REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST
URSIV

Priporočila s področja kibernetske in informacijske varnosti političnim strankam in kandidatom za varno izvedbo volitev v Državni zbor Republike Slovenije 2026

Številka: 041-2/2025-1544-19
Datum: 4. 2. 2026

Uvod

Sodobne volitve vse bolj temeljijo na digitalnih tehnologijah - od elektronske pošte in družbenih medijev do sistemov za upravljanje kampanj in podatkovnih baz podpornikov. Čeprav te tehnologije omogočajo učinkovitejše kampanje in boljšo komunikacijo z volivci, hkrati odpirajo kibernetska tveganja, ki jih lahko zlorabijo zlonamerni akterji.

Kibernetske grožnje volilnim procesom predstavljajo novo realnost. V zadnjih letih smo bili priča številnim primerom kibernetskih zlonamernih aktivnosti, usmerjenih na politične stranke, kandidate in volilno infrastrukturo po vsem svetu.

V letu 2025 je nekaj evropskih držav (Poljska, Hrvaška, Romunija, Portugalska, Nemčija, Danska, Moldavija) izvedlo volitve, pri čemer je bilo več držav soočenih z zlonamernimi dejanji, s katerimi so akterji poskušali spodkopati volilni proces in vplivati na odločitve volivcev ter s tem omajati zaupanje v rezultat volitev. Različni akterji so z zlonamernimi kibernetskimi aktivnostmi in dezinformacijskimi kampanjami na družbenih omrežjih poskušali vplivati na volitve v Moldaviji, na Poljskem, v Romuniji in na Danskem.

Države so poročale o številnih porazdeljenih napadih onemogočanja delovanja (ang. DDoS), katerih tarča so bili tako informacijski sistemi, ki so bili v podporo volilnim opravilom, kot tudi spletne strani različnih subjektov udeleženih v volilnem procesu (državni organi, centralne in okrajne volilne komisije, politične stranke, medijske hiše in informacijski sistemi subjektov kritične infrastrukture). Poleg DDoS napadov so beležili poskuse vdorov v različne uradne spletne strani (npr. v Moldaviji), kjer so s pomočjo vrivanja zlonamerne kode (SQL injection) poskušali pridobiti dostop do spletnih strežnikov in v njem zbranih podatkov.

Ta zlonamerna dejanja pogosto izvajajo državni akterji, kriminalne skupine ali politični konkurenti z namenom:

- kraje občutljivih informacij in notranjih dokumentov,
- motenja volilnih kampanj,
- širjenja dezinformacij,
- spodkopavanja zaupanja v demokratične procese.

Politične stranke in kandidati so še posebej ranljivi, saj pogosto:

- nimajo zadostnih tehničnih virov za zaščito,
- zaposlujejo začasno osebje brez ustrezne usposobljenosti na področju kibernetske varnosti,
- uporabljajo osebne naprave za službene namene,
- delujejo v hitrem, visokonapetostnem okolju, kjer lahko varnost pade v ozadje.

Namen tega dokumenta je zagotoviti jasna in izvedljiva priporočila, ki političnim strankam in njihovim kandidatom lahko pomagajo zaščititi kampanjo, ugled in zagotoviti demokratični proces vseh volilnih aktivnosti.

Ključna tveganja

Ribarjenje za podatki ali zvabljanje (angl. Phishing) in socialni inženiring

Tveganje: Zlonamerni akterji pošiljajo elektronska sporočila, ki lažno izkazujejo, da so od zaupanja vrednih virov (banke, volilne komisije, partnerske organizacije, upravljavci družabnih omrežij, ponudniki storitev, ...), da bi vas prepričali, da razkrijete občutljive podatke, kot so uporabniška imena in gesla, podatke kreditnih kartic, potrditvene kode v SMS-ih, PIN kode, kliknete na zlonamerne povezave in nenamerno prenesete okužene datoteke, s katerimi zlonamerni akter lahko prevzame nadzor nad napravo.

