STRATEGIJA

KRIPTOGRAFSKE ZAŠČITE

PODATKOV V

REPUBLIKI SLOVENIJI

Avgust 2016

Predgovor

Z razvojem informacijskih tehnologij in s tem povezanim razvojem obdelave informacij je danes sorazmerno enostavno prestreči in spremeniti digitalne zapise podatkov, zato so se povečale zahteve po njihovi varnosti, ko se obravnavajo in prenašajo po komunikacijsko-informacijskih sistemih. Poleg običajnih ukrepov varnosti v sistemih (npr. vstopno uporabniško ime in geslo, protivirusni programi, programske ali strojne požarne pregrade ipd.) je pri zaščiti sistemov in podatkov ključna uporaba kriptografije.

Kriptografija je znanstvena veda, ki ima številne praktične uporabnosti. Uporablja se v številnih kriptografskih rešitvah, ki so prosto dostopne na trgu, državljani razvitih držav jo uporabljamo dnevno. Uporablja se pri overjanju in šifriranju (bančne kartice, brezžični telefoni, e-poslovanje, plačljiva TV), nadzoru dostopov (sistemi za zaklepanje vozil, smučarske vozovnice), pri plačevanju (predplačniške telefonske kartice, e-denar) in lahko postane temeljni instrument za demokracijo z vpeljavo sistemov za elektronsko glasovanje.

Kriptografija zagotavlja varno komuniciranje ob navzočnosti tretje osebe, ki se jo obravnava kot prisluškovalca oziroma nezakonitega udeleženca komunikacije (lahko je to naš nasprotnik, sovražnik). Beseda kriptografija izhaja iz grških besed κρυπτός (skrito, tajno) in γράφειν (pisanje) in pomeni skrito oziroma tajno pisanje. Zaradi zgodovinskih razlogov je še danes izraz »šifriranje« pogosto sinonim za kriptografijo. Šifriranje je proces preoblikovanja digitalnega zapisa informacije iz berljive v neberljivo obliko.

Kriptografija opremlja oblikovalce informacijskih tehnologij z orodji, ki neposredno ali posredno pripomorejo k zagotavljanju varnostnih dejavnikov, kot so: zaupnost, celovitost, razpoložljivost, avtentičnost in nezatajljivost. Med slednjimi je zaupnost najpogostejši varnostni dejavnik, ki se zagotavlja s šifriranjem. Pri tem je potreben šifrirni ključ, s katerim lahko dešifriramo prejeta šifrirana sporočila v berljivo obliko. Šifrirni ključ je tudi eden od ključnih parametrov, ki mora biti ustrezno varovan. Kompromitacija šifrirnega ključa pomeni, da je postal javen in posledično ne zagotavlja več varnostne zahteve po zaupnosti. Varnost ne sme temeljiti le na tajnosti kriptografskih mehanizmov, temveč predvsem na tajnosti šifrirnega ključa. Drugo vprašanje je, kakšna je dejanska kriptografska varnost šifrirnega ključa. Odgovor na to vprašanje zagotavlja kriptoanaliza kriptografskih mehanizmov. Kriptografija in kriptoanaliza skupaj sta znani pod imenom kriptologija.

Sprejetje strategije kriptografske zaščite podatkov je za Republiko Slovenijo pomembno zaradi več razlogov, ki so obrazloženi v nadaljevanju, njeno uresničevanje pa mora postati trajnostno. Gre za dokument, ki opredeljuje področje kriptografije in priporoča uporabo kriptografskih rešitev. Sedanja zakonodaja sicer zahteva uporabo kriptografskih rešitev, vendar kljub temu še vedno nimamo enotnih stališč, ki bi jih lahko trajnostno upoštevali. Državni organi in organizacije so pogosto prepuščeni sami sebi in lastnim usmeritvam.

