# **Obrazac prijelaznog izvješća o incidentu sa znatnim učinkom**

|  |
| --- |
| ***Prijelazno izvješće*** |
| **OSNOVNI PODACI** |
| Opišite incident i kronologiju događaja, uključujući:* Kako je došlo do pojave incidenta (kronologija, vektor napada)?
* Postoji li poveznica s nekim ranijim incidentom/događajem?
* Kako je otkriven incident?
* Jesu li treće strane uključene u razvoj/rješavanje incidenta?
* Koji procesi kriznog upravljanja su započeti?
* Je li najviša rukovodeća razina upoznata s razvojem događaja?
 | Navedite najvažnije pojedinosti o incidentu, uključujući moguće uzroke, trenutačne učinke itd. |
| Trenutačni status incidenta | [ ] Dijagnostika [ ] Oporavak  |  |
| Klasifikacija incidenta 1 |  |  |
| **UČINAK INCIDENTA** |
| Incident je utjecao na | [ ] Povjerljivost podataka [ ] Cjelovitost podataka [ ] Dostupnost podataka, procesa i usluga |  |
| Incident je otkriven | Odaberite |  |
| Koje usluge/procesi su zahvaćene incidentom (zaustavljene, ugrožene, usporene)? | Nabrojite sve usluge/procese u organizaciji koji su zahvaćeni pojavom incidenta.(Primjer: usluga internetskog bankarstva, proces nadzora prometne signalizacije…) |
| Koliko dugo je zahvaćena usluga/proces bila pod negativnim učinkom incidenta (zaustavljena, ugrožena, usporena)? | Za svaku od zahvaćenih usluga navedite razdoblje u kojem je ta usluga bila zaustavljena, ugrožena ili usporena.(Primjer: internetsko bankarstvo nedostupno tri sata, usporen rad 24 sata) |
| Koji IT sustavi su zahvaćeni incidentom, osobito:* Aplikacije,
* Hardver,
* Baze podataka,
* Mrežna infrastruktura,
* Ostalo.
 | Nabrojite IT sustave u organizaciji koji su zahvaćeni pojavom incidenta.(Primjer: aplikacija internetskog bankarstva, četiri poslužitelja u podatkovnom centru Rijeka, Oracle baza podataka V.X.Y, itd.) |
| Navedite broj krajnjih korisnika na koje je incident imao negativan učinak (u smislu izostanka ili narušavanja kvalitete usluge). | Upišite podatke. |
| **RJEŠAVANJE INCIDENTA** |
| Koji su interni resursi angažirani na rješavanju incidenta? | (Primjer: pet djelatnika IT sektora, tri djelatnika pravne službe, Član Uprave, PR tim) |
| Koji su vanjski resursi angažirani na rješavanju incidenta (vanjski eksperti, dobavljači, pravne službe, PR)? | (Primjer: pet djelatnika tvrtke X zadužene za mrežu, jedan djelatnik tvrtke za krizno komuniciranje) |
| Navedite očekivani rok oporavka od incidenta? | (Primjer: prema prvim procjenama oporavak bi trebao završiti kroz dva do tri dana) |
| Koje su mjere/aktivnosti poduzete u svrhu oporavka od incidenta? | Navedite mjere/aktivnosti koje su poduzete u svrhu oporavka od incidenta. (Primjer: 1. Održani sastanci s Upravom, dobavljačima i nadležnim CSIRT-om; 2. Aktivirana rezervna lokacija; 3. PR tim održao konferenciju za medije upoznavši ih s detaljima incidenta; 4. Ostvaren kontakt s međunarodnim poslovnim partnerima u svrhu dolaska njihovih stručnjaka za tehnologiju koju koristimo…)  |
| Jesu li aktivirani planovi očuvanja kontinuiteta poslovanja (BCP) i planovi oporavka u slučaju katastrofa (DRP)? Ako jesu, navedite osnovne aktivnosti iz tih planova koje su u tijeku. | (Primjer: aktivirana je rezervna lokacija na koju je preseljen dio zaposlenika kako bi usluga mogla nastaviti s funkcioniranjem; započet je oporavak podataka na primarnoj lokaciji korištenjem pričuvnih kopija…) |

1 Ako je došlo do promjene klasifikacije