

Pravilnik o postopkih za upravljanje varnostnih dogodkov

Zgodovina sprememb:

| Verzija | Datum | Številka dokumenta |
|---------|------------|--------------------|
| 1 | 21.9.2011 | 007-47/2011/12 |
| 2 | 24.4.2015 | 007-47/2011/27 |
| 3 | 29.11.2017 | 007-47/2017/11 |
| 4 | 18.10.2018 | 007-47/2017/22 |
| 5 | 5.10.2022 | 007-47/2017/37 |

Na podlagi drugega odstavka 42. člena Zakona o državni statistiki (Ur. list RS, št. 45/1995, 9/2001) in v skladu z Uredbo o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18, 131/20) predstojnik Statističnega urada Republike Slovenije izdaja naslednji

Pravilnik o postopkih za upravljanje varnostnih dogodkov

1 SPLOŠNE DOLOČBE

1.1 Namen

Pravilnik določa organizacijsko strukturo in postopke zaznave, odziva, vodenja, analiziranja in poročanja o varnostnih dogodkih na Statističnemu uradu Republike Slovenije (v nadaljevanju: SURS), s čimer se zagotavlja sistematičen pristop pri obvladovanju potencialnih ali udejanjenih groženj za varnost informacij.

1.2 Cilj

Cilj pravilnika o postopkih za upravljanje varnostnih dogodkov je zagotoviti pravočasen in pravilen odziv vseh zaposlenih SURS na potencialne in udejanjene grožnje varnosti informacij SURS, s čimer bi se škodni vplivi groženj na delovanje in položaj SURS preprečili ali v najkrajšem možnem času odpravili in s tem zmanjšali vpliv na delovanje SURS na sprejemljiv nivo.

1.3 Predmet

Varnost informacij se za potrebe tega pravilnika nanaša na zagotavljanje celovitosti, razpoložljivosti in zaupnosti informacij. Varnostni dogodki, povezani z varnostjo oseb in fizičnih sredstev, niso predmet tega pravilnika.

2 KLASIFIKACIJA VARNOSTNIH DOGODKOV

2.1 Opredelitev varnostnega dogodka

Varnostni dogodek (incident) je vsak dogodek, ki je povzročil ali predstavlja tveganje, da bi lahko povzročil škodo informacijskim virom, ugledu ali osebju SURS. Za varnostni dogodek v okviru tega pravilnika se ne štejejo tisti dogodki, ki so povezani z naravnimi in drugimi nesrečami in se hkrati ne nanašajo neposredno na informacijsko varnost.

Upravljanje varnostnih dogodkov se nanaša na klasifikacijo varnostnih dogodkov, način zaznavanja, evidentiranje, spremljanje in poročanje o varnostnih dogodkih, postopkih zavarovanja in hrambe dokazov, ukrepanja in beleženja ukrepov v primeru varnostnih dogodkov ter pregledovanje, analiziranje in poročanje o evidentiranih varnostnih dogodkih.

Primeri pogostejših varnostnih dogodkov so:

- ☞ nepooblaščen vstop v varovane prostore SURS,
- ☞ odtujitev ali uničenje podatkovnega nosilca podatkov oz. informacij, ki so v skladu s Pravilnikom o klasifikaciji informacij opredeljene kot občutljive ali interne,
- ☞ poizkus pridobitve dostopa z uporabo tujega uporabniškega imena,
- ☞ nepooblaščne spremembe v nastavitvah informacijskega sistema,
- ☞ okužba z zlonamerno programsko opremo,
- ☞ odkritje varnostne pomanjkljivosti v informacijskem sistemu,
- ☞ razkritje informacij, ki so v skladu s Pravilnikom o klasifikaciji informacij opredeljene kot občutljive ali interne nepooblaščenim osebam.

2.2 Klasifikacija varnostnih dogodkov

Varnostni dogodki so z namenom opredelitve ustreznega odziva klasificirani v razrede. Razredi varnostnih dogodkov so opredeljeni na dva načina, in sicer glede na:

- ☞ vrsto varnostnega dogodka ali
- ☞ potencialen vpliv, ki ga varnostni dogodek lahko ima za informacijsko varnost SURS.