Izhajali smo iz strokovnega stališča, da se kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov, ne bi nabavljale v tujini. S takimi nabavami se dejansko razkrijejo vsi načini varovanja podatkov najmanj prodajalcu kriptografskih rešitve, s tem pa se posredno poveča možnost napada na naš sistem. Izjeme so kriptografske rešitve tujih proizvajalcev, ki jih po opravljenem postopku vrednotenja in izpolnitvi predpisanih pogojev potrdijo za to pristojni organi v Republiki Sloveniji. Pristop do kriptografije, zasnovan v strategiji, temelji na predpostavki, da država vzpostavi lastne kriptografske rešitve za namene varovanja tajnih podatkov, priporoča pa jih tudi za varovanje drugih podatkov. Tako politiko ima večina držav članic zveze NATO in EU. K sprejemu zakonskega okvira za ustrezno uporabo kriptografskih mehanizmov na vseh

področjih nas zavezujejo tudi usmeritve združenja OECD[1] in priporočila evropske agencije ENISA[2]. V primeru varovanja netajnih podatkov se podpira uporaba odprtokodnih rešitev.

Področje zaupanja in varnosti je tudi eden izmed sedmih stebrov Digitalne agende za Evropo, ki jo je leta 2010 objavila Evropska komisija z namenom, da bi omogočila izhod iz krize in gospodarstvo EU pripravila na izzive naslednjega desetletja (Evropa 2020 – strategija za pametno, trajnostno in vključujočo rast).

[1] OECD (Organisation for Economic Co-operation and Development) je mednarodna gospodarska organizacija razvitih držav, ki sprejemajo načela predstavniške demokracije in svobodnega trga. Slovenija je od leta 2010 članica organizacije OECD.
[2] ENISA (European Network and Information Security Agency) je evropska agencija za varnost omrežij in informacij.

1. Uvod

Delo na področju kriptologije je interdisciplinarno in zahteva povezovanje profilov strokovnjakov, kot so inženirji za programsko in strojno računalniško opremo ter matematiki. Republika Slovenija bo s tem tudi podprla razvoj in uvedbo varnih storitev v kibernetskem prostoru na ozemlju Republike Slovenije, ki bodo podprte s kriptografskimi rešitvami na vseh področjih (tajni podatki, osebni podatki, e-identiteta, e-podpis, e-transakcije ipd.) tako glede postavljanja tehnoloških zahtev za storitve kot tudi podpore domačemu razvojno-raziskovalnemu sektorju in proizvajalcem varnih storitev. Uporabnik in ponudnik teh storitev bosta tako javni kot zasebni sektor. To je mogoče le, če so znanja pametno izkoriščena. Znanja, veščine in kompetence strokovnjakov so ključni dejavniki, ki omogočajo, da se raziskovalni, razvojni in tržni potenciali lahko izkoristijo in prispevajo k povečanju produktivnosti in inovativnosti.

V slovenskih predpisih so kriptografske rešitve opredeljene kot kriptografska oprema (strojna in programska) in sistemi, ki se uporabljajo za šifrirno varovanje podatkov v komunikacijsko-informacijskih sistemih, v katerih se obravnavajo tajni, osebni in drugi občutljivi podatki. Med kriptografske rešitve spadajo tudi vsi moduli, ki so vgrajeni v posameznih delih sistemov in so namenjeni šifrirnemu varovanju podatkov. Šifrirno ovrednotenje je postopek, v katerem se ugotovi varnostna ustreznost predlagane kriptografske rešitve za varovanje prenosa tajnih podatkov določene stopnje tajnosti.

Med pomembnejšimi varnostnimi deli so šifrirni algoritmi in njihov prenos v kriptografske rešitve. Ob razvoju nacionalnih kriptografskih rešitev je smiselni prenos ustreznih obstoječih šifrirnih algoritmov v končnih rešitvah.

Pri šifrirnem vrednotenju tujih kriptografskih rešitev se Urad Vlade Republike Slovenije za varovanje tajnih podatkov srečuje s problemom dostopa do varnostno kritičnih delov, ker slednjih tuji proizvajalci oziroma pristojni organ države proizvajalke niso pripravljeni v celoti razkriti zaradi zaščite lastnih interesov. Posledično se uporabljajo za varovanje tajnih podatkov, osebnih podatkov in drugih občutljivih podatkov tuje kriptografske rešitve, za katere ne vemo natančno, kako delujejo oziroma ne poznamo načina delovanja posameznih varnostno kritičnih delov. Razlog za to je pomanjkanje državne podpore razvoju in proizvodnji domačih kriptografskih rešitev in pomanjkanje narodne zavesti po uporabi domačih kriptografskih rešitev. V Republiki Sloveniji je tako opažena odsotnost državne pobude za razvoj domačih kriptografskih rešitev. Gre večinoma za unikatne produkte z zelo ozkim krogom uporabnikov in posebnimi zahtevami. Za nacionalno varnost sta trajnostni razvoj in proizvodnja domačih kriptografskih rešitev bistvenega pomena.