Posebne oblike:

- Ciljno usmerjen napad z zvabljanjem (angl. Spear-phishing): Personalizirani napadi na ključne člane ekipe, ki temeljijo na podrobnem raziskovanju ciljnih oseb in njihove vloge v organizaciji;
- Lažna SMS sporočila (angl. Smishing): SMS sporočila z urgentnimi sporočili in povezavami, ki vodijo na zlonamerne spletne strani;
- Lažni telefonski klici (angl. Vishing): Klici, kjer se zlonamerni akterji predstavljajo kot uradne osebe ali tehnična podpora. Ti klici so lahko zmanipulirani z orodji generativne umetne inteligence, tako da zgolj iz glasu sogovornika ni možno ugotoviti, ali govorite z osebo, za katero se predstavlja.

Posledice: Izguba dostopa do elektronske pošte ali dostop nepooblaščenih do te pošte, razkritje občutljivih in zaupnih informacij, okužba sistemov z zlonamerno programsko opremo.

Zlonamerne aktivnosti z uporabo izsiljevalskega programja (angl. Ransomware) in/ali brisanja podatkov

Tveganje: Zlonamerna programska oprema, ki s šifrirnim ključem zašifrira vaše datoteke (lahko vključno z osebnimi in poslovnimi podatki) in, kjer nadzornik te programske opreme zahteva odkupnino za njihovo sprostitev. Pred šifriranjem zlonamerni akterji pogosto podatke najprej neopaženo prenesejo na svoje strežnike in nato grozijo z njihovo objavo na spletu, da bi povečali pritisk za plačilo. V nekaterih primerih zlonamerni akterji uporabijo uničevalce podatkov (angl. wiperware), ki podatke uničijo brez možnosti povrnitve.

Primeri:

- Leta 2019 je napad z izsiljevalskim programjem na Državno volilno komisijo Severne Makedonije mesec dni pred predsedniškimi volitvami začasno oviral delovanje njenih glavnih informacijskih in komunikacijskih sistemov, zaradi česar so bili volilni seznami, podatkovne zbirke in strežniki elektronske pošte, ki so jih državni agenti uporabljali za vzpostavitev volilnih uradov, v ključnem času nedostopni;
- Takšna zlonamerna dejanja lahko preprečijo dostop do volilnih seznamov, podatkovnih baz in strežnikov elektronske pošte v ključnem trenutku.

Posledice: Izguba dostopa do kampanjskih materialov, podatkovnih baz, finančnih evidenc; motenje volilne kampanje v kritičnem trenutku; javna objava občutljivih podatkov; v primeru uporabe uničevalcev podatkov je izguba podatkov nepovratna.

Vdori v sisteme in kraja podatkov

Tveganje: Nepooblaščen dostop do vaših sistemov, računov elektronske pošte, družbenih medijev ali podatkovnih baz z namenom kraje občutljivih informacij.
Napredne vztrajne grožnje (APT):

- Večfazni, dolgoročno načrtovani napadi, ki jih izvajajo ali financirajo države;
- Uporabljajo državne obveščevalne zmogljivosti za sofisticirane operacije; kamor sodi tudi uporaba vohunske programske opreme (npr. Pegasus), ki jo brez vaše vednosti namestijo na pametne mobilne telefone.

Primer: Napad na Centralno volilno komisijo Ukrajine leta 2014, kjer so zlonamerni akterji štiri dni pred volitvami uničili strežnike in sisteme.

Posledice:

- Kraja strateških kampanjskih načrtov:
- Dostop do osebnih podatkov podpornikov;
- Uhajanje internih komunikacij;
- Možnost kasnejše objave ukradenih dokumentov (t.i. "hack and leak" operacije);
- "Kontaminirane" objave: Zlonamerni akterji lahko med prave dokumente vmešajo ponarejene dokumente z lažnimi informacijami.