2.2.1 Vrste varnostnih dogodkov

Varnostni dogodki so razvrščeni na kategorije glede na vrsto dogodka. En dogodek lahko spada v več kategorij.

1. Nepooblaščen dostop do podatkov SURS;
2. Odtujitev podatkov SURS;
3. Razkritje podatkov, ki jih hrani SURS, nepooblaščenim osebam;
4. Dogodki, povezani z izvajanjem kaznivih dejanj (vlom v prostore SURS, kraja nosilcev podatkov ali podatkov v elektronski obliki, ...);
5. Napad na informacijski sistem SURS:
 - a. vdor v informacijski sistem z neavtorizirano uporabo uporabniškega imena in gesla druge osebe;
 - b. vdor ali poskus vdora v informacijski sistem z uporabo tehnik vdiranja (uganjevanje gesel, izkoriščanje oz. iskanje varnostnih lukenj informacijskega sistema, ipd.);
6. Uporaba informacijskega sistema SURS na način, ki pomeni kršitev zakonodaje ali potencialno vodi v odškodninski zahtevek tretje osebe nasproti SURS (npr. uporaba informacijskega sistema za prenos avtorskih vsebin, objava zakonsko reguliranih informacij (npr. pornografske vsebine), ipd.);
7. Zloraba pooblastil:
 - a. zloraba pooblastil uslužbenca SURS;
 - b. zloraba pooblastil zunanjega izvajalca ali uporabnika storitev SURS;
8. Izpostavljenost informacijskega sistema zlonamerni programski opreми (okužba s virusi, trojanskimi konji, ipd.) ali neupravičeni uporabi informacijskih virov (tehnično omogočen dostop do podatkov, do vpogleda v katere uporabnik ni upravičen ipd.);
9. Kršitve celovite politike varovanja informacij SURS.
10. Uničenje ali poškodovanje podatkov SURS.
11. Nedosegljivost informacijskih virov SURS

2.2.2 Varnostni dogodki glede na vpliv

Razvrščanje varnostnih dogodkov glede na njihov vpliv na informacijsko varnost SURS se izvede ob nastanku dogodka. Pri razvrščanju je potrebno vzeti v ozir vse relevantne okoliščine dogodka in tveganja za SURS, ki jih takšen dogodek lahko ima. Pri razvrščanju je potrebno upoštevati predvsem sledeče kriterije:

- ☞ obseg aktivnosti SURS (procesov, ljudi, organizacijskih enot, informacijskih sistemov), ki jih je dogodek prizadel;
- ☞ kritičnost sistema ali informacijske storitve za delovanje SURS, na katerega se dogodek nanaša;
- ☞ občutljivost podatkov, ki so ogroženi ali potencialno ogroženi (osebni in drugi občutljivi podatki);
- ☞ verjetnost ponovljivosti dogodka (npr. možnost razširitve okužbe z zlonamerno programsko opremo na druge dele informacijskega sistema, možnost vpliva razkritja podatkov na varnost drugih delov sistema, itd.).

Glede na navedene kriterije se vsak varnostni dogodek klasificira z eno izmed sledečih ravni nevarnosti:

1. Visoka nevarnost

Kot dogodki visoke nevarnosti se klasificirajo sledeči dogodki:

- ☞ dogodki, ki imajo lahko pomemben negativen vpliv na celoten informacijski sistem SURS ali njegov večji del, oziroma na večino uporabnikov ali organizacijskih enot SURS tako, da to vpliva na delovanje celotnega SURS in izpolnjevanje njegovih primarnih nalog;
- ☞ dogodki, ki ogrozijo delovanje celotne mrežne infrastrukture SURS;
- ☞ dogodki, ki lahko zaradi svoje narave vodijo v finančne izgube ali izpostavljenost pravni odgovornosti SURS;
- ☞ dogodki, katerih posledica je ogroženost osebnih in drugih zaupnih podatkov SURS;
- ☞ dogodki, ki pomenijo neposredno nevarnost za življenje in zdravje ljudi (zaposlenih ali drugih);
- ☞ takšna okužba sistemov z zlonamerno programsko opremo, kjer obstaja visoka verjetnost širitev okužbe na druge informacijske sisteme.