V komunikacijsko-informacijskih sistemih, v katerih se obravnavajo tajni podatki, je dovoljena uporaba kriptografskih rešitev, za katere je bilo izdano potrdilo o varnostni ustreznosti. Potrdilo o varnostni ustreznosti lahko izda Urad Vlade Republike Slovenije za varovanje tajnih podatkov ali drug z zakonom določeni organ, in sicer na podlagi šifrirnega ovrednotenja za vsako kriptografsko rešitev posebej. Za varovanje prenosa tajnih podatkov v komunikacijsko informacijskih sistemih je treba v čim večji meri uporabljati kriptografske rešitve domačih proizvajalcev, saj je uporaba tujih kriptografskih rešitev lahko varnostno neustrezna.

Strategija se osredotoča na kriptografske rešitve in njihovo uporabo v javni upravi, zlasti za varno komuniciranje in hrambo podatkov.

Strategija le v manjšem delu posega na širše področje uporabe kriptografskih rešitev in v teh primerih podpira uporabo preverjenih odprtokodnih rešitev.

2. Zasnova strategije, cilji in obdobje za dosego ciljev

Vlada Republike Slovenije je zasnovala Strategije kriptografske zaščite podatkov v Republiki Sloveniji z opredeljenimi cilji, za dosego katerih so oblikovani okvirni načrti in ukrepi za:

- vrednotenje kriptografskih rešitev,
- spodbujanje razvoja in uporabe kriptografskih rešitev,
- zagotavljanje kriptografskih rešitev,
- raziskovanje na področju kriptologije,
- usposabljanje uporabnikov kriptografskih rešitev,
- zagotavljanje kadrovskih virov:
    - podeljevanje štipendij za področje kriptologije,
    - zaposlovanje kriptoloških strokovnjakov.

Navedeni cilji so v naslednjem poglavju vsebinsko podrobneje opredeljeni s predstavitvijo obstoječega stanja in ciljnega stanja, ključnih nosilcev razvoja in deležnikov, ukrepov za doseganje ciljnega stanja in opredelitvijo tveganj.

Predviden čas za dosego ciljev je leto 2025.

3. Opredelitev ciljev

3.1 Vrednotenje *kriptografskih* rešitev

Obstoječe stanje

Postopki vrednotenj kriptografskih rešitev so urejeni s predpisi in se izvajajo z omejenim številom strokovno usposobljenega kadra.

Za potrebe varovanja tajnih podatkov postopke šifrirnih vrednotenj opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov, za obrambne potrebe pa Ministrstvo za obrambo. Urad Vlade Republike Slovenije za varovanje tajnih podatkov je za potrebe opravljanja šifrirnega vrednotenja ustanovil medresorsko strokovno delovno skupino za komunikacijsko varnost.

Ciljno stanje

V okviru Urada Vlade Republike Slovenije za varovanje tajnih podatkov vzpostaviti enotni organa, pristojen za kriptografsko zaščito tajnih podatkov, ki opravlja tudi postopke šifrirnih vrednotenj. Za nemoteno opravljanje nalog mora ta imeti ustrezno kadrovsko zasedbo in biti primerno opremljen – kriptološki laboratorij (prostor, strojna in programska oprema). V okviru Urada Vlade Republike Slovenije za varovanje tajnih podatkov mora biti zagotovljena tudi podpora upravnemu poslovanju.

Uvajanje novih kriptografskih rešitev mora potekati na podlagi predhodno opravljenega šifrirnega vrednotenja.

Trajnostno usposabljanje zaposlenih strokovnjakov na področju kriptologije.

Vključevanje strokovne in akademske javnosti v postopke vrednotenja kriptografskih rešitev.

Nosilec

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

Ukrepi za doseganje ciljnega stanja

Z ustrezno kadrovsko politiko (premestitve, dodatne zaposlitve) zagotoviti kadrovsko dopolnjenost. Zagotovitev ustreznega prostora in opreme.

