitvi varnosti ali celovitosti. Zakon o elektronskih komunikacijah. V: Uradni list RS [online], 2012, št. 109/2012, člen 81. Dostopno na: http://www.uradni-list.si/1/content?id=111442.

[9] European Union Agency for Network and Information Security (ENISA)

[10] https://www.varninainternetu.si/

[11] Mladinsko informativno svetovalno središče Slovenije.

[12] http://safe.si/

Skladno z možnostmi Slovenija sodeluje na mednarodnih vajah iz kibernetske varnosti. Na vajah Cyber Europe, ki jih organizira ENISA, je tako leta 2010 sodelovala kot opazovalka, v letih 2012 in 2014 pa tudi kot aktivna udeleženka. Prav tako od leta 2013 naprej aktivno sodeluje na vajah kibernetske obrambe Cyber Coalition v okviru zveze NATO. Sodelovanje na vajah se je izkazalo kot dobra priložnost za preverjanje zmogljivosti za zagotavljanje kibernetske varnosti na nacionalni ravni, mednarodno izmenjavo izkušenj in vzpostavitev novih povezav med deležniki. Do sedaj še ni bila izvedena nacionalna vaja iz kibernetske varnosti.

3 Vizija strategije

Vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti kot pomembnega integralnega dejavnika nacionalne varnosti bo prispevala k zagotovitvi odprtega, varnega in varovanega kibernetskega prostora, ki bo osnova za nemoteno delovanje infrastrukture, pomembne za delovanje državnih organov in gospodarstva, pa tudi za življenje vsakega posameznika.

Slovenija bo do leta 2020 vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in tudi odpravljal posledice varnostnih incidentov. Ta cilj obsega osem podciljev:

1. okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti;
2. varnost državljanov v kibernetskem prostoru;
3. kibernetska varnost v gospodarstvu;
4. zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore;
5. zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala;
6. razvoj obrambnih kibernetskih zmogljivosti;
7. zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah;
8. krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem.

4 Tveganja kibernetskega prostora

V sodobni družbi so tako rekoč vsa področja delovanja družbe odvisna od informacijsko-komunikacijskih sistemov, nadaljnji razvoj pa bo to odvisnost le še povečeval. Medsebojna povezanost sistemov pomeni, da ima ranljivost enega lahko posledice na delovanje ostalih. Zagotavljanje popolne varnosti pred kibernetskimi napadi, zlorabami, goljufijami, napakami človeške in tehnološke narave ter drugimi vplivi je nemogoče, zato je pri določanju prioritete posamezne grožnje treba uporabiti pristop, ki temelji na oceni tveganja.

V zadnjih letih [13] so zaznani rast števila varnostnih incidentov, naprednejši ciljani napadi, izpostavljenost informacijsko-komunikacijske infrastrukture ter njena zloraba za izvedbo

[13] Poročila SI-CERT o omrežni varnosti za leta 2011, 2012, 2013 in 2014. Dostopno na: https://www.cert.si.

porazdeljenih ohromitev storitve[14]. Posamezniki so izpostavljeni različnim spletnim goljufijam, poskusom zlorab elektronskih bančnih storitev in škodljivi programski kodi.

4.1 Tehnološki razvoj

Razvoj informacijsko-komunikacijskih tehnologij je izjemno hiter, kar sicer omogoča nove inovativne načine uporabe, nove poslovne modele in različne razvojne priložnosti, hkrati pa zahteva hitro prilagajanje zakonodajnega in drugih družbenih okvirov. Razvojne smernice nakazujejo uveljavljanje računalništva v oblaku, podatkovno vodenega gospodarstva oziroma masovnih podatkov, interneta stvari in na njih osnovanih inovativnih sodelovalnih poslovnih modelov, kjer so meje nadzora in odgovornosti za varovanje osebnih in ostalih podatkov zabrisane oziroma vsaj slabše opredeljene. Pri računalništvu v oblaku je poleg zagotavljanja varnosti in zasebnosti lahko problematična tudi kakovost zagotavljanja storitev, saj le-ta temelji na verigi medsebojnega zaupanja vseh deležnikov, ki sestavljajo računalniški oblak, in ne na oceni oblaka kot celote. Vseprisotna mobilna omrežja, internet stvari in masovni podatki bodo povečali izpostavljenost varnostnim tveganjem na različnih ravneh, ki jih ne bo mogoče rešiti brez sistemskega pristopa k obvladovanju tveganj in zagotavljanju ustrezno visokega nivoja kibernetske varnosti.

