POLITIKA UPRAVLJANJA TEHNIČKIM RANJIVOSTIMA

OZNAKA DOKUMENTA	*MT12POL02*	DATUM IZDANJA	*11-12-2023*
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
1	IT podrška
2	Menadžer za ISMS
3	System administrator

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

Ovaj dokument definiše politiku organizacije Meridian Tech d.o.o. Beograd o tome kako će se proceniti i upravljati tehničkim ranjivostima u IT okruženju. Namenjen je za IT podršku i za menadžment nadležan za bezbednost informacija kao i za pomoćno osoblje koje će implementirati i održavati bezbednost u kompaniji.

Ova politika pokriva sledeću kontrolu:

- 8.8 Upravljanje tehničkim ranjivostima

4. PODRUČJE PRIMENE

Dokument se koristi u celom informacionom sistemu kompanije.

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 systems), Sistem menadžmenta zaštite i bezbednosti informacija – ISO/IEC 27001:2022.

6. REFERENTNA DOKUMENTA

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

7. OPIS RADA

7.1 UPRAVLJANJE TEHNIČKIM RANJIVOSTIMA

7.1.1 Pretnja

- Malware je bilo koji kod softvera koji može biti štetan ili destruktivan na kapacitete za obradu informacija u organizaciji i jedan je od osnovnih alata koji se koristi od strane napadača da se zaobiđe bezbednost kako bi ostvario neku vrstu dobiti ili pak da poremeti normalno funkcionisanje poslovanja.

- Bitno je da su efikasne mere preduzete od strane kompanije da se zaštiti protiv ovih pretnji koje mogu doći iz više izvora uključujući organizovane bande, konkurentske organizacije, politički motivisane grupe, nesavesne zaposlene, jedinice za “sajber ratovanje” sponzorisane od strane država ili jednostavno pojedince koji vežbaju radoznalost ili testiraju svoje veštine.

- Bez obzira na izvor, rezultat uspešne povrede bezbednosti jeste kada su pogođeni organizacija i njeni akteri, ponekad ozbiljno, a šteta je svakako prouzrokovana.

- Zlonamerni programi dolaze u mnogim oblicima, i stalno se menjaju kako se prethodni putevi napada zatvaraju, i pronalaze se novi. Najčešći tipovi malvare danas su:
    - Virus
    - Trojan
    - Crv
    - Logička bomba
    - Rootkit
    - Keylogger
    - Backdoor

Često se ove vrste zlonamernih programa koriste u međusobnoj kombinaciji.

Da bi zlonamerni softver sproveo svoju namenjenu ulogu treba da bude instaliran na ciljnom uređaju ili računaru. Postoji nekoliko ključnih načina na koji zlonamerni softver inficira računare i mreže, iako se novi načini stvaraju neprekidno.

Najčešće tehnike infekcije koje se koriste od strane napadača jesu one koje nastoje da iskoriste ranjivosti u našem sistemu bezbednosti.

7.1.2 Šta je tehnička ranjivost?

Ranjivost je definisana u posebnoj publikaciji NIST 800-30 Rev 1 kao "ugrađena postojeća slabost u informacionom sistemu, bezbednosnim procedurama, internim kontrolama, ili implementacija koja bi mogla da se koristi kao izvor pretnje."

- Proces razvoja softvera je komplikovan i njegov izlaz u obliku softverskih programa je retko bez tzv. bagova (bug). Većina ovih grešaka jednostavno utiče na funkcionalnost softvera tako da on ne radi kako je predviđeno tokom razvoja. Međutim, ako se manipuliše u pravom smeru tokom razvoja, neko može dozvoliti napadaču da dobije neki oblik prednosti ili pristup koji nije bio namenjen od strane programera. Ova vrsta greške se obično smatra softverska ranjivost .