Zagotoviti ustrezna finančna sredstva za izvajanje postopkov šifrirnih ovrednotenj.

Vključitev predstavnikov akademskih raziskovalnih institucij v medresorsko strokovno delovno skupino za komunikacijsko varnost.

Sklenitev sporazumov o sodelovanju na področju kriptografije med Uradom Republike Slovenije za varovanje tajnih podatkov in akademskimi raziskovalnimi institucijami.

Tveganja

Pomanjkanje ustreznega kadra in zagotavljanje finančnih virov.

Medresorska strokovna delovna skupina za komunikacijsko varnost opravlja svoje delo v okviru svojih možnosti (časovnih, kadrovskih in finančnih) in pomeni tveganje za učinkovito izvajanje postopkov šifrirnih ovrednotenj.

3.2 Spodbujanje razvoja in uporabe *kriptografskih* rešitev

Obstoječe stanje

Republika Slovenija ni zadostno prepoznana v domačem in mednarodnem okolju kot proizvajalka kriptografskih rešitev. Razvoj kriptografskih rešitev je nenačrten. V Republiki Sloveniji ni državnega organa, ki bi podpiral in financiral razvoj kriptografskih rešitev. Z uporabo tujih kriptografskih rešitev se zanemarja domače znanje in posledično ne spodbuja razvoja domačega gospodarstva. Slovenske kriptografske rešitve, ki so odobrene za varovanje nacionalnih tajnih podatkov, na tujih trgih niso prisotne. Urad Vlade Republike Slovenije za varovanje tajnih podatkov je pristojen za izvajanje postopkov šifrirnih ovrednotenj in je prepoznan v EU in zvezi NATO kot nacionalni varnostni organ Republike Slovenije.

Ciljno stanje

Uvrstitev Republike Slovenije na seznam proizvajalk kriptografskih rešitev.

Sodelovanje Urada Vlade Republike Slovenije za varovanje tajnih podatkov (organa za kriptografsko zaščito) pri razvoju kriptografskih rešitev za varovanje tajnih podatkov.

Domača podjetja, ki so sposobna razvijati lastne kriptografske rešitve za varovanje različnih vrst podatkov in e-storitev.

Vključitev domačih kriptografskih rešitev, ki so odobrene za varovanje nacionalnih tajnih podatkov, na seznam EU in NATO potrjenih kriptografskih rešitev.

Nosilec in deležniki

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov (nosilec),
- Ministrstvo za gospodarski razvoj in tehnologijo,
- Javna agencija Republike Slovenije za spodbujanje podjetništva, internacionalizacije, tujih investicij in tehnologije.

Kot vsebinski nosilci sodelujejo:
- Slovenska obveščevalno-varnostna agencija,
- Ministrstvo za obrambo,
- Ministrstvo za zunanje zadeve in
- Ministrstvo za javno upravo.

Ukrepi za doseganje ciljnega stanja

Republika Slovenija mora zagotavljati soudeležbo pri razvoju novih kriptografskih rešitev z inovativnimi javnimi naročili.

Republika Slovenija mora razviti sposobnost oblikovanja jasnih meril, ki omogočajo proizvajalcem razvijati kakovostne kriptografske rešitve in jih k temu jasno usmerjati.

Razvojni projekti se določajo na podlagi splošnih in posebnih potreb po kriptografskih rešitvah. Splošne potrebe so javno znane zahteve informacijske družbe. Posebne potrebe so zahteve državnih organov, ki jih koordinira Urad Vlade Republike Slovenije za varovanje tajnih podatkov. Javna agencija za raziskovalno dejavnost Republike Slovenije, Javne agencija Republike Slovenije za spodbujanje podjetništva, internacionalizacije, tujih investicij in tehnologije ter Urad Vlade Republike Slovenije za varovanje tajnih podatkov koordinirajo svoje aktivnosti s ciljem financiranja skupaj določenih razvojnih projektov na področju kriptologije.