DDoS napadi oz. aktivnosti z vplivom na dostopnost in razpoložljivost informacijskih ali komunikacijskih sistemov

Tveganje: Zlonamerni akterji preplavijo spletno stran ali spletne storitve z ogromno količino prometa ali neobičajnimi zahtevki, kar povzroči, da postanejo nedostopne za legitimne uporabnike. Zlonamerne aktivnosti so lahko usmerjene na omrežno plast (s prometom ohromi usmerjevalnike in omrežno infrastrukturo), transportno (izčrpava vire varnostnih sistemov) ali aplikacijsko (izčrpava vire za delovanje spletne aplikacije). Čeprav so napadi DDoS postali krajši (večina traja manj kot eno uro), ostajajo zelo učinkoviti pri spodkopavanju zaupanja javnosti, saj so informacije, ki jih nudijo strežniki oziroma spletne strani nedostopne.

Primeri:

- Češka republika (2017): DDoS napadi na spletne strani volilnih rezultatov;
- Finska (2019): Napad na spletno storitev za objavo volilnih rezultatov;
- Švedska (2018, 2022): Ponavljajoči napadi na volilne spletne strani;
- Nizozemska, Francija, Velika Britanija, ZDA, Romunija (2024): DDoS napadi na spletne strani kampanj in političnih strank.

Posledice: Spletna stran postane nedostopna prav v kritičnih trenutkih kampanje (npr. pred volitvami, med objavo pomembnih sporočil); škodovanje ugleda; izguba možnosti komuniciranja z volivci.

Varnost spletnih strani in spletnih aplikacij

Ranljivosti programske opreme: Spletne strani političnih strank in kandidatov pogosto uporabljajo sisteme za upravljanje vsebin (CMS-Content Management Systems) kot so WordPress, Joomla ali Drupal ter različne vtičnike, (plugins) s katerimi se razširjajo funkcionalnosti spletnih strani brez poseganja v osnovno kodo CMS-ja. Neposodobljena programska oprema, vključno z vtičniki, lahko vsebuje varnostne ranljivosti, ki jih zlonamerni akterji lahko izkoriščajo za:

- vrivanje škodljive kode (SQL injection, XSS napadi),
- prevzem celotne spletne strani,
- krajo podatkov obiskovalcev,
- uporabo vaše spletne strani za napade na druge sisteme.

Nepooblaščen poseg v vsebino ali izgled spletne strani (razobličenje spletne strani): Zlonamerni akterji spremenijo videz ali vsebino spletne strani z namenom:

- diskreditiranja kandidata ali stranke,
- širjenja lažnih informacij,
- ustvarjanja zmede,
- škodovanja ugledu.

Primeri:

- Poljska (2024): Zlonamerni akterji so vdrli na spletno stran nacionalne tiskovne agencije in objavili lažen članek o vojaški mobilizaciji, da bi vplivali na volivce;
- Latvija (2018): Na priljubljenem družbenem omrežju Draugiem.lv so se na dan parlamentarnih volitev pojavila proruska sporočila.

Ranljivosti v dobavni verigi

Zlonamerni akterji lahko ciljajo na izvajalce, ki tehnično skrbijo za vsebino ali delovanje spletnih strani ali ponudnike gostovanja spletnih storitev, ki se uporabljajo v volilnem postopku (ponudniki gostovanja, razvijalci programske opreme, skrbniki sistema, IT storitve, uredniki spletnih strani, medijske agencije), da bi prek njih pridobili dostop do sistemov in podatkov. To vključuje:

- komponente komercialnih programskih paketov,
- zunanje storitve gostovanja, zunanje ponudnike digitalnega oglaševanja,
- vtičnike in razširitve tretjih oseb,
- knjižnice odprte kode.

Posledice izkoriščanja dobavnih verig: zlonamerni akter lahko dobi trajna stranska vrata do sistemov, kar posledično lahko pripelje do:

- nepooblaščenega dostopa do sistema,
- izhodišče za namestitev izsiljevalskega programja,
- objava lažnih sporočil ali informacij v vašem imenu,
- kraja podatkov obiskovalcev spletnih strani ali podatkov podpornikov in članov stranke (e-naslovi, telefonske številke, naslovi IP),
- uporaba vaše strani za širjenje zlonamerne programske opreme (nepooblaščena namestitev zlonamerne kode),
- nedostopnost spletne strani v kritičnih trenutkih,
- nepooblaščen dostop do kanalov družbenih omrežij prek povezanih oglaševalskih računov,
- izguba zaupanja volivcev in na splošno škoda na ugledu, ki jo je težko popraviti.

