PROCEDURA ZA UPRAVLJANJE BEZBEDNOSNIM INCIDENTIMA

OZNAKA DOKUMENTA	MT16PRO01	**DATUM IZDANJA**	12-12-2023
PRIMERAK BROJ	01	**IZDANJE**	02

AUTORIZACIJA	**IME I PREZIME**	**FUNKCIJA**	**POTPIS**
PRIPREMIO	Vladimir Miladinović	Menadžer ISMS	
ODOBRIO	Boris Čorni	Rukovodilac IT sektora	

SADRŽAJ

1 ZAPIS O DOPUNI

Datum	Brojevi strane(a)	Detalji izmene	Broj zahteva za izmenu dokumenta

2 DISTRIBUCIJA I KONTROLA

2.1 DISTRIBUCIJA

Rb. broj	Funkcija/odeljenje
1	Sistem administrator
2	Menadžer za ISMS
3	IT služba

2.2 KONTROLA

Nekontrolisani primerci ovog dokumenta se mogu izdati zainteresovanim stranama ili kupcima organizacije shodno odluci Direktora. Održavaće se zapisi o svakom nekontrolisanom primerku. Svaki primerak će se datirati i označiti sa **„NEKONTROLISANI PRIMERAK - UNIŠTITI NAKON UPOTREBE”** na naslovnoj strani.

3 SVRHA

Cilj ove procedure jeste ublažiti negativne posledice bezbednosnih incidenata te obezbediti brže reagovanje na njih i uspostavljanje normalnog funkcionisanja operacija pogođenih incidentima. Procedura omogućava brzo dodeljivanje incidenata odgovornim licima, čime je omogućeno brzo i profesionalno reagovanje na njih kao i praćenje i rešavanje datih incidentnih situacija.

4 PODRUČJE PRIMENE

Procedura se odnosi na sve zaposlene u organizaciji Meridian Tech d.o.o. Beograd.

5 TERMINI I DEFINICIJE

U cilju boljeg razumevanja ISMS-a organizacije, u nastavku su navedene definicije značajnijih pojmova koji se koriste u ovoj proceduri.

U dokumentaciji ISMS-a organizacije se koriste sledeće skraćenice:

ISMS – (Information security management Sistems), Sistem menadžmenta zaštite i bezbednosti informacija - ISO/IEC 27001:2022.

6 REFERENTNA DOKUMENTA

ISO 27001:2022 *Sistem menadžmenta bezbednošću informacija - Zahtevi*

7 OPIS RADA

Šta je bezbednosni incident?

U kontekstu ovog dokumenta, bezbednosnim incidentom može se smatrati onaj koji ima jednu ili više sledećih osobina:

- Krši uslove jedne ili više Politika bezbednosti informacija
- Dovodi kompaniju u neku vrstu rizika npr. gubitak poverenja, integriteta ili dostupnosti podataka
- Može biti posledica neke namerne, zlonamerne aktivnosti
- Treba mu se pristupiti kao hitnom pitanju
- Uzrok incidenta možda nije najjasniji i zahteva pažljivu i poverljivu istragu

Zbog ovih posebnih osobina postavljene su smernice, kako bi se obezbedilo da se takvi incidenti pravilno istražuju.

7.1 PROCEDURA ZA PRIJAVU BEZBEDNOSNIH INCIDENATA

Ukoliko incidente otkriju zaposleni u organizaciji, problem se prijavljuje ISMS Menadžeru koji obaveštava dispečersku službu. Dispečerska služba otvara problem u Dispečer program sa sledećim informacijama:

- Status
- Kategorije
- Naslov
- Opis
- Ko je otvorio
- Otvoren
- Nastao
- Rešio
- Rešen
- Proteklo vreme
- Broj komentara
- Dodeljeni korisnici

Problem se može prijavit na sldeći način:

- Viber
- Skyp
- Redovnim internim mailom, adresirano na boris.corni@meridianbet.com

Takođe, radi veće bezbednosti obavestiti:

- Odgovornog menadžera
- Sistem administratora

Kada zaposleni prijavi bezbednosni incident preporučuje se sledeće:

- Prestati sa radom – ukoliko je moguće nastaviti diskretan rad sa svim aplikacijama
- Ne isključivati kompjuter ili bilo koju aktivnu aplikaciju
- Ne nastavljati upravljanje sistemom ili aplikacijom dok se ne dobije službeno ovlašćenje od strane IT da je moguće nastaviti sa normalnim radom
- Ne pričati o bezbednosnom incidentu osim sa ovlašćenim licima koja su uključenja u njegovo otklanjanje

Preporučuje se da zaposleni prijave sve potencijalne bezbednosne incidente, bez obzira da li će se oni kasnije pokazati kao pravi ili ne. Pored prijavljivanja bezbednosnih incidenata, postoje rešenja i automatski sistemi monitoringa koji mogu da pomognu pri ranom otkrivanju i rešavanju incidenata. Osobe odgovorne za nadgledanje ovih sistema monitoringa odgovorne su i za prijavljivanje incidenata.