Slovenska obveščevalno-varnostna agencija, Ministrstvo za obrambo, Ministrstvo za zunanje zadeve, Ministrstvo za javno upravo in Ministrstvo za notranje zadeve – Policija kot največji uporabniki kriptografskih rešitev in Urad Vlade Republike Slovenije za varovanje tajnih podatkov kot državni varnostni organ, pristojen za izvajanje šifrirnih vrednotenj, morajo v okviru svojih pristojnosti sodelovati pri pripravi inovativnih javnih naročil za nove kriptografske rešitve.

Javna agencija Republike Slovenije za spodbujanje podjetništva, internacionalizacije, tujih investicij in tehnologije v razvojne programe redno vključuje projekte, povezane z razvojem kriptografskih rešitev.

Urad Vlade Republike Slovenije za varovanje tajnih podatkov se določi kot pristojni organ za koordiniranje aktivnostih pri drugem šifrirnem ovrednotenju za pridobitev potrdila za varovanje tajnih podatkov EU.

Urad Vlade Republike Slovenije za varovanje tajnih podatkov in Ministrstvo za obrambo se določita kot pristojna organa za koordiniranje aktivnosti za pridobitev potrdila za varovanje tajnih podatkov NATO.

Urad Vlade Republike Slovenije za varovanje tajnih podatkov in Ministrstvo za obrambo ponudita domačim proizvajalcem kriptografskih rešitev možnost pridobitve potrdil za varovanje tajnih podatkov EU in NATO.

Tveganja

Neobstoj domačih kriptografskih rešitev pomeni veliko tveganje za nacionalno varnost Republike Slovenije.

Neobstoj aktivnosti države na področju kriptologije pomeni tveganje, da Republika Slovenija pride v stanje brez ustreznih kriptoloških strokovnjakov, ki so potrebni za razvoj novih kriptografskih rešitev.

Samostojen razvoj novih kriptografskih rešitev brez državne podpore predstavlja za posamezno podjetje tveganje za obstoj.

Pri šifrirnem ovrednotenju tujih kriptografskih rešitev se srečujemo s problemom možnosti seznanitve s ključnimi kriptografskimi mehanizmi, ker slednjih tuji proizvajalci oziroma pristojni organi držav proizvajalk niso pripravljeni razkriti zaradi zaščite lastnih interesov. Nepoznavanje kriptografskih mehanizmov, ki se uporabljajo v nacionalnih komunikacijsko informacijskih sistemih, lahko predstavlja veliko tveganje za nacionalno varnost Republike Slovenije.

Postopek drugega šifrirnega ovrednotenja pomeni tveganje saj ne zagotavlja, da se bo proces zaključil s potrditvijo predlagane kriptografskih rešitve za varovanje tajnih podatkov EU določene stopnje tajnosti.

Postopek šifrirnega ovrednotenja za pridobitev odobritve za varovanje tajnih podatkov zveze NATO pomeni tveganje in ne zagotavlja, da se bo tudi uspešno zaključil.

3.3 Zagotavljanje *kriptografskih* rešitev

Obstoječe stanje

V državni upravi se za šifriranje tajnih in drugih podatkov skoraj izključno uporabljajo različne tuje kriptografskih rešitve, kar je lahko varnostno tvegano. Odsotnost enotnega pristopa pri sprejemanju odločitev o izbiri posameznih kriptografskih rešitev se kaže v množici različnih rešitev in zaradi tega povečani finančni potratnosti (manjše količine raznovrstnih rešitev, vzdrževalne pogodbe) in večji obremenitvi strokovnega kadra zaradi skrbništva nad različnimi rešitvami.

Urad Vlade Republike Slovenije za varovanje tajnih podatkov vodi seznam odobrenih kriptografskih rešitev za varovanje prenosa tajnih podatkov za različne stopnje tajnosti.

Ciljno stanje

Uporaba potrjenih kriptografskih rešitev za varovanje prenosa vseh podatkov v komunikacijsko informacijskih sistemih državnih organov.

Omogočanje uporabe kriptografskih rešitev za varni prenos podatkov tudi v širšem okolju (banke, poslovni subjekti, kritična infrastruktura).

Nosilec in deležniki

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov (nosilec),
- Ministrstvo za obrambo,
- Slovenska obveščevalno-varnostna agencija,
- Ministrstvo za notranje zadeve,
- Ministrstvo za zunanje zadeve,
- Ministrstvo za javno upravo in
- Javna agencija Republike Slovenije za spodbujanje podjetništva, internacionalizacije, tujih investicij in tehnologije.

