Plan reagovanja na incidente — Dr Tijana

POVERLJIVO — dokument firme „Dr Tijana“ je priprema za Plan reagovanja na incidente. Ne distribuirati van BDB tima i ovlašćenih lica klijenta.

Datum generisanja: 07.11.2026. 23:22

Dokument je pripremljen na osnovu odgovora klijenta u upitniku za ovu uslugu. Pre usvajanja od strane rukovodstva, sadržaj proveriti, dopuniti i urediti.

1. Svrha i obim primene

Ovaj Plan reagovanja na incidente ("Plan") uređuje postupanje [NAZIV FIRME] u slučaju bezbednosnog incidenta koji pogađa informacione sisteme, podatke ili usluge firme. Plan obuhvata klasifikaciju incidenata, obaveze prijavljivanja Nacionalnom CERT-u u zakonskom roku od 24 sata, internu i eksternu komunikaciju, izolaciju pogođenih sistema i analizu uzroka nakon incidenta.

Plan se primenjuje na sve zaposlene i angažovana lica [NAZIV FIRME] koja koriste informacione sisteme firme, uključujući sisteme za zakazivanje i vođenje medicinske dokumentacije pacijenata. S obzirom na to da je osnovna delatnost [NAZIV FIRME] pružanje zdravstvenih usluga, posebna pažnja posvećuje se incidentima koji ugrožavaju dostupnost zakazivanja i vođenja medicinske dokumentacije, kao i poverljivost zdravstvenih podataka pacijenata.

Plan obuhvata sledeće tipove incidenata: curenje ili krađu podataka, kompromitovan nalog i ransomver napad. Ovim Planom se ne isključuje primena na druge vrste incidenata koji mogu ugroziti informacionu bezbednost firme.

2. Pravila i mere

2.1 Klasifikacija incidenata

Svaki uočeni incident klasifikuje se u jedan od sledeća četiri nivoa ozbiljnosti: nizak, srednji, visok, kritičan. Kriterijumi za svrstavanje incidenta u određeni nivo (uticaj na dostupnost zakazivanja i medicinske dokumentacije, obim pogođenih podataka o pacijentima, broj pogođenih naloga ili sistema) [KLIJENT DA DOPUNI: konkretni kriterijumi razgraničenja između nivoa nizak/srednji/visok/kritičan].

Incidenti koji uključuju curenje ili krađu zdravstvenih podataka pacijenata, kompromitovan nalog ili ransomver automatski se razmatraju kao incidenti sa potencijalno visokim ili

kritičnim nivoom ozbiljnosti, s obzirom na osetljivost podataka i direktan uticaj na mogućnost pružanja zdravstvenih usluga.

2.2 Prijavljivanje incidenta

Svako lice koje uoči bezbednosni incident ili sumnju na incident dužno je da o tome odmah obavesti direktora, [IME ODGOVORNOG LICA], koji je prva kontakt osoba za sve incidente u [NAZIV FIRME].

Direktor je ovlašćeno lice za komunikaciju sa nadležnim organima, uključujući Nacionalni CERT i inspekcijske organe, u slučaju bezbednosnog incidenta.

Incidenti koji ispunjavaju uslove za obaveznu prijavu Nacionalnom CERT-u prijavljuju se u zakonskom roku od 24 sata od trenutka saznanja za incident. Rok od 24 sata računa se od momenta kada je direktor obavešten o incidentu.

2.3 Interna komunikacija tokom incidenta

Tokom trajanja incidenta, obaveštavanje zaposlenih i drugih angažovanih lica o toku incidenta i merama koje je potrebno preduzeti sprovodi se po sledećem redosledu i kanalima komunikacije: [KLIJENT DA DOPUNI: ko koga obaveštava, kojim kanalom (npr. telefon, email, lično) i kojim redosledom tokom incidenta].

2.4 Obaveštavanje pogođenih pacijenata i korisnika

Kada incident ugrozi poverljivost, integritet ili dostupnost podataka pacijenata ili korisnika usluga [NAZIV FIRME], pogođena lica obaveštavaju se o incidentu. Rok, sadržaj obaveštenja i način obaveštavanja (telefon, email, pismeno obaveštenje) određuju se u skladu sa: [KLIJENT DA DOPUNI: rok za obaveštavanje pogođenih pacijenata, sadržaj i kanal obaveštenja, nosilac odgovornosti za slanje obaveštenja].

2.5 Izolacija pogođenih sistema

Po saznanju za incident koji ugrožava sistem zakazivanja, sistem za vođenje medicinske dokumentacije ili druge informacione sisteme [NAZIV FIRME], preduzimaju se mere izolacije pogođenog sistema radi sprečavanja daljeg širenja incidenta. Konkretni koraci izolacije (isključivanje sa mreže, privremeno gašenje sistema, promena pristupnih podataka) i lice zaduženo za njihovo sprovođenje: [KLIJENT DA DOPUNI: koraci izolacije po tipu incidenta i nosilac odgovornosti za njihovo sprovođenje].

2.6 Rezervni kanali komunikacije

U skladu sa naučenom lekcijom iz prekida internet veze koji se desio pre dve godine, kada

nije postojao rezervni kanal za zakazivanje pacijenata, [NAZIV FIRME] uspostavlja rezervnu mobilnu internet vezu kao alternativni kanal za nastavak rada sistema zakazivanja u slučaju prekida primarne internet veze. Aktiviranje rezervne veze sprovodi se odmah po utvrđivanju da je primarna veza nedostupna, a za njeno održavanje u funkcionalnom stanju i proveru dostupnosti zadužen je [KLIJENT DA DOPUNI: lice zaduženo za nabavku, održavanje i periodičnu proveru rezervne mobilne internet veze].