4.2 Internet

Zelo pomembno je dejstvo, da internet podpira delovanje informacijsko-komunikacijskih sistemov na številnih področjih, zato ga je treba temu ustrezno obravnavati in kot ključni podporni sistem zaščititi. Internet je izpostavljen tveganjem, ki jih povzroča človek, naravne in druge nesreče ter tehnične okvare. Posebno pozornost je treba posvetiti zakonodajno-normativnemu okviru, ki obravnava vprašanja, povezana z zaščito kritične infrastrukture sektorja informacijsko-komunikacijske podpore.

4.3 Kibernetski kriminal

Evropska agenda za varnost[15] navaja kibernetski kriminal kot eno od treh groženj za evropsko varnost. Z rastjo vsesplošne uporabe informacijsko-komunikacijskih tehnologij se povečuje tudi kibernetski kriminal, ki obsega širok spekter dejavnosti. Na eni strani vključuje kazniva dejanja, povezana z vdori v zasebnost posameznikov, krajo identitet, pridobivanjem informacij o posameznikih in pravnih osebah z namenom izsiljevanja, spletnimi goljufijami in prevarami, razširjanjem otroške pornografije, digitalnim piratstvom, gospodarskim vohunjenjem, pranjem denarja in ponarejanjem. Na drugi strani pa vključuje kazniva dejanja, povezana s poskusi oviranja delovanja interneta, ki obsegajo vse od množičnega pošiljanje neželene e-pošte in izvajanja porazdeljenih ohromitev storitve, do kibernetskega terorizma, ki lahko povzroči motnje v delovanju informacijsko-komunikacijske infrastrukture in informacijskih sistemov ter v nekaterih primerih

[14] DDoS (Distributed Denial-of-Service)

[15] The European Agenda on Security [online], 2015. Dostopno na: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

posledično celo ogroža življenja. Sredstva in načini, ki se uporabljajo pri kibernetskem kriminalu, se uporabljajo tudi pri bolj tradicionalnih oblikah kriminala.

4.4 Obveščevalna dejavnost

Zaradi velike odvisnosti celotne družbe od informacijsko-komunikacijskih tehnologij se je povečalo tveganje, povezano z obveščevalno dejavnostjo tujih obveščevalnih služb. Potencial kibernetskega prostora lahko za dosego svojih ciljev izkoristijo različni državni ali nedržavni deležniki, predvsem z izvajanjem kibernetskih obveščevalnih operacij, s katerimi lahko v določenih segmentih ogrozijo politične, varnostne in gospodarske interese Republike Slovenije.

4.5 Spreminjanje varnostnega okolja

Varnostno tveganje predstavljajo tudi zlonamerni hekerski vdori v informacijske sisteme državne uprave oziroma državnih organov. Obliko asimetričnega bojevanja predstavlja tveganje zlonamernega delovanja zoper kibernetsko varnost kritične infrastrukture. Tako delovanje je še posebej nevarno v povezavi z vse bolj organiziranimi mednarodnimi terorističnimi mrežami.

4.6 Vdori v zasebnost

V informacijski družbi je zasebnost posameznika vse pogosteje na udaru, saj se mora soočati z interesi za pridobivanje, obdelavo in hranjenje osebnih podatkov tako s strani različnih podjetij za komercialne namene kot tudi s strani državnih organov. Pričakovati je, da se bodo z naraščanjem terorističnih groženj in z izvajanjem ukrepov za njihovo preprečevanje povečale tudi težnje po večjem nadzoru in posledično omejevanju posameznikove zasebnosti v kibernetskem prostoru.

5 Opredelitev deležnikov

V sistemu zagotavljanja kibernetske varnosti sodelujejo organizacije iz javnega in zasebnega sektorja. Poleg bodoče osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti ter vseh odzivnih centrov v državi imajo pomembno vlogo tudi Agencija za komunikacijska omrežja in storitve (AKOS), telekomunikacijski operaterji in upravljavci telekomunikacijske infrastrukture, ponudniki storitev informacijske družbe, akademsko-raziskovalna sfera (nekatere fakultete in raziskovalne organizacije), stanovska (zbornice s področja gospodarstva in podjetništva) in strokovna združenja (slovenska združenja in slovenske sekcije mednarodnih združenj s področja informacijsko-komunikacijskih tehnologij in kibernetske varnosti) ter proizvajalci programske opreme, ki nudijo podporo državnim organom.