Ukrepi za doseganje ciljnega stanja

Urad Vlade Republike Slovenije za varovanje tajnih podatkov izvaja šifrirno vrednotenje kriptografskih rešitev in objavlja seznam odobrenih kriptografskih rešitev na svoji spletni strani.

Urad Vlade Republike Slovenije za varovanje tajnih podatkov ob sodelovanju drugih deležnikov koordinira in promovira uporabo kriptografskih rešitev za zagotavljanje varnih storitev v kibernetskem prostoru.

Državni organi (nosilci in deležniki) sodelujejo pri razvoju in izvedbi končnih kriptografskih rešitev za prenos tajnih podatkov za potrebe drugih državnih organov. Urad Vlade Republike Slovenije za varovanje tajnih podatkov koordinira postopke z zunanjim izvajalcem.

Izvajanje promocije uporabe kriptografskih rešitev v drugih panogah, kot so bančni sektor, zavarovalništvo itd.

Javna agencija Republike Slovenije za spodbujanje podjetništva, internacionalizacije, tujih investicij in tehnologije nudi pomoč domačim podjetjem na javnih razpisih za črpanje evropskih sredstev za razvoj in proizvodnjo kriptografskih rešitev.

Tveganja

Brez razvoja in proizvodnje domačih kriptografskih rešitev nimamo lastnih produktov za varovanje prenosa podatkov po komunikacijsko informacijskih sistemih in posledično zaupamo varnost nacionalnih podatkov izključno tujim kriptografskim rešitvam oziroma drugim državam.

Pri vsaki kriptografskih rešitvi, ki je ni mogoče do najmanjše podrobnosti preučiti, obstaja tveganje, da uporablja neustrezne kriptografske mehanizme ali ima celo vgrajena stranska vrata za prestrezanje podatkov.
Ker ni domačih kriptografskih rešitev, je onemogočeno ustvarjanje dodane vrednosti.

3.4 Raziskovanje na področju kriptologije

Obstoječe stanje

V Republiki Sloveniji so aktivne številne programske skupine, vendar med njimi ni nobene, ki bi delovala izključno na področju kriptologije. V preteklosti je nekatere raziskovalne projekte s področja kriptologije financirala država (Javna agencija za raziskovalno dejavnost Republike Slovenije, Ministrstvo za obrambo in Slovenska obveščevalno-varnostna agencija).

Ciljno stanje

Spodbujanje in državno sofinanciranje razvojnih projektov na področju kriptologije.

Nosilec in deležniki

- Javna agencija za raziskovalno dejavnost Republike Slovenije (nosilec),
- Ministrstvo za izobraževanje, znanost in šport,
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in
- akademska raziskovalna sfera.

Ukrepi za doseganje ciljnega stanja

Javna agencija za raziskovalno dejavnost Republike Slovenije, ki opravlja strokovne, razvojne in izvršilne naloge v zvezi z izvajanjem sprejete raziskovalne in inovacijske strategije Slovenije v okviru veljavnega proračunskega memoranduma in državnega proračuna ter druge naloge pospeševanja raziskovalne dejavnosti, v skladu z namenom ustanovitve skupaj z Uradom Vlade Republike Slovenije za varovanje tajnih podatkov vključi projekte s področja kriptologije v svoje delovanje v okviru ciljnih raziskovalnih programov.

Tveganja

Pri potrjevanju razvojnih projektov za kriptologijo obstaja tveganje, da predlagatelj projekta nima namena delovati na področju kriptologije.

Pri določitvi razvojnih projektov za kriptologijo obstaja tveganje, da se delo preusmeri na druga področja.

3.5 Usposabljanje uporabnikov *kriptografskih* rešitev

Obstoječe stanje

Zaradi nizke splošne varnostne kulture, ki se kaže v odnosu posameznikov, skupin ter tudi organizacij in državnih organov do zaščite in varovanja podatkov ter pomena dojemanja varnosti, je uporaba kriptografskih rešitev v komunikacijsko-informacijskih sistemih omejena le na ozek krog varnostnih struktur, širše pa je popolnoma neurejena. Primeri prisluškovanja visokim uradnikom najbolj nazorno kažejo na pomanjkljivosti tudi v ožjem delu državne uprave.