Varnostni dogodki visoke nevarnosti zahtevajo takojšen odziv skrbnika informacijske varnosti in po potrebi drugih uslužbencev ter izvajanje ustreznih aktivnosti, dokler se škodljivih posledic dogodka ne zaustavi ali odpravi. V primeru takšnih dogodkov nastane tudi obveznost obveščanja o nastanku dogodka, kot je to opredeljeno v tabeli iz Priloge 1 tega pravilnika.

2. Srednja nevarnost

Kot dogodki srednje nevarnosti se klasificirajo sledeči dogodki:

- ☞ dogodki, ki lahko negativno vplivajo na del informacijskega sistema SURS ali na del uporabnikov, ki niso kritični za izpolnjevanje primarnih nalog SURS; takšni dogodki lahko ogrozijo delovanje posamezne organizacijske enote SURS;
- ☞ dogodki, ki vplivajo na informacijsko storitev / aplikativni sistem zgolj ene organizacijske enote SURS;
- ☞ dogodki, ki ogrozijo delovanje večjega dela omrežja SURS;
- ☞ takšna okužba sistemov z zlonamerno programsko opremo, kjer obstaja srednje velika verjetnost širitev okužbe na druge informacijske sisteme.

Varnostni dogodki srednje nevarnosti zahtevajo hiter odziv skrbnika informacijske varnosti in po potrebi drugih uslužbencev. V primeru takšnih dogodkov nastane tudi obveznost obveščanja o nastanku dogodka, kot je to opredeljeno v tabeli iz Priloge 1 tega pravilnika.

3. Nizka nevarnost

Kot dogodki nizke nevarnosti se klasificirajo sledeči dogodki:

- ☞ dogodki, ki lahko negativno vplivajo na manjši del informacijskega sistema SURS ali zgolj na malo število uporabnikov; takšni dogodki ne ogrozijo delovanja celotnih organizacijskih enot SURS;
- ☞ dogodki, ki negativno vplivajo zgolj na manjši del omrežja SURS;
- ☞ takšna okužba sistemov z zlonamerno programsko opremo, kjer verjetnost širitev okužbe na druge informacijske sisteme ni visoka.

Dogodki nizke nevarnosti zahtevajo hiter odziv skrbnika informacijske varnosti (najkasneje naslednji delovni dan) in po potrebi drugih uslužbencev. V primeru takšnih dogodkov nastane tudi obveznost obveščanja o nastanku dogodka, kot je to opredeljeno v tabeli iz Priloge 1 tega pravilnika.

4. Ni nevarnosti

Kot dogodki, kjer nevarnost ni razpoznana, se klasificirajo tisti dogodki, kjer se pri preiskavi domnevnega varnostnega dogodka ugotovi, da do dogodka sploh ni prišlo oz. da dogodek nima vpliva na informacijsko varnost SURS.

3 OBVEŠČANJE O VARNOSTNIH DOGODKIH

3.1 Odgovornost za obveščanje

Vsi uporabniki so dolžni o kakršnem koli nastalem varnostnem dogodku ali o sumu varnostnega dogodka brez odlašanja obveščati pristojne organe SURS. Prav tako so vsi uporabniki dolžni obveščati o odkritih varnostnih pomanjkljivostih informacijskega sistema ali postopkov SURS.

V tistih delih informacijskega sistema, kjer je to mogoče in smiselno, organizacijska enota, pristojna za infrastrukturo vzpostavi mehanizme za samodejno spremljanje dogodkov in sporočanje o potencialnih varnostnih dogodkih tehničnim skrbnikom posameznih informacijskih virov.

3.2 Način obveščanja

Vsa obvestila o varnostnih dogodkih je potrebno sporočiti na elektronski naslov itsec.surs@gov.si ali skrbniku informacijske varnosti.

4 UPRAVLJANJE VARNOSTNIH DOGODKOV

4.1 Odgovornosti za upravljanje z varnostnimi dogodki

Skrbnik informacijske varnosti je krovno odgovoren za upravljanje in spremembe postopkov upravljanja z varnostnimi dogodki, kot so določeni v tem pravilniku ter za izvajanje postopka upravljanja z varnostnimi dogodki.

Vodja organizacijske enote, pristojne za infrastrukturo je odgovoren za zagotavljanje ustreznega informacijskega sistema, ki bo podprl postopke upravljanja z varnostnimi dogodki, kot so določeni v tem pravilniku in za izvajanje teh postopkov.