V širšem pomenu med deležnike pri zagotavljanju kibernetske varnosti v Sloveniji štejejo tudi organizacije s tega področja v tujini, predvsem takrat, ko se skupaj s slovenskimi deležniki odzivajo na varnostne incidente. V tem oziru so pomembni predvsem partnerji v okviru EU in NATO.

6 Vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti in jasne strukture upravljanja

Uspešno zagotavljanje visokega nivoja kibernetske varnosti zahteva učinkovito izrabo obstoječih virov in primerno več-nivojsko organiziranost. Slovenija bo vzpostavila osrednjo koordinacijo nacionalnega sistema zagotavljanja kibernetske varnosti in zagotovila pogoje za njeno stabilno delovanje. Koordinacija bo na strateški ravni koordinirala zmogljivosti za zagotavljanje kibernetske varnosti na nižjih ravneh v državi ter predstavljala enotno kontaktno točko pri mednarodnem sodelovanju. O obliki organiziranosti zagotavljanja koordinacijskih funkcij bo odločila Vlada Republike Slovenije.

Na operativni ravni zagotavljanja kibernetske varnosti bodo s svojimi zmogljivostmi delovali SI-CERT na nacionalni ravni, Ministrstvo za obrambo na področju obrambe in varstva pred naravnimi in drugimi nesrečami, Policija na področju zagotavljanja kibernetske varnosti v okviru javne varnosti in zatiranja kibernetskega kriminala, SOVA na področju protiobveščevalnega delovanja in nastajajoči SIGOV-CERT na področju javne uprave.

Slika 1: Shematski prikaz sistema zagotavljanja kibernetske varnosti

V sistem zagotavljanja kibernetske varnosti bodo povezani tudi drugi deležniki. Pomembni so upravljavci kritične infrastrukture v zasebnem in javnem sektorju, še posebej v sektorju energetike – zagotavljanje električne energije (proizvajalci in distributerji električne energije) in v sektorju

informacijsko-komunikacijske podpore (telekomunikacijski operaterji, ponudniki storitev informacijske družbe itd.).

K sistemu zagotavljanja kibernetske varnosti bo na področju ozaveščanja, izobraževanja in raziskav prispevala tudi akademsko-raziskovalna sfera z visokošolskimi študijskimi programi in predmeti s področja kibernetske varnosti na vseh ravneh izobraževanja ter izsledki raziskovalnih organizacij. Sistem bo odprt tudi za pobude iz civilne družbe. Tu gre predvsem za pobude za izboljšave in pomoč pri ozaveščanju različnih ciljnih skupin s strani strokovnih združenj (slovenska združenja in slovenske sekcije mednarodnih združenj s področja informacijsko-komunikacijskih tehnologij in kibernetske varnosti).

7 Področja udejanjanja strategije

Udejanjanje strategije bo osredotočeno na preprečevanje varnostnih incidentov, odzivanje na varnostne incidente ter na ozaveščanje ciljnih skupin o pomenu kibernetske varnosti.

7.1 Preprečevanje

Preprečevanje varnostnih incidentov obsega vse od tehnične zasnove komponent informacijskih sistemov do zagotavljanja nacionalnih in mednarodnih zakonskih okvirov in predpisov, ki pripomorejo k razvoju varnejših aplikacij in infrastrukture. Pri tem je treba zagotoviti, da bo v zasnovo aplikacij in informacijsko-komunikacijske infrastrukture vključena varnost in zaščita zasebnosti posameznika in da bodo upoštevani standardi, ki zagotavljajo varno in nemoteno delovanje sistemov, vključno z uporabo šifrirnih rešitev[16]. Izvaja se ocenjevanja tveganj, na osnovi katerih se pripravi in izvaja ukrepe za znižanje nesprejemljivih tveganj ter analiza izvedenih ukrepov. Spodbuja se uporaba tehnologij, temelječih na odprtih standardih za zagotavljanje interoperabilnosti, ki jih je možno čim bolj nadzirati in niso delno ali v celoti zaprte zaradi varovanja patentnih pravic.