Kompromitacija računov na družbenih medijih

Tveganje: Prevzem vaših računov na družbenih medijih (Facebook, X, Instagram, TikTok, itd.) zaradi šibkih gesel, uporaba istih gesel pri različnih storitvah ali uspešnih napadov ribarjenja.

Posledice: Objava lažnih sporočil v vašem imenu; širjenje dezinformacij; uničenje ugleda; izguba zaupanja sledilcev.

Nova grožnja - manipulacija algoritmov (Romunija, 2024)

Romunsko ustavno sodišče je razveljavilo prvi krog predsedniških volitev, ker je tajna operacija za vplivanje na volivce na platformi TikTok odigrala odločilno vlogo pri zmagi enega od neodvisnih kandidatov. Obveščevalne službe so ugotovile, da so bili algoritmi TikTok manipulirani, da so sistematično poudarjali program enega od teh kandidatov.

Posledice: manipulacija javnega mnenja preko manipuliranih algoritmov.

Dezinformacije in manipulacija z informacijami

Tveganje: Širjenje lažnih informacij o vas, vaši stranki ali volilnem procesu, pogosto v kombinaciji s kibernetskimi napadi. Uporaba umetne inteligence za ustvarjanje lažnih videov (deepfakes), slik ali avdio posnetkov.

Glavni akterji kibernetskih groženj

Število ciljno usmerjenih zlonamernih aktivnosti se je v zadnjem desetletju povečalo in prav tako se je povečalo število in raznolikost akterjev, ki ogrožajo okolje kibernetske varnosti na volitvah. Grožnje so lahko državno sponzorirani akterji (APT skupine), kibernetski kriminalci ali politično motivirani posamezniki ali skupine.

Grožnjo lahko predstavljajo tudi zaposleni, zunanji izvajalci ali posamezniki oziroma vsi, ki imajo dostop do sistemov in naprav in pride do incidenta bodisi namerno, ali zaradi malomarnosti.

Priporočeni ukrepi

Temeljna varnostna kibernetska higiena

Močna gesla in upravljanje gesel:

- uporabljajte močna, edinstvena gesla (najmanj 12 znakov, kombinacija črk, številk in simbolov ali daljših fraz, ki se jih uporabnik lažje zapomni),
- nikoli ne uporabljajte istega gesla za različne račune in storitve,
- uporabite upravitelja gesel (npr. Bitwarden, 1Password, KeePass) za varno shranjevanje gesel,
- ob začetku uporabe spremenite privzeta gesla na vseh napravah in storitvah.

Večfaktorska avtentikacija (MFA/2FA):

- vključite večfaktorsko avtentikacijo na vseh računih (e-pošta, družbeni mediji, bančništvo, kampanjske platforme) in še posebej pri oddaljenem dostopu in skrbniških računih;
- prednostno uporabljajte aplikacije za avtentikacijo (Google Authenticator, Microsoft Authenticator);
- varno shranite varnostne rezervne kode;
- Izogibajte se avtentikaciji preko SMS-jev, saj se lahko SMS prestreže in zlonamerno uporabi brez vednosti uporabnika.

Redne posodobitve

- redno posodabljajte operacijske sisteme, aplikacije in protivirusno programsko opremo,
- omogočite samodejne varnostne posodobitve, kjer je to mogoče,
- ne uporabljajte zastarelih ali nepodprtih programskih orodij.

Študije kažejo, da je 98% kibernetskih napadov mogoče preprečiti z osnovnimi praksami IT higiene.