4.2 Odziv na varnostni dogodek

4.2.1 Sprejem obvestila o varnostnem dogodku

Skrbnik informacijske varnosti mora ob prejemu obvestila o nastanku varnostnega dogodka pridobiti čim več informacij o nastalem ali potencialnem varnostnem dogodku, predvsem pa:

- ☞ ime in priimek, delovno mesto in kontaktne podatke osebe, ki je posredovala obvestilo o varnostnem dogodku;
- ☞ opis varnostnega dogodka;
- ☞ dodatne informacije o varnostnem dogodku, s katerimi bo omogočeno lažje preiskovanje virov posameznih dogodkov (npr. IP številke, elektronska sporočila vključno z glavo, ipd.);
- ☞ datum in ura nastalega varnostnega dogodka;
- ☞ drugi dokazi in podatki o sumljivih aktivnostih (npr. prejeta elektronska sporočila, strežniški dnevniki dogodkov, ipd.).

4.2.2 Analiza dogodka

Po sprejetju obvestila o nastalem varnostnem dogodku, skrbnik informacijske varnosti izvede analizo dogodka, z namenom ugotoviti naravo dogodka, tveganja, ki iz njega izhajajo ter načrtovanje primerne odziva na dogodek.

Cilj analize je pridobiti razumevanje narave in obsega varnostnega dogodka, zbiranje potrebnih informacij za opredelitev posameznih korakov odziva na varnostni dogodek in opredelitev ogroženosti osebnih ali drugih zaupnih podatkov zaradi varnostnega dogodka.

Analiza mora opredeliti odstopanja od normalnega delovanja informacijskega sistema SURS, katerih vzrok je varnostni dogodek. Opredelitev odstopanj mora vsebovati čim več informacij o nastalem dogodku, kot so strežniški dnevniki prizadetih sistemov / omrežij, zapisniki pogovorov z zaposlenimi ali sistemskimi administratorji, zajemi prometa po omrežju, revizijske sledi posameznih aplikacij, itd. V okviru analize se opredeli tudi okviren obseg vpliva varnostnega dogodka na informacijski sistem SURS.

Pri izvedbi analize po potrebi lahko sodelujejo tudi drugi strokovnjaki s področja informacijske varnosti.

4.2.3 Klasifikacija dogodka in beleženje

Skrbnik informacijske varnosti glede na rezultate analize varnostni dogodek klasificira v skladu s kriteriji, ki so opredeljeni v poglavju 2 tega pravilnika. Oznaka klasifikacije posameznega varnostnega dogodka mora vsebovati:

- ☞ vrsto varnostnega dogodka,
- ☞ opredelitev vpliva varnostnega dogodka.

Skrbnik informacijske varnosti izvede vnos dogodka v sistem za beleženje varnostnih dogodkov.

4.2.4 Izvedba aktivnosti za omejitev škodljivega vpliva varnostnega dogodka

Na podlagi klasifikacije varnostnega dogodka skrbnik informacijske varnosti izvede aktivnosti za omejevanje vpliva varnostnega dogodka. Cilj tega koraka je preprečevanje ogroženosti podatkov in zavarovanje informacijskih sistemov ali drugih delov informacijskega sistema SURS pred nadaljnjo škodo.

Postopki omejevanja škodljivega vpliva varnostnega dogodka segajo od osamitve prizadetih sistemov ali omrežij, fizičnega zavarovanja prostorov zaradi odkritih pomanjkljivosti ali ranljivosti do prekinitve delovanja določenih prizadetih delov informacijskega sistema. Nekateri postopki omejitve vpliva se lahko v določenih primerih tudi ne izvedejo takoj, če je to potrebno za ugotavljanje izvora varnostnega dogodka, pod pogojem, da odlog izvedbe ne ogrozi drugih delov informacijskega sistema ali varnosti informacij SURS (npr. zadržanje delovanje določenega dela informacijskega sistema zaradi odkrivanja vira vdora, če so hkrati zagotovljeni varnostni postopki, ki zagotavljajo, da takšno stanje dodatno ne ogrozi informacij ali informacijskega sistema SURS).