7.2 Odzivanje

Samo preventiva ni dovolj za doseganje visoke stopnje kibernetske varnosti. Ker varnostnih incidentov nikoli ne bo mogoče v celoti odpraviti, je treba zagotoviti ustrezne mehanizme odzivanja nanje. Pri tem so pomembne izkušnje iz faze preprečevanja, pa tudi iz primerov odzivanja na varnostne incidente v preteklosti. Izkušnje lahko prihajajo od domačih in tujih organov, ki skrbijo za zagotavljanje kibernetske varnosti, zato je njihova čim boljša povezanost zelo pomembna. Na podlagi izkušenj ter analize incidentov in tveganj se stalno posodabljajo in izboljšujejo tudi postopki odzivanja. Pri tem se tvorno sodeluje tudi pri pripravi standardnih postopkov odzivanja ob kibernetskih krizah na mednarodni oziroma svetovni ravni.

[16] Šifriranje je proces preoblikovanja digitalnega zapisa informacije iz berljive v neberljivo obliko. S šifrirnimi mehanizmi se zagotavlja zaupnost med entitetami, udeleženimi v komunikaciji.

7.3 Ozaveščanje

Ljudje so tisti, ki informacijsko-komunikacijske tehnologije razvijajo, gradijo in uporabljajo. Z ozaveščanjem in izobraževanjem se lahko zmanjšuje tveganja in gradi kulturo varne uporabe tehnologij. V fazi ozaveščanja je treba uporabiti izkušnje iz faz preprečevanja in odzivanja, da se uporabnikom predstavijo realna tveganja in učinkovite metode, kako se jim izogniti. Načini in vsebine ozaveščanja se v največji možni meri prilagodijo različnim ciljnim skupinam. Za otroke in mlade se teme s področja kibernetske varnosti vključi v učne programe na različnih ravneh izobraževanja. Izoblikujejo se prilagojeni programi ozaveščanja za ostalo prebivalstvo ter gospodarske subjekte. Spodbuja se uporaba šifrirnih rešitev kot enega od temeljev zagotavljanja kibernetske varnosti.

8 Cilji strategije in ukrepi za njihovo doseganje

Uresničevanje strategije, ki bo temeljilo na nadgradnji in dopolnitvi obstoječih zmogljivosti sistema zagotavljanja kibernetske varnosti, bodo na podlagi pristojnosti, ki jih določajo ustava in zakoni, spremljali Vlada Republike Slovenije, osrednja koordinacija nacionalnega sistema za kibernetsko varnost in pristojna resorna ministrstva.

Za uresničevanje ciljev strategije kibernetske varnosti bo izvedeno več ukrepov. Če se bo med uresničevanjem strategije pokazala potreba, bodo ukrepi lahko ustrezno dopolnjeni.

CILJI	UKREPI
1. Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti	• vzpostavitev osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti; • kadrovska in tehnološka okrepitev organov na operativni ravni sistema zagotavljanja kibernetske varnosti skupaj z vzpostavitvijo SIGOV-CERT; • redna udeležba na mednarodnih vajah s področja kibernetske varnosti ter izvedba nacionalnih vaj; • postopna nadgradnja omrežja državnih organov HKOM z opremo, ki je ustrezno potrjena s strani slovenskih organov kot varna in primerna za uporabo; • vzpostavitev kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novo vzpostavljenih organov.
2. Varnost državljanov v kibernetskem prostoru	• redno izvajanje programov ozaveščanja na področju kibernetske varnosti; • uvedba vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja.
3. Kibernetska varnost v gospodarstvu	• spodbujanje razvoja in vpeljave novih tehnologij na področju kibernetske varnosti; • redno izvajanje programov ozaveščanja na področju kibernetske varnosti za gospodarske subjekte.
4. Zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore	• redno ocenjevanje tveganj za delovanje kritične infrastrukture sektorja informacijsko-komunikacijske podpore, načrtovanje ustreznih ukrepov za zaščito ter

CILJI	UKREPI
	posodabljanje ocene tveganj na tem področju.
5. Zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala	• implementacija ustreznih kibernetskih zmogljivosti za varovanje informacijskih in komunikacijskih sistemov policije; • redno usposabljanje s področja kibernetske varnosti za organe pregona, ki sodelujejo pri razvoju kibernetskih zmogljivosti za področje javne varnosti in pri zatiranju kibernetskega kriminala; • redno posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij.
6. Razvoj obrambnih kibernetskih zmogljivosti	• razvoj ustreznih kibernetskih zmogljivosti za varovanje obrambnih komunikacijskih in informacijskih sistemov.
7. Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah	• zagotovitev pogojev za nemoteno delovanje ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah.
8. Krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem	• zagotovitev pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti.