Takodje, u okviru ove procedure se nalazi i dokument Informacije o pretnjama koji predstavlja šablon, dok se detalje informacije nalaze u poviru Dispečar programa.

7.2 PROCEDURE ZA UPRAVLJANJE BEZBEDNOSNIM INCIDENTIMA

Menadžer ISMS-a je vođa i glavni koordinator aktivnostima vezanim za incidente. Ukoliko je potreban tim za reagovanje na incidente, njega će činiti:

- Menadžer ISMS-a
- Sistemskog administratora
- Odgovoran menadžer
- Odgovornu osobu za Sektor ljudskih resursa – koordinator disciplinskih mera

U zavisnosi od ozbiljnosti incidenta timu se mogu priključiti i dodatni članovi, a to su:

- Predstavnik određene državne agencije
- Eksterni konsultanti i saradnici

Procedure za upravljenje bezbednosnim incidentima su :

- Ograničiti neposredni uticaj incidenta
- Analiza i identifikacija uzroka incidenta
- Kategorizacija incidenta
- Uvođenje ograničenja rada i zabrana koje proizilaze iz incidenta
- Pružanje uputstava krajnjim korisnicima za rad u datim uslovima
- Planiranje i implementacija preventivnih kontrola u slučaju greške ili sumnje u rešenje

- Planiranje i implementacija korektivnih mera kako bi se sprečilo ponavljanje incidenta
- Komuniciranje sa uključenima ili pogođenima datim incidentom
- Izveštavanje o preduzetim aktivnostima prilikom upravljanja incidentom
- Obavestite nadležne vlasti (policija, tužilaštvo, CERT..)

U slučaju pojave bezbednosnog incidenta, zaposleni je odgovoran da prikupi i zaštiti sve dokaze i tragove koji bi mogli da posluže internoj analizi incidenta kao istražni materijal, ili koji bi se koristili prilikom pregovora o kompenzaciji nabavke softvera i hardvera.

Aktivnosti preduzete za obnovu, popravku i ispravku formalno se kontrolišu, i uzimaju u obzir:

- Pristup ovlašćenim osobama proizvodnim podacima, sistemu i okruženju
- Dokumentaciju o svim hitnim i odmah preduzetim merama
- Izveštavanje menadžmenta o odmah preduzetim merama i o njihovom nadgledanju

7.3 OBAVEŠTENJE O BEZBEDNOSNIM INCIDENTIMA

Rešenje incidenta se evidentira u Dispečar programu, gde se nakon što je problem uspešno rešen, status označava kao "REŠEN". Ovaj postupak omogućava praćenje i dokumentovanje svih aktivnosti u vezi s incidentom, što doprinosi boljoj organizaciji i efikasnosti rada.

7.4 SAKUPLJANJE DOKAZA U SLUČAJU BEZBEDNOSNIH INCIDENATA

Posebno (ali ne isključivo) ako se sumnja da je po sredi “prljava igra”, moraju se voditi tačni zapisi o svim preduzetim aktivnostima i prikupiti dokazi.

Svi podaci u vezi bezedonosnog incidenta beleže se u dispečar program.

Dokazi će možda biti potrebni:

- za dalju analizu uzroka incidenta
- kao forenzički dokaz u krivičnim i građanskim sudskim postupcima
- kao podrška prilikom pregovora o kompenzaciji sa dobavljačima softvera ili servisa

U slučaju kada izbijanje bezbednosnog incidenta dovede do podnošenja privatne tužbe protiv osobe ili organizacije, dokazi koji će biti predstavljeni u procesu moraju se sakupiti. Sledeće treba uzeti u obzir:

- Prihvatljivost dokaza, mogu se koristiti na sudu ili pri sprovođenju disciplinskih mera
- Jačina dokaz, kvalitet i celovitost dokaza

U slučaju dokaznog dokumenta u papirnoj formi, dokaz se čuva na sigurnoj lokaciji sa mogućnošću ulaza osobe koja ga je otkrila. U slučaju dokaznih informacija koje se čuvaju na kompjuterskim medijima, informacije se čuvaju na medijima kako bi se omogućio pristup pohranjenim informacijama. Originalni mediji i tragovi čuvaju se na bezbednosnim lokacijama van mogućnosti pristupa. Sve istražne aktivnosti sprovode se na kopijama izvornih podataka. Stepen integriteta i brige održavaju se na najvišem nivou.

