REPUBLIKA SLOVENIJA
VLADA REPUBLIKE SLOVENIJE

Gregorčičeva 20–25, SI-1001 Ljubljana

T: +386 1 478 1000
F: +386 1 478 1607
E: gp.gs@gov.si
http://www.vlada.si/

DRŽAVNI ZBOR REPUBLIKE SLOVENIJE
Prejeto: 02 -12- 2016
Šifra: 020-07/16-1353/3
Povezava: 011-04/16-28
EPA: EU:
Sign. zn.:
Kratica:

Predsednik Državnega zbora

Številka: 00104-249/2016/6
Datum: 1. 12. 2016
Zveza: dopis št.: 020-07/16-1353/2 z dne 7. 11. 2016

Na podlagi 249. člena Poslovnika državnega zbora (Uradni list RS, 92/07 – uradno prečiščeno besedilo, 105/10 in 80/13) vam pošiljam:

– Odgovor na poslansko vprašanje Branka Grimsa v zvezi z izsiljevanjem spletnih uporabnikov,

ki ga je Vlada Republike Slovenije sprejela na 112. redni seji dne 1. 12. 2016.

Mag. Lilijana Kozlovič
generalna sekretarka

Priloga: 1

Podpisnik: Lilijana Kozlovič
Izdajatelj: Republika Slovenija
Številka certifikata: 76 32 9e c4 (

REPUBLIKA SLOVENIJA
VLADA REPUBLIKE SLOVENIJE

Gregorčičeva 20–25, SI-1001 Ljubljana

T: +386 1 478 1000
F: +386 1 478 1607
E: gp.gs@gov.si
http://www.vlada.si/

Številka: 00104-249/2016/5
Datum: 1. 12. 2016

Odgovor na poslansko vprašanje Branka Grimsa v zvezi z izsiljevanjem spletnih uporabnikov

Predsednik Državnega zbora Republike Slovenije, dr. Milan Brglez, je dne 7. 11. 2016 na Vlado Republike Slovenije (v nadaljevanju: Vlada RS) posredoval pisno poslansko vprašanje poslanca Branka Grimsa v zvezi z izsiljevanjem spletnih uporabnikov. Poslanec je na Vlado RS naslovil naslednje vprašanje: »Kako bo Vlada Republike Slovenije ukrepala, da bo zaščitila podjetja in zasebne uporabnike pred izsiljevanjem na spletu?«

V nadaljevanju Vlada RS posreduje odgovor na zastavljeno poslansko vprašanje.

V procesu digitalizacije družbe, ki jo zaznamuje izjemen razmah interneta, mobilnih tehnologij, družbenih omrežij, računalništva v oblaku, lokacijskih storitev, masovnih podatkov ter zbiranje in obdelava osebnih podatkov, vedno bolj do izraza prihajajo tudi negativni pojavi, povezani s spletnim kriminalom. Pri tem so se v zadnjem času še posebej razširili različni izsiljevalski virusi (ransomware), ki zaklenejo podatke na okuženih računalnikih. Za vnovičen dostop do podatkov spletni kriminalci od uporabnikov zahtevajo precejšnja plačila v valuti Bitcoin. Tudi plačilo take odkupnine uporabnikom še ne zagotavlja, da bodo res lahko prišli do svojih podatkov. Transakcije z Bitcoini so praktično neizsledljive, zato je zelo oteženo delo organov pregona pri reševanju takih primerov. Čeprav so v primerih nekaterih izsiljevalskih virusov varnostna podjetja, ki se ukvarjajo z antivirusno programsko opremo, uspela pripraviti orodja, ki odklenejo podatke na okuženih računalnikih, pa je marsikateri uporabnik, predvsem pa podjetje, plačalo kriminalcem, da so lahko hitro prišli do svojih podatkov, saj bi bilo v nasprotnem primeru lahko ogroženo njihovo poslovanje. Na žalost pri izsiljevalskih virusih zaradi njihove raznolikosti in kompleksnosti ni mogoče pričakovati, da bodo hitro na voljo ustrezna orodja za pomoč. To je dejstvo, ki velja za ves svet in ne le za Slovenijo.