Tabela 1: Tabela ciljev strategije kibernetske varnosti in potrebnih ukrepov za njihovo doseganje

8.1 Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti

Slovenija bo okrepila in tudi nadgradila obstoječi sistem zagotavljanja kibernetske varnosti v državi, vključno s svojo diplomatsko-konzularno mrežo. Zaradi naraščajočega obsega varnostnih incidentov obstoječe zmogljivosti odzivnih centrov ne zadoščajo več. Za zagotovitev ustreznega odzivanja nanje bodo zato okrepljene zmogljivosti nacionalnega odzivnega centra SI-CERT in odzivnega centra za področje obrambe in varstva pred naravnimi in drugimi nesrečami (kibernetske zmogljivosti Ministrstva za obrambo) ter vzpostavljen samostojni odzivni center za sisteme v javni upravi (SIGOV-CERT). V okvir okrepitve sistema zagotavljanja kibernetske varnosti sodi tudi priprava načrta odzivanja na varnostne incidente.

Na strateški ravni sistema zagotavljanja kibernetske varnosti bo vzpostavljena osrednja koordinacija za celovito obravnavo problematike in koordinacijo aktivnosti na vseh področjih kibernetske varnosti. Ena izmed funkcij koordinacije bo prevzem vloge enotne kontaktne točke države za mednarodno sodelovanje na področju kibernetske varnosti.

Slovenija se bo tudi v prihodnje redno udeleževala mednarodnih vaj s področja kibernetske varnosti. Poleg tega bo izvajala tudi vaje na nacionalni ravni. Vsebina posamezne vaje bo lahko skladna z vsakokratno oceno tveganja za določeno grožnjo, vendar na podlagi čim bolj realističnega scenarija. Vsaj občasno se bodo izvedle vaje, v katerih bodo sodelovali vsi organi, ki se ukvarjajo z zagotavljanjem kibernetske varnosti. Tako se bodo preverili vsi mehanizmi, uigranost in medsebojno

sodelovanje sodelujočih. Vsaki vaji bo sledila podrobna analiza rezultatov in oblikovanje predlogov za izboljšave ter po potrebi tudi dopolnitev oziroma osvežitev načrta odzivanja na varnostne incidente.

Za dosego cilja okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti se izvedejo ukrepi:

- vzpostavitev osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti;
- kadrovska in tehnološka okrepitev organov na operativni ravni sistema zagotavljanja kibernetske varnosti skupaj z vzpostavitvijo SIGOV-CERT;
- redna udeležba na mednarodnih vajah s področja kibernetske varnosti ter izvedba nacionalnih vaj;
- postopna nadgradnja omrežja državnih organov HKOM z opremo, ki je ustrezno potrjena s strani slovenskih organov kot varna in primerna za uporabo;
- vzpostavitev kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novo vzpostavljenih organov.

8.2 Varnost državljanov v kibernetskem prostoru

Vsakemu posamezniku mora biti omogočena čim varnejša uporaba informacijsko-komunikacijskih tehnologij ob hkratnem spoštovanju zasebnosti in človekovih pravic. Državljani morajo imeti možnost, da se seznanijo s tveganji v kibernetskem prostoru in načini za njihovo obvladovanje ter s tem povezano odgovornostjo vsakega posameznika za lastno varnost v globalnem komunikacijskem omrežju. Zagotavljanje kibernetske varnosti ne sme nesorazmerno posegati v zasebnost z uporabo pretiranih ukrepov ali sredstev. V oblikovanje zakonodaje, ki ureja dopustno mero vdora v informacijsko zasebnost, morajo biti vselej pravočasno in enakopravno vključeni vsi relevantni in zainteresirani deležniki.

Ozaveščanje uporabnikov o pomenu kibernetske varnosti je izredno pomembno, saj prispeva h graditvi oziroma dvigu kulture kibernetske varnosti. Tako se uporabniki naučijo samostojno poskrbeti za svojo varnost v kibernetskem prostoru. Zato se bo nadaljevalo z izvajanjem že obstoječih programov ozaveščanja, poleg tega pa bodo oblikovani tudi novi. Spodbujalo se bo sodelovanje pri različnih pobudah za dvig ozaveščenosti in vključitev civilne družbe v aktivnosti na tem področju. Učinkovito ozaveščanje se bo osredotočalo na posamezne ciljne skupine (npr. otroke in mladino, različne starostne skupine državljanov, gospodarske subjekte).