Zaščita pred ribarjenjem

Usposabljanje in ozaveščanje:

- Redno usposabljajte vse člane ekipe o prepoznavanju napadov vseh oblik ribarjenja.
- Opozorite druge v primeru prejetega sporočila ali lažne spletne strani, ki poskuša prejemnika zvabiti, da jim sporoči občutljive podatke (SI-CERT vodi aktualen seznam phishing URL naslovov, ki se jih lahko vključi v sisteme za zaščito elektronske pošte in druge varnostne rešitve).
- Bodite pozorni na:

1. Nepričakovana sporočila ali telefonske klice z zahtevami po razkritju osebnih podatkov, uporabniških imenih ali geslih;
2. Sporočila, ki vzpodbujajo k hitremu ukrepanju ali vzbujajo strah;
3. Sumljive povezave in priloge (v e-sporočilih, SMS-ih, aplikacijah za takojšnje sporočanje);
4. Napake v pisavi in nenavadne e-poštne naslove/domene pošiljateljev;
5. Ciljno usmerjene napade ribarjenja (spear-phishing), ki temeljijo na poznavanju vaše organizacije.

Priporočamo ogled spletnega tečaja Varni v pisarni (https://www.varnivpisarni.si/), ki ga je pripravil SI-CERT, kjer se na enostaven, razumljiv in vizualno privlačen način predstavi osnove informacijske varnosti.

Preverjanje pred ukrepanjem:

- Nikoli ne klikajte neposredno na povezave v sumljivih e-sporočilih ali SMS sporočilih (preverite, kam vodijo povezave),
- Preverite e-poštne naslove pošiljateljev (ne samo prikazanih imen),
- Pri dvomu neposredno kontaktirajte domnevnega pošiljatelja po drugem kanalu,
- Ne odprite prilog iz neznanih ali nepričakovanih virov.

Tehnični ukrepi:

- Uporabite e-poštne filtre za prepoznavanje in blokiranje sporočil z namenom zvabljanja na lažna spletna mesta,
- Uporabljajte protivirusno programsko opremo in napredne varnostne rešitve za prepoznavo škodljive kode,
- Ločite osebne in službene e-poštne račune,
- Pri priznanem varnostnem strokovnjaku za kibernetsko varnost oziroma organizaciji naročite varnostni pregled (spletnih strani in infrastrukture).

Varno ravnanje z napravami

Računalniki in prenosniki:

- uporabite šifriranje diska ali datotek (BitLocker za Windows, FileVault za macOS, 7-ZIP, PGP),
- nastavite samodejno zaklepanje zaslona (po 5-10 minutah neaktivnosti),
- ne puščajte naprav brez nadzora na javnih mestih,
- uporabljajte VPN pri povezavi na javne Wi-Fi točke oziroma se popolnoma izogibajte javnih WiFi točk.

Mobilne naprave:

- vključite šifriranje naprave,
- uporabite močne PIN kode ali biometrično zaklepanje,
- ne nameščajte in odstranite obstoječe aplikacije iz neznanih virov,
- bodite previdni pri odobravanju dovoljenj aplikacijam (še posebej pri dostopu aplikacij do imenikov, lokacije, sporočil). Posebej so nevarne široke pravice dostopnosti, saj zlonamerni aplikaciji omogočajo popoln nadzor nad napravo.

Ločitev osebnega in službenega:

- po možnosti uporabljajte ločene naprave za osebno in službeno uporabo,
- če to ni mogoče, ločite osebne in službene račune in podatke.

Zaščita občutljivih podatkov

Varnostno kopiranje:

- redno ustvarjajte varnostne kopije vseh pomembnih podatkov (npr. e-pošta, dokumenti, fotografije, spletne strani, baze podatkov, slik virtualnih strojev, vsebnikov, delovnih postaj, nastavitve; dnevno ali tedensko),
- varnostne kopije šifrirajte in jih shranjujte na ločenih lokacijah (zunanji trdi disk, zaupanja vredna oblačna storitev),
- preizkusite obnovitev podatkov iz varnostnih kopij.

Varnostna kopija je lahko edina rešitev obnove podatkov v primeru napada z izsiljevalskim programjem.

Upravljanje dostopa:

- dodelite dostop do občutljivih podatkov samo tistim, ki ga potrebujejo, in tudi zagotovite sledljivost dostopov,
- pregledujte in posodabljajte dostopne pravice,
- vodite evidenco dostopnih pravic,
- takoj odvzemite dostop zaposlenim, ki zapustijo ekipo in tudi zunanjim dobaviteljem, ki več ne potrebujejo dostopa,
- vodite in periodično preverjate evidenco dostopov do občutljivih sistemov.

