REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST
URSIV

INTERNATIONAL COUNTER RANSOMWARE INITIATIVE
CRI

Smernice za organizacije ob incidentih z izsiljevalsko programsko opremo

Maj 2026

Uvodna izjava

1. Članice Mednarodne pobude za boj proti izsiljevalski programski opremi (ang. Counter Ransomware Initiative - CRI) v sodelovanju z zavarovalniškimi združenji izdajajo smernice za organizacije, ki so postale žrtve napada z izsiljevalsko programsko opremo (ang. ransomware), ter za partnerske organizacije, ki jim pri tem nudijo podporo[1].

2. Plačilo odkupnine praviloma spodbuja poslovni model izsiljevalske programske opreme. Leto 2023 je bilo globalno najslabše leto doslej glede na skupni znesek plačanih odkupnin[2].

3. Izsiljevalska programska oprema predstavlja kompleksen in čezmejni problem, ki zahteva tesno mednarodno sodelovanje. Na 3. združenju CRI Summit leta 2023 je bila sprejeta izjava[3], ki močno odsvetuje plačevanje odkupnin. V izjavi je bilo poudarjeno, da plačilo odkupnine:

- ne zagotavlja konca incidenta niti odstranitve zlonamerne programske opreme iz sistemov,
- spodbuja kriminalce k nadaljevanju in širjenju njihovih dejavnosti,
- kriminalnim združbam zagotavlja sredstva za nadaljnje nezakonite aktivnosti,
- ne zagotavlja, da bodo podatki dejansko povrnjeni.

4. Te smernice niso pravno zavezujoče in ne prevladajo nad veljavno zakonodajo ali regulativnimi zahtevami v posameznih članicah CRI. Končna odločitev o plačilu odkupnine je vedno v rokah napadene organizacije. Kadar žrtev razmišlja o plačilu zahteve po odkupnini in je takšno plačilo zakonito, zavarovanje žrtvi ne preprečuje izvedbe plačila. Kadar je mogoče, je priporočljivo že v zgodnji fazi vključiti strokovnjake.

5. Ko organizacija postane žrtev izsiljevalskega napada, je odločitev o tem, ali odkupnino plačati ali ne, pogosto zelo zahtevna. CRI je zato pripravila smernice, ki organizacijam nudijo celovit pregled korakov, ki jih je smiselno preučiti, preden sploh razmišljajo o plačilu. Smernice vključujejo tudi pregled možnih negativnih posledic plačila.

1 Dokument je prevod dokumenta, ki so ga pripravile partnerske države znotraj iniciative CRI.

2 Izsiljevalska programska oprema je leta 2023 povzročila za 1 milijardo dolarjev škode (chainalysis.com)

3 Skupna izjava pobude CRI o plačilih izsiljevalske programske opreme – GOV.UK (www.gov.uk)

6. Cilj teh smernic je zmanjšati celotni vpliv izsiljevalskega napada na organizacijo ter prispevati k:

- zmanjšanju motenj poslovanja in stroškov za podjetja,
- zmanjšanju števila plačanih odkupnin,
- zmanjšanju višine odkupnin v primerih, ko se organizacije kljub vsemu odločijo za plačilo.

7. Kibernetsko zavarovanje predstavlja pomemben del upravljanja tveganj. Članice CRI priznavajo pomembno vlogo kibernetskega zavarovanja pri krepitvi odpornosti organizacij proti kibernetskim napadom, tudi z vidika izboljševanja zaščitnih ukrepov. Članice CRI in zavarovalniška združenja bodo sodelovala pri nadaljnji krepitvi vloge komercialnega kibernetskega zavarovanja pri zaščiti organizacij pred izsiljevalskimi napadi.

8. CRI in zavarovalniška združenja priporočajo, da organizacije pred končno odločitvijo o morebitnem plačilu odkupnine temeljito preučijo spodnje smernice.

Smernice za organizacije ob incidentih z izsiljevalsko programsko opremo

1. Organizacijam se priporoča, da se na izsiljevalske napade pripravijo vnaprej, kot del načrtov neprekinjenega poslovanja, ter pravočasno razvijejo politike, postopke, okvire delovanja in komunikacijske načrte.

Upoštevanje pravnih in regulativnih zahtev glede plačila in poročanja

2. Pred morebitnim plačilom odkupnine morajo organizacije upoštevati pravne in regulatorne vidike, pri čemer lahko strokovnjaki, kot so zavarovalnice, nudijo ustrezna pojasnila in usmeritve.

3. V določenih primerih plačilo morda ni zakonito, na primer kadar bi bila odkupnina plačana subjektu, ki je uvrščen na seznam sankcioniranih oseb ali organizacij.