Vsebine s področja kibernetske varnosti bodo primerno vključene v učne programe izobraževalnih ustanov na vseh ravneh izobraževalnega sistema. Poleg tega je treba spodbuditi univerze (npr. s povečanim povpraševanjem gospodarstva), da bodo ponudile samostojne študijske programe s področja kibernetske varnosti. Ključni deležniki pri zagotavljanju kibernetske varnosti morajo s stalnim usposabljanjem skrbeti za razvoj kompetenc in za certificiranje kadrov, ki opravljajo oziroma bodo opravljali naloge zagotavljanja kibernetske varnosti.

Za dosego cilja varnost državljanov v kibernetskem prostoru se izvedeta ukrepa:

- redno izvajanje programov ozaveščanja na področju kibernetske varnosti;
- uvedba vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja.

8.3 Kibernetska varnost v gospodarstvu

V Sloveniji na področju informacijsko-komunikacijskih tehnologij v gospodarstvu že sedaj obstaja velik potencial, ob ustreznih osredotočenih vlaganjih v raziskave, razvoj in inovacije pa je možen preboj tudi na področju kibernetske varnosti. Zagotavljanje kibernetske varnosti v gospodarstvu je še posebej pomembno v okolju digitalizacije podjetništva in industrije. Država bo sofinancirala projekte in ciljno usmerjene raziskave s tega področja, ki imajo potencial prispevka h kibernetski varnosti. Uporabni rezultati takih projektov in raziskav morajo stalno nadgrajevati sistem kibernetske varnosti. Država bo tako kot na drugih področjih tudi na področju kibernetske varnosti spodbujala povezovanje akademsko-raziskovalne sfere z gospodarstvom na nacionalni in tudi mednarodni ravni. Tako bo pomagala ustvariti kritično maso strokovnjakov s tega področja, s tem pa oblikovanje javno-zasebnih partnerstev, ki bodo sposobna razviti inovativne izdelke in storitve z visoko dodano vrednostjo za domači in svetovni trg.

Vse bolj digitaliziranemu gospodarstvu mora biti za njegovo delovanje omogočeno varno komunikacijsko okolje. Zato se bodo še naprej izvajali programi za ozaveščanje podjetij o tveganjih kibernetskega prostora in varni uporabi informacijsko-komunikacijskih tehnologij. Pri tem bo skladno s sprotnimi analizami stanja večja pozornost namenjena ugotovljenim kritičnim področjem. Spodbujalo se bo prizadevanja za razvoj in uporabo standardov na področju kibernetske varnosti.

Za dosego cilja kibernetska varnost v gospodarstvu se izvedeta ukrepa:

- spodbujanje razvoja in vpeljave novih tehnologij na področju kibernetske varnosti;
- redno izvajanje programov ozaveščanja na področju kibernetske varnosti za gospodarske subjekte.

8.4 Zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore

Kritična infrastruktura sektorja informacijsko-komunikacijske podpore mora biti zasnovana in upravljana tako, da zagotavlja sistemsko informacijsko-komunikacijsko podporo na različnih ravneh. Zagotoviti je treba neprekinjeno delovanje infrastrukture, ki pogojuje delovanje internetnih sistemov v državi in strojne ter programske opreme, ki podpira ključne funkcije v državi. Vzpostavijo se hitri in učinkoviti mehanizmi za odzivanje na grožnje in odpravljanje napak (sanacija škode), ki so posledica varnostnih incidentov ter mehanizmi preventivnega delovanja, ki grožnje in napake v največji meri preprečujejo. Z vzpostavitvijo samostojnega odzivnega centra za sisteme v javni upravi (SIGOV-CERT) se razbremeni SI-CERT, ki lahko ob ustrezni okrepitvi pozornost usmeri tudi na zagotavljanje kibernetske varnosti v sektorju informacijsko-komunikacijske podpore.

Za dosego cilja zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore se izvede ukrep:

- redno ocenjevanje tveganj za delovanje kritične infrastrukture sektorja informacijsko-komunikacijske podpore, načrtovanje ustreznih ukrepov za zaščito ter posodabljanje ocene tveganj na tem področju.