Šifriranje:

- šifrirajte občutljive datoteke pred pošiljanjem ali shranjevanjem v oblak,
- uporabljajte varne komunikacijske kanale (Signal, WhatsApp s šifriranjem od konca do konca) za občutljive pogovore in sporočila,
- ne pošiljajte občutljivih informacij po nešifriranem e-sporočilu (uporaba digitalnih potrdil in orodij za podpisovanje in šifriranje e-sporočil, kot je OpenPGP, Kleopatra - Gpg4Win, GPG Suite).

Varnost družbenih medijev in spletne prisotnosti

Zavarovanje računov:

- vključite večfaktorsko avtentikacijo na vseh računih družbenih medijev, ki jih uporabljate,
- pregledujte nastavitve zasebnosti in omejite, kdo lahko vidi in komentira vaše objave,
- pozanimajte se, ali je bil vaš e-poštni naslov ali gesla, ki jih uporabljate objavljen na temnem spletu ali v javnih zbirkah potrjenih podatkovnih incidentov (npr. https://haveibeenpwned.com/),
- redno pregledujte nedavne aktivnosti in takoj zamenjajte geslo v primeru zaznane zlorabe,
- bodite previdni pri uporabi zunanjih aplikacij, katerim je omogočen dostop do uporabniškega računa (3rd party apps), predvsem za upravljanje vsebin, AI kreiranje vsebin ipd (redno preverjajte dostope aplikacij in storitev do vašega računa).

Varno objavljanje:

- ne razkrivajte podrobnosti o lokaciji v realnem času,
- bodite previdni pri deljenju osebnih informacij,
- preverite vsebino pred objavo (odporno na manipulacijo, točnost).

Zavedanje o manipulaciji algoritmov:

- bodite pozorni na nenavadno hitro širjenje vsebin o vaši stranki/kandidatu,
- preverite, ali je vsebina pravilno označena kot politično oglaševanje,
- prijavite nepravilnosti platformam družbenih medijev.

Odzivanje na incidente:

- imejte načrt odziva za primer kompromitiranega računa,
- takoj spremenite gesla in obvestite sledilce, če je račun ogrožen,
- prijavite incident platformi in pristojnim organom.

Varnost spletnih strani in spletnih aplikacij

Osnovna zaščita:

- Uporabite zanesljivo gostovanje z varnostnimi funkcijami (preverite tehnične kapacitete in reference ponudnika):
  - DDoS zaščita,
  - požarni zidovi aplikacij (WAF - Web Application Firewall),
  - varnostno spremljanje 24/7,
  - geografsko porazdeljeni strežniki za boljšo odpornost,
  - omejevanje hitrosti dostopa (rate limiting).
- uporaba sodobnih in varnih kriptografskih algoritmov (priporočena izbira protokol TLS 1.3) - obvezno za vse spletne strani,
- varnostno arhiviranje spletne strani (dnevno, shranjeno na ločeni lokaciji) ter načrt obnove podatkov,
- imejte rezervno gostovanje ali statično različico strani za kritične trenutke.

Upravljanje sistema za upravljanje vsebin (CMS-Content Management Systems):

- takoj namestite s strani proizvajalca priporočene varnostne posodobitve za CMS (npr. WordPress, Drupal, Joomla),
- posodabljajte vse vtičnike in teme - neposodobljeni vtičniki so najpogostejša ranljivost,
- odstranite neuporabljene vtičnike in teme - vsak dodatek je potencialna ranljivost,
- uporabljajte samo preverjene vtičnike iz uradnih virov (preverite, kdaj so bili nazadnje posodobljeni),
- omejite število vtičnikov na minimum potrebnega.

Preverite aktualno stanje odpornosti in varnosti z vdornim testiranjem.