Ciljno stanje

Za primerno uporabo varnostnih elementov je ključno zavedanje uporabnikov o pomembnosti šifriranja podatkov in poznavanja osnov delovanja in uporabe kriptografskih sistemov ter pogostih napadov na sisteme in omrežja. Pomembna sta tudi poznavanje in prepoznavanje groženj in ranljivosti v informacijskih in komunikacijskih sistemih.

Nosilec in deležniki

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov (nosilec),
- vsi državni organi
- vsi organi javne uprave.

Ukrepi za doseganje ciljnega stanja

Oblikovanje in izvajanje programa varnostnega ozaveščanja.

Vključevanje elementov s področja varnega komuniciranja in obravnave podatkov v program usposabljanja novo zaposlenih delavcev.

Vključevanje elementov kriptografije v obstoječe in nove programe usposabljanja na področju informacijske družbe.

Tveganja

Brez primernega usposabljanja se bo varnostno stanje skokoma poslabševalo.

Ohranjevalo se bo mišljenje posameznikov in družbe, da je varna obravnava in izmenjava podatkov nepotrebna in je namenjena le prikrivanju nepravilnosti v delovanju državne uprave.

3.6 Zagotavljanje kadrovskih virov

3.6.1 Podeljevanje štipendij za področje kriptologije

Obstoječe stanje

Sedanji sistem štipendiranja ne predvideva posebnih štipendij na področju kriptologije.

Ciljno stanje

Republika Slovenija na letni ravni štipendira študente s področja kriptologije na prvi in drugi bolonjski stopnji izobraževanja. Zainteresiranim diplomantom druge bolonjske stopnje izobraževanja se omogoči napotitev na doktorski študij, ki vključuje vsebine kriptologije. Na ta način bi lahko usposabljanje povezali s katerim od raziskovalnih projektov s področja kriptologije.

Nosilec in deležniki

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov (nosilec),
- Ministrstvo za javno upravo,
- Ministrstvo za obrambo,
- Ministrstvo za gospodarski razvoj in tehnologijo,
- Ministrstvo za notranje zadeve,
- Ministrstvo za zunanje zadeve in
- Slovenska obveščevalno-varnostna agencija.

Ukrepi za doseganje ciljnega stanja

Vlaganje v izobraževanje kriptološkega kadra.

Nosilci in deležniki določijo merila za pridobitev štipendij.

Ustrezno kadrovsko politiko mora zagotoviti delodajalec, pri tem je potrebno upoštevati dodeljene kvote v Skupnem kadrovskem načrtu ter zagotoviti finančna sredstva za morebitne nove zaposlitve.

Tveganja

Brez štipendiranja področja kriptologije tvegamo dolgoročno pomanjkanje ustreznega kadra za razvoj in proizvodnjo kriptografskih rešitev.

Brez zagotavljanja novih kadrov na področju kriptologije je tvegano uresničevanje strategije.

3.6.2 Zaposlovanje kriptoloških strokovnjakov

Obstoječe stanje

Sedanji kadrovski sistem javnega sektorja nima opredeljenega področja zaposlovanja kriptoloških strokovnjakov.

Ciljno stanje

Povečati pretok kriptološkega znanja med javnim sektorjem, izobraževalnimi in raziskovalnimi ustanovami ter gospodarstvom in s tem podpreti javno-zasebno partnerstvo.

Nosilec in deležniki

- Ministrstvo za javno upravo (nosilec),
- Ministrstvo za obrambo,
- Ministrstvo za gospodarski razvoj in tehnologijo,
- Ministrstvo za notranje zadeve,
- Ministrstvo za zunanje zadeve,
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in
- Slovenska obveščevalno-varnostna agencija.

Ukrepi za doseganje ciljnega stanja

Za uresničevanje strategije je treba omogočiti zaposlovanje strokovnjakov s področja kriptologije.

Ministrstvo za obrambo, Slovenska obveščevalno-varnostna agencija, Ministrstvo za notranje zadeve, Ministrstvo za javno upravo in Ministrstvo za zunanje zadeve kot največji uporabniki kriptografskih rešitev morajo sodelovati z izobraževalnimi ustanovami pri pridobivanju kadra s področja kriptologije.