2.7 Analiza uzroka i evidencija incidenata

Nakon svakog incidenta nivoa srednji, visok ili kritičan, sprovodi se analiza uzroka incidenta (post-incident review) radi utvrđivanja uzroka, toka incidenta i mera za sprečavanje ponavljanja.

Svi incidenti, uključujući i one koji su blagovremeno sprečeni ili nisu prouzrokovali štetu, evidentiraju se. Evidencija incidenata vodi se u [KLIJENT DA DOPUNI: naziv alata/obrasca/registra u kojem se evidentiraju incidenti] i sadrži najmanje datum uočavanja, opis incidenta, nivo ozbiljnosti, preduzete mere i ishod.

3. Odgovornosti

Direktor je prva kontakt osoba za prijavu svakog uočenog incidenta, donosi odluku o klasifikaciji incidenta prema nivou ozbiljnosti, ovlašćen je za komunikaciju sa Nacionalnim CERT-om i drugim nadležnim organima, odgovoran je za poštovanje zakonskog roka od 24 sata za prijavu CERT-u, nadzire sprovođenje mera izolacije pogođenih sistema, pokreće analizu uzroka nakon incidenta i odgovoran je za praćenje usklađenosti [NAZIV FIRME] sa propisima o informacionoj bezbednosti.

Svi zaposleni i angažovana lica dužni su da odmah prijave direktoru svaki uočeni ili sumnjivi bezbednosni incident, da postupaju u skladu sa uputstvima dobijenim tokom reagovanja na incident i da ne preduzimaju samostalne mere koje nisu odobrene u toku incidenta, osim mera neodložne izolacije sopstvenog uređaja ili naloga radi sprečavanja širenja incidenta.

Lice zaduženo za vođenje evidencije incidenata i sprovođenje analize uzroka: [KLIJENT DA DOPUNI: nosilac odgovornosti za vođenje evidencije incidenata i sprovođenje post-incident review-a, ukoliko se razlikuje od direktora].

Formalni tim za reagovanje na incidente (IRT) sa definisanim ulogama trenutno nije uspostavljen u [NAZIV FIRME]; do uspostavljanja takvog tima, sve uloge iz ovog Plana vrši direktor, uz mogućnost angažovanja [KLIJENT DA DOPUNI: eksterni IT saradnik/pružalac usluga, ukoliko postoji, i njegova uloga u reagovanju na incidente].

4. Procedure

4.1 Prijava i prva reakcija
Korak 1: Lice koje uoči incident odmah obaveštava direktora, usmeno ili [KLIJENT DA DOPUNI: kanal prijave incidenta, npr. telefon, email].
Korak 2: Direktor procenjuje prirodu incidenta i svrstava ga u jedan od nivoa ozbiljnosti (nizak, srednji, visok, kritičan).
Korak 3: Za incidente nivoa visok ili kritičan, direktor nalaže neodložnu izolaciju pogođenog sistema u skladu sa tačkom 2.5 ovog Plana.

4.2 Prijava Nacionalnom CERT-u
Korak 1: Direktor utvrđuje da li incident podleže obaveznoj prijavi Nacionalnom CERT-u.
Korak 2: Ukoliko incident podleže prijavi, direktor sastavlja i dostavlja prijavu Nacionalnom CERT-u najkasnije u roku od 24 sata od saznanja za incident.
Korak 3: Sadržaj prijave i kontakt kanal ka Nacionalnom CERT-u: [KLIJENT DA DOPUNI: način podnošenja prijave CERT-u i obavezni sadržaj prijave].

4.3 Interna i eksterna komunikacija
Korak 1: Direktor obaveštava relevantna lica unutar [NAZIV FIRME] o incidentu u skladu sa tačkom 2.3 ovog Plana.
Korak 2: Ukoliko je incidentom ugrožena poverljivost, integritet ili dostupnost podataka pacijenata, direktor pokreće obaveštavanje pogođenih lica u skladu sa tačkom 2.4 ovog Plana.
Korak 3: Svaka komunikacija sa inspekcijskim organima ili drugim nadležnim institucijama vodi se isključivo preko direktora.

4.4 Oporavak i nastavak rada
Korak 1: Ukoliko je incidentom prekinut rad sistema zakazivanja usled nedostupnosti primarne internet veze, aktivira se rezervna mobilna internet veza u skladu sa tačkom 2.6 ovog Plana.
Korak 2: Po otklanjanju incidenta, direktor proverava da li su pogođeni sistemi (zakazivanje, medicinska dokumentacija) vraćeni u stanje pre incidenta pre nastavka redovnog rada.

4.5 Analiza uzroka i evidentiranje
Korak 1: Nakon okončanja incidenta nivoa srednji, visok ili kritičan, sprovodi se analiza uzroka incidenta najkasnije u roku od [KLIJENT DA DOPUNI: rok za sprovođenje post-incident review-a nakon okončanja incidenta].
Korak 2: Rezultati analize, uključujući uzrok, tok incidenta i preduzete mere, unose se u evidenciju incidenata.
Korak 3: Na osnovu analize uzroka, direktor odlučuje o potrebi izmene ovog Plana ili uvođenju dodatnih mera, uključujući i naučene lekcije iz prethodnih incidenata (npr. uvođenje rezervne mobilne internet veze nakon prekida interneta pre dve godine).

Ovaj dokument stupa na snagu danom usvajanja od strane rukovodstva Dr Tijana.

U _____, ____.____._____. godine

M.P.

Ovlašćeno lice:

_____