8.5 Zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala

Slovenija bo razvila kibernetske zmogljivosti, ki bodo sposobne samostojno in v sodelovanju z drugimi državami varovati komunikacijske in informacijske sisteme s področja javne varnosti (Schengen, Europol, Interpol) ter zagotavljati podporo za operativno delo policije. Pospešeno se bodo razvijale zmogljivosti policije in pravosodnih organov na področju zatiranja kibernetskega kriminala. Večja pozornost bo namenjena področju razvoja digitalne forenzike in skrbi za primerno usposobljenost vseh organov pregona, ki delujejo na tem področju. Znanja s področja zatiranja kibernetskega kriminala so pomembna tudi za uspešen pregon klasičnih vrst kaznivih dejanj, saj se tudi za izvedbo le-teh vedno bolj uporabljajo storitve, ki jih omogoča internet in druge vrste omrežij. Pri razvoju kibernetskih zmogljivosti bo država sodelovala tudi z gospodarstvom in institucijami znanja. Pri odkrivanju novih oblik kibernetskega kriminala in izmenjavi informacij bo pomembno sodelovanje policije z odzivnimi centri, akademsko-raziskovalno sfero, proizvajalci strojne in programske opreme ter s strokovnimi združenji s področja informacijsko-komunikacijskih tehnologij tako na nacionalni kot tudi mednarodni ravni. Zakonodaja in postopki na tem področju morajo slediti hitremu razvoju informacijsko-komunikacijskih tehnologij, v njihovo pripravo pa naj se vključijo tudi ustrezni tehnični strokovnjaki.

Za dosego cilja zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala se izvedejo ukrepi:

- implementacija ustreznih kibernetskih zmogljivosti za varovanje informacijskih in komunikacijskih sistemov policije;
- redno usposabljanje s področja kibernetske varnosti za organe pregona, ki sodelujejo pri razvoju kibernetskih zmogljivosti za področje javne varnosti in pri zatiranju kibernetskega kriminala;
- redno posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij.

8.6 Razvoj obrambnih kibernetskih zmogljivosti

Slovenija bo razvila obrambne kibernetske zmogljivosti, ki bodo sposobne samostojno in v sodelovanju z drugimi državami EU in NATO varovati obrambne komunikacijske in informacijske sisteme ter zagotavljati podporo vojaškim operacijam in kriznemu načrtovanju. Obrambne kibernetske zmogljivosti bo država razvijala samostojno in tudi v sodelovanju s partnerji iz EU in NATO ter pri tem sodelovala z gospodarstvom in institucijami znanja.

Za dosego cilja razvoj obrambnih kibernetskih zmogljivosti se izvede ukrep:

- razvoj ustreznih kibernetskih zmogljivosti za varovanje obrambnih komunikacijskih in informacijskih sistemov.

8.7 Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah

Slovenija je izpostavljena naravnim in drugim nesrečam[17], ki so lahko tudi velikega obsega. Zato je treba zagotoviti ustrezne vire in izvesti ukrepe za zagotavljanje učinkovitega delovanja informacijsko-komunikacijskih sistemov v vseh okoliščinah, tudi ob velikih naravnih in drugih nesrečah. Z ukrepi zagotavljanja kibernetske varnosti se zagotovi celovitost podatkov ter razpoložljivost, zanesljivost in varnost dostopa do storitev in podatkov.

Za dosego cilja zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah se izvede ukrep:

- zagotovitev pogojev za nemoteno delovanje ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah.

8.8 Krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem

Glede na globalno naravo interneta in s tem tudi problematike kibernetske varnosti je mednarodno sodelovanje pri zagotavljanju kibernetske varnosti za Slovenijo kot majhno državo nujno potrebno. Tako sodelovanje omogoča kakovostno izmenjavo izkušenj, znanja in najboljših praks, kar vse prispeva h krepitvi nacionalne varnosti. Država bo zato še naprej spodbujala sodelovanje njenih predstavnikov v mednarodnih organizacijah, kot so OZN, EU, NATO, OVSE, OECD in ITU, ter v mednarodnih strokovnih združenjih s tega področja. Slovenija si bo prizadevala za razvoj mednarodnih norm delovanja v kibernetskem prostoru ter v sodelovanju z drugimi državami in mednarodnimi partnerji za vzpostavitev praktičnih ukrepov za krepitev zaupanja. Na mednarodni ravni bo Slovenija dejavna pri prenosu znanja na področju kibernetske varnosti.

Za dosego cilja krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem se izvede ukrep:

- zagotovitev pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti.

[17] Resolucija o nacionalnem programu varstva pred naravnimi in drugimi nesrečami v letih 2009 do 2015 (RENPVNDN) poudarja občutljivost Republike Slovenije za različne vire ogrožanja, ki jo še posebej povečuje njena geografska pestrost, omejenost naravnih virov in prostora, majhnost ozemlja, prehodnost in policentrična poseljenost. V: Uradni list RS [online], 2009, št. 57/2009. Dostopno na: http://www.uradni-list.si/1/objava.jsp?urlid=200957&stevilka=2789.