7.5 VRSTE INCIDENATA

Vrste informacione imovine:

- Informacije (datoteke podataka, baze podataka, Informacije o klijentima, itd.);
- Pisani dokumeni (ugovori, uputstva za upotrebu, smernice, radni papiri, itd.);
- Softver (aplikacije, sistemski softveri, prilagođeni softveri, itd.);
- Hardver (kompjuteri, mediji,itd.);
- Ljudi (zaposleni, osoblje, klijenti, itd.);
- Imidž i reputacija kompanije;
- Servisi (komunikacioni, tehnički, itd.)

Informaciona imovina može biti ugrožena po osnovu:

- Poverljivost - informacije su dostupne samo ovlašćenim licima i neće biti otkrivene neovlašćenim licima, namerno ili nepažnjom;
- Integritet podrazumeva da informacioni sistem primenjuje odgovarajuće mera kako bi se zaštitio od neovlašćene modifikacije, i da sadrži kompletne, tačne i pouzdane informacije;
- Raspoloživost – ovlašćeno lice ima pristup informacijama i infromacionom sistemu kada za to imaju poslovnu potrebu .

Primeri bezbednosnih incidenata koje zaposleni treba da prijave su:

Gubitak, tj. gubitak servisa, opreme, prostora, resursa ili sredstava zbog:

- Prekida u radu servisa
- Isključenja provajdera IT servisa;
- Prekida rada / nestanka struje;
- Prekida rada ključne opreme za klimatizaciju prostora
- Incidenata / nesreća pruzrokovane prirodnim katastrofama
- Incidenata u slučaju izbijanja požara

Sisitemske smetnje / preopterećenja, kvar softvera, hardvera ili komunikacionih sistema

- Stalno smanjene performansi aplikacija;
- Duži prekidi u softverskih rešenja;
- Smanjena tačnost i potpunost podataka o klijentima i transakcija;
- Greške u obradi podataka;

Ljudske greške, zloupotrebe, odstranjivanja i otkrivanja informacija i resursa

- Namerno pogrešno rukovanje opremom;
- Neovlašćeno objavljivanje poverljivih informacija (stanje računa);
- Otkrivanje lozinke, korišćenje lozinke druge osobe;
- Objavljivanje ličnih podataka o klijentima trećim, neovlašćenim licima;
- Greške su rezultat nepotpunih podataka;
- Kršenje odredbi fizičke bezbednosti.

Krađa ključnih informacionih sistema (hardvera, softvera, komunikacionih sistema)

- Kretanje neovlašćenih osoba u sigurnosnim zonama kompanije
- Prisustvo neovlašćenih stranih ugovarača u kompaniji

Nekontrolisane promene u sistemu i napadi

- Hakerski napadi;
- Napadi virusa;
- Poricanje napada na servis;
- Zlonamerni programski kod;
- Samovoljna instalacija neodobrenih softvera ili uređaja;
- Nekontrolisane promene usled promena u proizvodnji i konfiguraciji;
- Nepravilno ponašanje sisitema - indikacija napada;

Neovlašćeni pristup resursima i informacijama

- Neovlašćeni pristup kompjuterskim mrežama / aplikacijama;
- Neovlašćeni pristup delovima aplikacije za koje zaposleni nema ovlašćenje

Ostala kršenja bezbednosne politike informacionog sistema kompanije. Strane upletene u incident ili mogući uzrok incidenta:

- Zaposleni
- Strana lica (pripravnici, studenti, konsultanti...)
- Pružaoci servisa

8 ODGOVORNOSTI I OVLAŠĆENJA

ISMS Menadžer je odgovoran za planiranje i organizovanje aktivnosti Procedure za upravljanje bezbednosnim incidentima. Za kontrolu primene procedure ovlašćen je Direktor.

9 ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje bezbednosnim incidentima formiraju deo dokumentovanih informacija organizacije Meridian Tech d.o.o. Beograd. Dokumentovane informacije se moraju zadržavati i održavati u skladu sa ovim postupkom.

U realizaciji ovog postupka nastaju zapisi, odnosno dokumentovane informacije navedeni u tabeli.

Naziv	Referentna oznaka obrasca	Vreme čuvanja	Mesto čuvanja	Odgovorno lice

10 PRILOZI

Nema.