Zaščita pred vdorom:

- zagotovite močna gesla,
- omejite število poskusov prijave (proti brute-force napadom),
- dvofaktorska avtentikacija za vse skrbniške račune,
- spremenite privzete URL-je za prijavo (npr. ne uporabljajte /wp-admin),
- omejite dostop do administrativnega vmesnika samo na IP naslove, iz katerih se bo povezoval skrbnik,
- redno pregledujte dnevnike dostopa za odkrivanje sumljivih aktivnosti.

Varnostno testiranje:

- redno izvajajte varnostne preglede s strani strokovnjaka za kibernetsko varnost z referencami,
- penetracijsko testiranje sistemov in aplikacij, dovolj zgodaj pred začetkom volilne kampanje,
- nastavite varnostni monitoring z alarmiranjem ob sumljivih aktivnostih,
- preverjajte integriteto datotek - odkrivanje sprememb v kodi.

Varnost dobavne verige:

- uporabljajte samo zaupanja vredne ponudnike storitev in programske opreme,
- preverite reference programskih razvijalcev pred najemom,
- zahtevajte strokovni vpogled v kodo tretjih oseb, če je kritična za vašo varnost,
- omejite odvisnost od zunanjih knjižnic in storitev,
- spremljajte obvestila o ranljivostih v uporabljeni programski opremi.

Načrt za hitro okrevanje:

- shranjujte čisto različico spletne strani za hitro obnovo,
- testiranje obnovitve iz varnostnih kopij,
- vzpostavite seznam kontaktnih podatkov za nujno podporo (gostovanje, IT podpora),
- imejte komunikacijski načrt za obveščanje javnosti v primeru kibernetskega incidenta.

Načrtovanje odziva na incidente

Pripravite načrt:

- določite vloge (kdo je odgovoren za kaj med incidentom),
- pripravite komunikacijsko strategijo (kako boste komunicirali z mediji, podporniki, javnostjo),
- imejte seznam kontaktov (pristojna skupina za odzivanje na incidente, policija, IT strokovnjaki),
- določite postopke eskalacije,
- vnaprej pripravite izjave za različne scenarije (DDoS, kraja podatkov, izsiljevanje s škodljivim programjem, razobličenje spletnih strani).

Ključne kontaktne točke:

- IT strokovnjak/ekipa za nujno podporo,
- odzivni center za obravnavanje incidentov SI-CERT,
- Policija - Sektor kriminalistične policije (oddelek za kibernetsko kriminaliteto; telefon: 113 nujna številka),
- Državna volilna komisija za vprašanja volilne integritete (https://www.dvk-rs.si/) ,
- vaš ponudnik gostovanja (imejte 24/7 kontakt).

Posebni scenariji:

Ob DDoS napadu:

- pri ponudniku dostopa aktivirajte DDoS zaščito (predhodno si zagotovite ustrezen dogovor),
- obvestite ponudnika gostovanja,
- aktivirajte rezervno statično stran (če je na voljo),
- obvestite javnost preko družbenih medijev,
- ne čakajte, da napad mine - ukrepajte takoj.

Ob zlonamerni spremembi spletne strani:

- takoj odstranite spremenjeno vsebino in obnovite stran iz varnostne kopije,
- spremenite vsa gesla administrativnih računov,
- strokovnjak naj pregleda dnevnike za odkrivanje vzroka vdora,
- zagotovite, da zlonamerni akter ni vnesel dodatne zlonamerne kode,
- javno obsodite zlonamerno dejanje in pojasnite, da niste vi objavili spremenjene vsebine,
- odstranite morebitne ranljivosti programske opreme in okrepite varnostne ukrepe za preprečitev ponovitve.

Zaščita pred dezinformacijami in manipulacijo informacij

Monitoring:

- spremljajte družbene medije in splet za omembe vaše stranke/kandidata,
- uporabite orodja za spremljanje (Google Alerts, analitika družbenih medijev),
- hitro identificirajte dezinformacije in lažne vsebine, vključno z deepfakes.

Odzivanje:

- imejte strategijo odziva na dezinformacije (hitro, dejstveno, transparentno),
- prijavite lažne vsebine platformam družbenih medijev,
- dokumentirajte napade z dezinformacijami za morebitne pravne korake.