4.2.5 Odprava posledic varnostnega dogodka

Cilj odprave posledic varnostnega dogodka je izvedba postopkov za odpravo posledic varnostnega dogodka, zavarovanje dokazov, zagotovitev normalnega delovanja informacijskega sistema in preprečevanje ponovnega nastanka enakega varnostnega dogodka.

Postopke za odpravo posledic pripravi skrbnik informacijske varnosti glede na vrsto varnostnega dogodka. Po potrebi se izvede tudi dodatna analiza varnostnega dogodka in potencialnih ranljivosti informacijskega sistema SURS za enakovrstne dogodke.

Načrtovani ukrepi za preprečevanje ponovnega nastanka varnostnih dogodkov lahko obsegajo spremembe varnostnih nastavitvev informacijskega sistema (npr. spremembe gesel, nadgradnja operacijskih ali aplikacijskih sistemov, spremembe nastavitvev omrežnih naprav) ali organizacijske ukrepe (npr. izobraževanje uporabnikov, opredeljevanje dodatnih organizacijskih varnostnih postopkov ipd.).

4.2.6 Obveščanje pristojnih organov

Če gre pri posameznem varnostnem dogodku za sum storitve kaznivega dejanja ali drugega prekrška, SURS o tem obvesti policijo ali druge pristojne organe nadzora.

4.3 Zavarovanje dokazov

V primeru, ko je odkrit varnostni dogodek takšne narave, da zahteva sprožitev uradnega ali sodnega postopka, je potrebno med izvajanjem postopkov odziva na varnostni dogodek poskrbeti za ustrezno zavarovanje dokazov.

Za ustrezno zbiranje in zavarovanje dokazov je krovno odgovoren skrbnik informacijske varnosti.

Pri izvajanju postopkov odziva na varnostni dogodek mora skrbnik informacijske varnosti zagotoviti sledeče:

- ☞ pred zbiranjem dokazov je potrebno pridobiti dovoljenje posameznikov, če dokazi vsebujejo osebne podatke;
- ☞ pri zbiranju dokazov je potrebno voditi zapisnik izvedenih dejanj in popis vseh zbranih podatkov in/ali predmetov, vključno z datumom in uro zbiranja, prisotnimi osebami in morebitnimi drugimi pomembnimi okoliščinami;
- ☞ vse zbrane dokaze je potrebno zavarovati tako, da niso dostopni tretjim osebam, vsak dostop do dokazov pa zabeležiti.

4.4 Sistem spremljanja in evidentiranja varnostnih dogodkov

4.4.1 Beleženje varnostnih dogodkov in ukrepov

Skrbnik informacijske varnosti vzpostavi sistem za beleženje varnostnih dogodkov, v katerega se vpisuje podatke o vseh primerih varnostnih dogodkov ter o poročilih o posameznih dogodkih.

Sistem za beleženje varnostnih dogodkov vsebuje:

- ☞ identifikacijsko številko varnostnega dogodka;
- ☞ opis varnostnega dogodka, stopnjo nevarnosti in vrsto varnostnega dogodka;
- ☞ opis in lokacija prizadetih informacijskih virov SURS;
- ☞ opredelitev osebnih ali drugih zaupnih podatkov, če so ti prizadeti;
- ☞ osebe, ki so sporočile nastanek ali sum varnostnega dogodka in njihovi kontaktni podatki;
- ☞ datum in čas, ko je bil varnostni dogodek prvič opažen;
- ☞ dodatne informacije o varnostnem dogodku, s katerimi bo omogočeno lažje preiskovanje virov posameznih dogodkov (npr. IP številke, elektronska sporočila vključno z glavo, ipd.);
- ☞ drugi dokazi in podatki o sumljivih aktivnostih (npr. prejeta elektronska sporočila, strežniški dnevniki dogodkov, ipd.);
- ☞ rezultat analize varnostnega dogodka;
- ☞ informacije o aktivnostih za odpravo oz. omilitev posledic varnostnega dogodka.

4.4.2 Sistem za beleženje varnostnih dogodkov

Skrbnik informacijske varnosti na podlagi sistema za beleženje varnostnih dogodkov izvaja postopke analize trendov varnostnih dogodkov in preprečevanja nastajanja potencialnih cikličnih varnostnih dogodkov.