4. Organizacije morajo upoštevati lokalno zakonodajo in druge veljavne predpise v vseh državah, kjer poslujejo, ter – kadar je to potrebno in primerno – incident v najkrajšem možnem času prijaviti pristojnemu organu.

5. Pri tem morajo organizacije oceniti morebitne pravne in regulativne obveznosti, vključno z:

- obveznostmi poročanja ali obveščanja državnih organov, organov pregona, pogodbenih partnerjev, posameznikov ali drugih relevantnih deležnikov,
- ugotavljanjem, ali je plačilo napadalcu pravno dopustno.

Prijava incidenta pristojnim organom

6. Prijava incidenta pristojnim organom lahko žrtvam bistveno pomaga. Organom omogoča, da nudijo ustrezne nasvete in podporo, hkrati pa krepi odpornost organizacij in zmanjšuje tveganje prihodnjih napadov. Pravočasna prijava napada in morebitnega plačila je pomembna tudi za pristojne organe, kot so organi pregona, saj jim omogoča učinkovitejše preiskave in zbiranje dokazov za preprečevanje delovanja akterjev v prihodnje ter boljše razumevanje tovrstnih kriminalnih operacij.. To pristojnim organom omogoča učinkovitejšo podporo prihodnjim žrtvam in lahko prispeva k preprečevanju prihodnjih napadov, tudi z izsleditvijo ter kazenskim pregonom odgovornih oseb.

Celovita presoja vseh možnosti

7. Neposredno po napadu je situacija pogosto zelo stresna. Napadalci poznajo taktike pritiska in poskušajo žrtve prisiliti v hitre odločitve. Zavestna odločitev za umirjen pregled vseh možnosti lahko vodi do boljših odločitev in ugodnejšega izida.

8. Skrbni pregled dejstev, zbiranje informacij in analiza možnih posledic morajo biti del vsakega načrta odzivanja na incidente. Tak pristop omogoča:

- da se ne spregledajo ključne informacije,
- na podatkih utemeljeno odločitev o tem, ali plačati ali ne,
- izpolnjevanje zakonskih obveznosti, kot je poročanje o incidentu.

Vključevanje strokovnjakov

9. Kadar je mogoče, je smiselno vključiti zunanje strokovnjake, kot so zavarovalnice, nacionalni tehnični organi, organi pregona ali podjetja za odzivanje na kibernetske incidente (CIR). Njihove izkušnje lahko pomembno izboljšajo kakovost odločanja. Zavarovalnice pogosto priporočijo specializirana podjetja za odzivanje na incidente. Če ima organizacija kibernetsko zavarovanje, mora ravnati v skladu z določili zavarovalne police glede poročanja.

Preučitev alternativ plačilu odkupnine

10. V skladu s skupno izjavo CRI iz leta 2023 se organizacijam praviloma močno odsvetuje plačilo odkupnine.

11. Kljub temu pa lahko v skladu z lokalno zakonodajo pride do primerov, ko organizacija o plačilu vseeno razmišlja. V takih primerih se priporoča posvet z zavarovalnicami ali drugimi specializiranimi strokovnjaki.

12. Odločitev mora temeljiti na čim bolj celovitem razumevanju dejanskega vpliva incidenta in realni presoji, ali bi plačilo spremenilo izid ali ne. Napadalci pogosto trdijo, da je plačilo edina možnost za obnovo, kljub znanim tveganjem in negativnim posledicam.

Zbiranje informacij za oceno vpliva in pravnih obveznosti

13. Organizacijam se priporoča, da:

14. Ocenijo tehnično stanje, vključno z razpoložljivostjo varnostnih kopij, možnostmi pridobitve dešifrirnih ključev iz drugih virov ter časom, potrebnim za obnovo delovanja po dešifriranju. Orodja so lahko na voljo prek podjetij za kibernetsko varnost, organov pregona, projektov, kot je »No More Ransom«, ali drugih komercialnih in odprtokodnih rešitev.

15. Uvedejo začasne rešitve za zmanjševanje motenj poslovanja in ocenijo, kako dolgo jih je mogoče vzdrževati. Ocenijo naj vpliv na delovanje sistemov, poslovne procese, stranke in zaposlene, vključno z morebitnimi posrednimi vplivi na dobavno verigo, ter tveganje nadaljnjega odtekanja podatkov.