9 Tveganja za udejanjanje strategije

Največje tveganje za udejanjanje strategije je nezadostno zavedanje o pomenu področja zagotavljanja kibernetske varnosti, s čimer je povezana nizka splošna varnostna kultura, ter pomanjkanje politične volje in soglasja za sistemsko ureditev področja na nacionalni ravni. Nesistematičen razvoj tako pomembnega področja, kot je zagotavljanje kibernetske varnosti, bi imel za državo zelo negativne posledice, v primeru kibernetskih napadov velikega obsega pa bi bile te tudi težko popravljive.

Uspešno izvajanje strategije pa bo nasprotno pozitivno vplivalo na zagotavljanje nacionalne varnosti ter imelo pozitivne multiplikativne učinke, povezane s povečano stopnjo varnosti. Prav tako bo vplivalo na porast zaupanja uporabnikov v internet in s tem razvoj novih storitev in poslovnih modelov, povezanih z njegovo uporabo, kar se bo izrazilo v digitalni gospodarski rasti in povečanju družbene blaginje.

PREDNOSTI	POMANJKLJIVOSTI
• Operativna raven sistema zagotavljanja kibernetske varnosti je vzpostavljena. • Kakovostni, čeprav nezadostni kadrovski viri na operativni ravni sistema. • Dobri rezultati dosedanjih preventivnih ukrepov (programi ozaveščanja). • Sodelovanje na skupnih mednarodnih vajah.	• Strateška raven zagotavljanja kibernetske varnosti ni vzpostavljena. • Pomanjkanje virov (finančnih, kadrovskih, materialno-tehničnih). • Nezadostno sodelovanje med ključnimi deležniki. • Področje ni sistemsko urejeno.
PRILOŽNOSTI	**NEVARNOSTI**
• Večje zaupanje uporabnikov (podjetij, državne uprave, posameznikov) v uporabo interneta, kar povečuje njegovo uporabo (B2C, B2B, B2G, G2C), znižuje stroške poslovanja in posledično omogoča digitalno gospodarsko rast. • Povezovanje obstoječih zmogljivosti in izkoriščanje sinergij.	• Nezadostno zavedanje pomena področja ter s tem povezano pomanjkanje politične volje in soglasja za hitro in učinkovito ukrepanje ter sistemsko ureditev na nacionalni ravni. • Možnost odpovedi sistema ob porastu varnostnih incidentov, če sistem ne bo okrepljen.

Tabela 2: Analiza prednosti, pomanjkljivosti, priložnosti in nevarnosti za udejanjanje strategije

Strategija kibernetske varnosti nima neposrednih finančnih posledic, ker gre za strateški dokument, ki je načelno vodilo razvojnih aktivnosti na področju zagotavljanja kibernetske varnosti. Finančne posledice bodo nastale z izvajanjem strategije, ki bo omejeno z razpoložljivimi sredstvi v okviru vsakokratnega veljavnega državnega proračuna, torej ob upoštevanju 23. člena Zakona o izvrševanju proračuna, ki določa, da je obseg sredstev za financiranje posameznih izdatkov lahko le v znesku, določenem s proračunom. Izvajanje strategije bo hkrati omejeno z razpoložljivimi sredstvi v okviru Operativnega programa za izvajanje evropske kohezijske politike v obdobju 2014–2020.

A Seznam kratic

AKOS	Agencija za komunikacijska omrežja in storitve Republike Slovenije
Arnes	Akademska in raziskovalna mreža Slovenije
B2B	Business to Business (podjetje – podjetje)
B2C	Business to Customer (podjetje – stranka)
B2G	Business to Government (podjetje – državna uprava)
CERT	Computer Emergency Response Team (Odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij)
ENISA	European Union Agency for Network and Information Security (Agencija EU za varnost omrežij in informacij)
EU	Evropska unija
G2C	Government to Customer (državna uprava – stranka)
ITU	International Telecommunication Union (Mednarodna zveza za telekomunikacije)
NATO	North Atlantic Treaty Organization (Organizacija severnoatlantske pogodbe)
OVSE	Organizacija za varnost in sodelovanje v Evropi
OZN	Organizacija združenih narodov
SI-CERT	Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij
SIGOV-CERT	Odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij za sisteme v javni upravi
SOVA	Slovenska obveščevalno-varnostna agencija