Na podlagi sistema za beleženje varnostnih dogodkov skrbnik informacijske varnosti izdeluje tudi analize notranjih ukrepov in politik za zagotavljanje informacijske varnosti in predlaga njihove izboljšave in spremembe.

4.4.3 Poročilo o izvedenih ukrepih in letno poročilo

Po zaključku postopkov odziva na varnostni dogodek mora skrbnik informacijske varnosti pripraviti poročilo o varnostnem dogodku.

Na podlagi poročila lahko skrbnik informacijske varnosti opredeli dodatne aktivnosti za preprečevanje potencialnih varnostnih dogodkov ali izboljšanje postopkov in politik za zagotavljanje varovanja informacij.

Skrbnik informacijske varnosti vsako leto pripravi letno poročilo o nastalih varnostnih dogodkih za preteklo leto. Poročilo vsebuje seznam in opis nastalih varnostnih dogodkov, izvedene ukrepe, analizo odkritih pomanjkljivosti sistema varovanja informacij ter predloge za njegovo izboljšanje.

5 KONČNI DOLOČBI

Ta pravilnik začne veljati petnajsti dan po objavi na internem portalu SURS.

Z dnem začetka veljavnosti tega pravilnika preneha veljati Pravilnik o postopkih za upravljanje varnostnih dogodkov št. 007-47/2017/22 z dne 18. 10. 2018.

Številka:

Datum:

Tomaž Smrekar,
generalni direktor

Priloga 1: Tabela odziva na varnostne dogodke

| Nevarnost dogodka | Kriteriji za klasifikacijo nevarnosti | Odzivni čas od trenutka prijave varnost. dogodka | Odgovornost za odziv na varnostni dogodek | Potrebno nadaljnje poročanje | Zahtevano poročilo po zaključku |
|-------------------|--|--|---|------------------------------|---------------------------------|
| Visoka | <p>Pomemben negativen vpliv na celoten informacijski sistem SURS ali njegov večji del, oziroma na večino informacijskih uporabnikov ali oddelkov SURS.</p> <p>Vpliv na delovanje celotnega SURS in izpolnjevanje njegovih primarnih nalog.</p> <p>Grožnja delovanju celotne mrežne infrastrukture.</p> <p>Dogodki, ki lahko zaradi svoje narave vodijo v finančne izgube ali izpostavljenost pravni odgovornosti SURS.</p> <p>Ogroženost osebnih in drugih zaupnih podatkov.</p> <p>Neposredna nevarnost za življenje in zdravje ljudi (zaposlenih ali drugih);</p> <p>Visoka verjetnost širitev okužbe z zlonamerno programsko opremo na druge informacijske sisteme.</p> | 0 ur / brez odlašanja | Skrbnik informacijske varnosti | Predstojnik | DA |

| | | | | | |
|---------|---|-----------------------|--------------------------------|--------------------------------|---------------------------------|
| Srednja | Negativen vpliv na del informacijskega sistema SURS ali na del informacijskih uporabnikov, ki niso kritični za izpolnjevanje primarnih nalog SURS. | 4 ure | Skrbnik informacijske varnosti | Predstojnik | DA |
| | Grožnja delovanju organizacijske enote. Vpliv na informacijsko storitev / aplikacijski sistem zgolj ene organizacijske enote. Ogroženo delovanje večjega dela omrežja (npr. oddelka). Srednje velika verjetnost širitve okužbe z zlonamerno programsko opremo na druge informacijske sisteme. | | | | |
| Nizka | Negativen vpliv na manjši del informacijskega sistema SURS ali zgolj na malo število informacijskih uporabnikov. | Naslednji delovni dan | Skrbnik informacijske varnosti | Skrbnik informacijske varnosti | V okviru periodičnega poročanja |
| | Ni grožnje za delovanje celotnih organizacijskih enot. Negativen vpliv zgolj na manjši del omrežja. Verjetnost širitve okužbe z zlonamerno programsko opremo na druge informacijske sisteme je nizka. Odkrita je varnostna pomanjkljivost, ki bi lahko v prihodnosti ogrozila informacijsko varnost. | | | | |
| N/A | Uporablja se za tiste varnostne dogodke, kjer je po pregledu / analizi ugotovljeno, da do varnostnega dogodka sploh ni prišlo. | | | | |