Kaj storiti ob incidentu

- Aktivirajte načrt odzivanja na incident in osebe, ki ste jih določili v okviru tega načrta,
- Ne plačajte odkupnin brez posvetovanja s strokovnjaki,
- Dokumentirajte incident (posnetki zaslona, dnevniški zapisi, čas dogodkov),
- Izolirajte okužene naprave ali sisteme od omrežja,
- Obvestite odgovorne osebe v skladu z načrtom,
- Obvestite policijo v primeru nastanka kaznivega dejanja,
- Aktivirajte načrt za obnovitev (varnostne kopije, rezervno gostovanje),
- Komunicirajte transparentno z javnostjo:
  - potrdite incident,
  - pojasnite, kaj se je zgodilo,
  - navedite, katere ukrepe ste sprejeli,
  - zagotovite, da podatki volivcev niso ogroženi.

Na podlagi 59. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25) lahko politične stranke ali kandidati zaznane incidente prostovoljno priglasijo odzivnemu centru za obravnavanje incidentov SI-CERT, ki deluje v okviru javnega zavoda Arnes. SI-CERT opravlja koordinacijo razreševanja incidentov in nudi tehnično pomoč ob vdorih, računalniških okužbah in drugih zlorabah. Kontaktni naslov za prijavo incidentov je cert@cert.si.

Zaključek

Kibernetska varnost ni enkratno dejanje, temveč stalen proces. Grožnje se nenehno razvijajo, zato je pomembno, da ostanete pozorni, obveščeni in pripravljeni.

Upoštevajte ključna načela:

- Previdnost: Ne klikajte kar koli, ne razkrivajte kar koli, ne zaupajte komur koli,
- Pripravljenost: Imejte načrte, varnostne kopije in kontakte pripravljene vnaprej,
- Odgovornost: Kibernetska varnost je odgovornost vsakogar v ekipi, ne le IT osebja,
- Sodelovanje: Delite informacije o grožnjah s pristojnimi organi in drugimi demokratičnimi akterji,
- Transparentnost: Zaupanje javnosti je odvisno od vaše odprtosti glede varnostnih ukrepov.

Cilj kibernetskih zlonamernih akterjev ni vedno neposredno vplivati na volilne rezultate. Pogosto je njihov cilj sejati dvom, povzročiti kaos in oslabiti zaupanje v demokratične procese. Tudi neuspešni napadi lahko dosežejo svoj cilj, če povzročijo, da volivci dvomijo v integriteto volitev. Z ustreznimi varnostnimi ukrepi ne ščitite samo sebe in svoje stranke - ščitite tudi integriteto volitev in demokratičnega sistema, v katerem živimo.

Navedeni ukrepi predstavljajo temeljna in priporočena izhodišča za krepitev kibernetske varnosti v volilnem obdobju, vendar ne izčrpavajo vseh možnih tveganj ali rešitev; posamezne politične stranke in kandidati naj jih zato prilagodijo svojemu konkretnemu okolju, razpoložljivim virom in aktualni oceni tveganj ter jih po potrebi dopolnijo z dodatnimi ukrepi.

Viri: Ta dokument temelji na mednarodnih najboljših praksah in priporočilih EU Skupine za sodelovanje (NIS Cooperation Group) in ENISA[1], NATO[2], izkušnjah z obravnavo preteklih incidentov na URSIV ter volitev v drugih državah EU.

Dr. Uroš Svete
direktor urada

[1] NIS Cooperation Group: Updated Compendium on Elections Cybersecurity and Resilience (2024): https://digital-strategy.ec.europa.eu/en/news/new-cybersecurity-compendium-how-protect-integrity-elections-publishedm dostop 27. 1. 2026
[2] NATO: RENFORCER LA CYBERSÉCURITÉ DES INFRASTRUCTURES DÉMOCRATIQUES ET DES SYSTÈMES ÉLECTORAUX DES PAYS ALLIÉS, https://www.nato-pa.int/fr/document/2025-cybersecurite-rapport-kairidis-010-cds, dostop 25. 1. 2026