Nosilci in deležniki v sistemizaciji delovnih mest (njihovih organov) na področju informacijske varnosti kot pogoj določijo izobrazbo s področja kriptologije.

Tveganja

Brez vzpostavljenih primernih razmer za zaposlovanje kriptoloških strokovnjakov je tvegano uresničevanje Strategije kriptografske zaščite podatkov v Republiki Sloveniji.

Brez vzpostavljenih primernih razmer za zaposlovanje kriptoloških strokovnjakov tvegamo odhod visoko strokovnega kadra v tujino.

4. Načrt uresničevanja strategije

4.1 Viri financiranja

Predviden vir financiranja je državni proračun Republike Slovenije, v primerih skupnih projektov pa tudi sofinanciranje podjetij.

Predvideni letni odhodki v ocenjeni višini 500.000 EUR bodo namenjeni sredstvom za plače novo zaposlenih strokovnjakov, materialnim stroškom, plačilu strokovnega sodelovanja z akademsko-raziskovalnimi institucijami, vzpostavitvi nacionalnega kriptografskega laboratorija, usposabljanju izvajalcev in uporabnikom programa varnostnega ozaveščanja ter štipendiranju.

4.2 Sodelovanje z deležniki in izvajanje strategije

Odgovorni nosilci in deležniki za izvedbo strategije kriptografske zaščite podatkov oblikujejo skupni akcijski načrt za posamezne cilje v roku enega leta od sprejetja strategije.

V akcijskem načrtu bodo podrobneje opredeljeni časovni okvir za izvedbo ciljev in načini ter viri financiranja.

4.3 Spremljanje in vrednotenje izvajanja strategije

Urad Vlade Republike Slovenije za varovanje tajnih podatkov je zadolžen za spremljanje izvajanja Strategije kriptografske zaščite podatkov v Republiki Sloveniji. Za pridobivanje podatkov o izobraževanju na področju kriptologije sodeluje s slovenskimi univerzami. Raziskovalno aktivnost na področju kriptologije spremlja Javna agencija za raziskovalno dejavnost Republike Slovenije. Javna agencija Republike Slovenije za spodbujanje podjetništva, internacionalizacije, tujih investicij in tehnologije spremlja vključenost domače industrije v razvoj in proizvodnjo kriptografskih rešitev.

Za dosego posameznih ciljev so zadolženi njihovi nosilci, ki izvajajo potrebne aktivnosti in na svojem področju opravljajo nadzor nad opravljenim delom. Posamezni nosilci o doseženem napredku vsakih šest mesecev poročajo Uradu Vlade Republike Slovenije za varovanje tajnih podatkov.

5. Pozitivni učinki uresničevanja strategije

Uresničevanje strategije bi imelo naslednje pozitivne učinke:

- prepoznavnost Republike Slovenije v domačem in mednarodnem okolju kot proizvajalke kriptografskih rešitev in uvrstitev na seznam držav proizvajalk kriptografskih rešitev,
- promocija domačega znanja in posledično spodbujanje razvoja domačega gospodarstva,
- načrtni razvoj nacionalni kriptografskih rešitev,
- obvezna uporaba kriptografskih rešitev za varovanje prenosa vseh podatkov v komunikacijsko-informacijskih sistemih državnih organov,
- spodbujanje uporabe kriptografskih rešitev za varni prenos podatkov tudi v širšem okolju (banke, poslovni subjekti, kritična infrastruktura),
- spodbujanje domačega gospodarstva za proizvodnjo in s tem vključitev domačih kriptografskih rešitev, ki so odobrene za varovanje nacionalnih tajnih podatkov, na seznam potrjenih kriptografskih rešitev EU in NATO,
- spodbujanje in državno sofinanciranje razvojnih projektov na področju kriptologije,
- zavedanje uporabnikov o pomembnosti šifriranja podatkov in poznavanja osnov delovanja in uporabe kriptografskih sistemov ter pogostih napadov na sisteme in omrežja,
- poznavanje in prepoznavanje groženj in ranljivosti v informacijskih in komunikacijskih sistemih,
- vključevanje elementov kriptografije v obstoječe in nove programe na področju informacijske družbe.