Uvrstitev Slovenije na visoko mesto v raziskavi podjetja Kaspersky Lab je lahko posledica različnih vzrokov. Prvi je lahko že ta, da ima antivirusna programska oprema omenjenega proizvajalca visok tržni delež v Sloveniji in je tako tudi zaznava okužb višja. Drug vzrok pa je lahko tudi prenizka ozaveščenost in obveščenost o nevarnostih izsiljevalskih virusov ter s tem povezano slabo samozaščitno ravnanje uporabnikov. Ne glede na vzrok za slabo stanje na področju izsiljevalskih virusov v Sloveniji je za njihovo zajezitev še vedno najbolj učinkovito preventivno delovanje z ozaveščanjem uporabnikov o možnih spletnih nevarnostih. Tukaj je mišljena predvsem izredna previdnost pri odpiranju priponk elektronske pošte neznanih pošiljateljev, obiski sumljivih spletnih strani ali uporaba piratske programske opreme.

Na področju ozaveščanja v Sloveniji potekata dva projekta. Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT) od leta 2011 izvaja nacionalni program ozaveščanja in izobraževanja Varni na internetu[1]. Ključni cilj projekta, ki je namenjen najširši slovenski javnosti, poseben sklop vsebin pa tudi malim

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

podjetjem, obrtnikom in samostojnim podjetnikom, je dvig stopnje informiranosti o varni rabi interneta. Projekt, ki ga financira Ministrstvo za javno upravo, 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[2], financirata pa ga Generalni direktorat Connect pri Evropski komisiji in Ministrstvo za javno upravo, se izvajajo programi SAFE.SI[3], 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.

V preteklosti so na SI-CERT skupaj s slovensko policijo in Uradom RS za preprečevanje pranja denarja na podlagi njihove analize uspeli identificirati avtorja računalniškega virusa, s katerim je slovenski kriminalni združbi v šestih mesecih uspela kraja 1,8 mio EUR iz računov okoli petdesetih slovenskih podjetij.

V letih 2012 do 2016 so prejeli več kot tisoč prijav izsiljevalskih virusov z zahtevanimi odkupninami v višini po okoli 500 EUR. Brez primernega odzivanja na SI-CERT in obveščanja javnosti bi škoda presegla 500.000 EUR.

Januarja 2015 je potekal dolgotrajni sofisticiran napad na komitente šestih bank v Sloveniji. Storilci so poslali preko 100.000 sporočil, oškodovanja komitentov pa so ocenjena na 100.000 EUR v zgolj tednu dni. Če ne bi na SI-CERT v sodelovanju s prizadetimi bankami poskrbeli za takojšen odziv, bi bila oškodovanja gotovo nekajkrat večja.

Vlada Republike Slovenije je letos februarja sprejela Strategijo kibernetske varnosti, ki vsebuje ukrepe za sistemsko ureditev področja in predvsem okrepitev nacionalnega sistema zagotavljanja kibernetske varnosti. Država bo vzpostavila nacionalni organ za kibernetsko varnost na strateški ravni sistema, ki bo povezal in koordiniral vse zmogljivosti na operativni ravni sistema ter bo hkrati enotna kontaktna točka za mednarodno sodelovanje na področju kibernetske varnosti. Prav tako bo okrepljena operativna raven sistema s prepotrebno okrepitvijo SI-CERT, ki se bo tako lahko še bolje odzival na kibernetske grožnje slovenskim državljanom in podjetjem ter vzpostavitvijo vladnega odzivnega centra (SIGOV-CERT) za računalniška omrežja v javnem sektorju. SI-CERT aktivno sodeluje pri vzpostavitvi vseevropskega omrežja zaupanja, v katerem sodelujejo nacionalni CERT-i, ki si bodo tako lahko hitreje in učinkoviteje izmenjevali informacije o kibernetskih grožnjah in primernih odzivih nanje. Prav tako je načrtovana tudi okrepitev programov ozaveščanja ter uvedba področja kibernetske varnosti v izobraževalne programe na vseh ravneh izobraževalnega sistema. Namen vseh teh ukrepov je zagotoviti boljšo ozaveščenost celotne populacije, s tem pa tudi zajezitev izsiljevalskih virusov v Sloveniji.

V bližnji prihodnosti bo Slovenija v svoj pravni red morala prenesti direktivo o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji (NIS direktivo), katere uresničitev bo od države zahtevala tudi znatno večje vlaganje v nacionalni sistem kibernetske varnosti. Glede na izredno pomembnost zagotavljanja kibernetske varnosti za življenje in

---

[2] Mladinsko informativno svetovalno središče Slovenije.
[3] http://safe.si/

delovanje posameznikov, podjetij in celotne družbe, bo pri pridobivanju podpore za zagotovitev potrebnih sredstev zelo dobrodošla tudi podpora poslank in poslancev Državnega zbora Republike Slovenije.