Ocena vpliva incidenta

16. Sprejetje ukrepov za oceno posledic incidenta organizacijam omogoča boljšo pripravljenost in učinkovitejše razprave glede zavarovalnega kritja. Pomembno je poudariti, da lahko nekateri stroški – kot so obveščanje prizadetih posameznikov, regulativne kazni zaradi neustreznega varovanja podatkov in drugi stroški – nastanejo že zaradi odtujitve podatkov med izsiljevalskim napadom, ne glede na to, ali so podatki pozneje dejansko objavljeni. Zato je treba vpliv teh stroškov obravnavati ločeno od odločitve o morebitnem plačilu odkupnine.

Dejavniki, ki lahko vplivajo na odločitev o plačilu zahtevane odkupnine, lahko vključujejo:

- preveritev obstoječega zavarovalnega kritja;
- oceno izgube prihodkov zaradi prekinitve poslovanja, izvedbe varnostnih izboljšav, nadurnega dela zaposlenih, pravnih stroškov ali regulativnih kazni;
- ugotavljanje morebitno odtujenih podatkov ali intelektualne lastnine ter oceno morebitne škode za organizacijo, stranke in uporabnike, če bi bili odtujeni podatki javno razkriti.

17. V skoraj vseh sodobnih izsiljevalskih napadih napadalci poleg šifriranja tudi odtujijo podatke. Zato žrtve ne smejo zaupati obljubam, da bodo podatki po plačilu izbrisani. Priporočljivo je natančno oceniti, kateri podatki so bili kompromitirani in kako občutljivi so. Pravna pomoč je pomembna za zagotavljanje skladnosti z zakonodajo ter za pravilno komunikacijo s pristojnimi organi. Organizacije morajo oceniti tudi morebitna tveganja za življenje, osebne podatke ali nacionalno varnost v primeru objave podatkov. Smiselno je preveriti resničnost trditev napadalcev glede količine in vrste odtujenih podatkov.

Dokumentiranje odločitev

18. Natančno beleženje poteka odziva, sprejetih odločitev, izvedenih ukrepov ter razpoložljivih ali manjkajočih podatkov je ključno za kasnejšo analizo, učenje in morebitne regulativne postopke. Med incidentom je priporočljivo odločanje dokumentirati na sistemih, ki niso prizadeti, ali povsem izven digitalnega okolja.

19. Namen tega je: zagotoviti sledljivost odločitev, omogočiti jasna in utemeljena pojasnila, zmanjšati tveganje ponovitve napada.

20. Pristopi se lahko razlikujejo glede na jurisdikcijo, saj se pravni sistemi, regulativni postopki in notranje zahteve organizacij razlikujejo.

V odločitve vključite vse potrebne deležnike v organizaciji, vključno s tehničnim osebjem in višjim vodstvom oziroma ključnimi odločevalci.

21. Odločanje o plačilu odkupnine hitro vključi najvišje vodstvo. Kljub temu je pomembno, da se odločitvene možnosti ne predstavijo prehitro in da so podprte z najmočnejšimi možnimi dokazi.

Zavedanje, da plačilo ne zagotavlja povrnitve dostopa

22. Tudi če organizacija pridobi dešifrirni ključ, to redko pomeni takojšnjo vrnitev v normalno delovanje. Dešifriranje kompleksnih omrežij je lahko dolgotrajno. V določenih primerih je ob razpoložljivih varnostnih kopijah hitrejša obnova iz teh kopij.

23. Plačilo prav tako ne zagotavlja konca incidenta. Sistem, obnovljen iz varnostne kopije ali po dešifriranju, ni nujno varen. Varnostne kopije so lahko kompromitirane, napadalci pa lahko namenoma pustijo odprta vrata za prihodnje napade.

24. Pomembno je upoštevati tudi, da zlonamerni akterji morda ne bodo izpolnili obljub o izbrisu odtujenih podatkov ter da praviloma ne boste imeli možnosti preveriti, ali so bili odtujeni podatki dejansko izbrisani.

Ocena po incidentu: preiskava temeljnega vzroka incidenta in izvedba potrebnih ukrepov za preprečitev ponovnega napada

25. Plačilo odkupnine brez razjasnitve prvotnega vzroka kompromitacije in izvedbe ustreznih ukrepov za zmanjšanje tveganj organizacijo izpostavlja nadaljnjim incidentom. Organizacije bi morale neodvisno preveriti, kako je prišlo do kompromitacije.

26. Organizacije bi morale oceniti, ali so bile odpravljene vse ranljivosti, povezane z začetnim vdorom. Ugotavljanje načina kompromitacije organizacijam pomaga okrepiti obrambo pred prihodnjimi izsiljevalskimi napadi. To vključuje izvajanje preventivnih ukrepov in ukrepov za zmanjševanje tveganj, kot so upravljanje poverilnic, ločevanje in segmentacija omrežij ter vzpostavitev varnostnih kopij brez povezave oziroma ločenih od omrežja.