- Ove ranjivosti se stalno pronalaze i ispravljaju putem softverskih ažuriranja (updates) ili putem zakrpa (patches). Nažalost, nije uvek programer ili korisnik taj koji otkriva ove ranjivosti. Kada se otkrije od strane potencijalnog napadača, ranjivost postaje nešto što se koristi za dobit i drži se, naravno, u tajnosti što je duže moguće. Novootkrivena ranjivost se često naziva "zero day exploit " i teško je braniti se protiv ovih ranjivosti.

- Politika kompanije u pogledu tehničkih ranjivosti jeste biti svestan njihovog postojanja i gde god je to moguće nastojati da se ove ranjivosti zatvore, bilo direktno ili indirektno preko drugih sredstava.

7.1.3 Izvor informacija

- Prvi korak u upravljanju tehničkim ranjivostima je da ih postanemo svesni. Pošto govorimo o tehničkim ranjivostima one će naravno zavisiti od tehnologije primenjenih unutar organizacije. Neophodno je onda da se uspostavi puno razumevanje tehnoloških komponenti koje čine infrastrukturu organizacije i njihove verzije (jer je većina tehničkih ranjivosti veoma vezana za verzije).

Ovo treba da uključi:

- Operating systems e.g. Windows, UNIX, Cisco
- Databases e.g. SQL Server, MySQL
- Web servers e.g. IIS, Apache
- Desktop software e.g. Office, Acrobat
- Web technologies e.g. Flash, Java
- Application software e.g. SAP, Alfresco
- Hardware e.g. servers, routers

- Inventar softvera bi trebao uključivati dobavljača softvera, naziv softvera, brojeve verzija, trenutno stanje implementacije (npr. koji softver je

instaliran na kojim sistemima) i osobu(e) unutar organizacije odgovorne za softver.

- Ove informacije treba da budu dostupne u Configuration Management Database (CMDB) kompanije ukoliko takva baza postoji.

- Informacije o ranjivosti sa bilo koje od gore navedenih komponenti su generalno dostupne od vendora (prodavca) koji će izdati ažuriranja (update) i zakrpe da se poprave one ranjivosti za koje smo svesni da postoje.

- Proces stoga treba uspostaviti kako bi se osiguralo da se sve relevantne informacije o update-ima primaju i pregledaju od strane nadležnog osoblja ili IT podrške. Ovde se obično daju i smernice o nivou hitnosti u vezi svakog ažuriranja.

- Gde se promene konfiguracije preporučuju za zatvaranje ranjivosti, ovo bi trebalo da bude preduzeto kroz proces upravljanja promenama kompanije, tako da su odgovarajuće kontrole uspostavljene za testiranje, za procenu rizika i za backout plan (restore na period pre sistemske ili softverske integracije).

7.1.4 Zakrpe i ažuriranja

- Zakrpe i ažuriranja se obično izdaju od strane proizvođača softvera prema redovnom rasporedu u vidu kumulativnih paketa. One su uvek povezane sa specifičnom verzijom softvera, koja se odnosi i možda ima zavisnosti predviđene sa drugim softverskim modulima, proizvodima ili operativnim sistemima.

- Zahtevati od dobavljača informacionog sistema (uključujući njihove komponente) da osiguraju izveštavanje o ranjivostima, rukovanju i obelodanjivanju, uključujući zahteve u primenjivim ugovorima

- Procedure treba da se uspostave da bi se dobile kopije softverskih ažuriranja elektronskim putem kada budu izdate od strane vendora. Zakazivanje instalacije ažuriranja će zavisiti od niza faktora, uključujući:
    - Kritičnost sistema koji se ažuriraju
    - Očekivano vreme potrebno da se instalira ažuriranje
    - Stepen rizika povezan sa bilo kojom ranjivošću koja je zatvorena putem update-a
    - Koordinacije ažuriranja povezanih komponenti infrastrukture
    - Zavisnosti između ažuriranja

Treba stvoriti i održavati plan puštanja ažuriranja kako bi se pratilo kada će biti ažuriranje raznih sistema, uzimajući u obzir faktore navedene gore. Plan mora da se upravlja kroz proces upravljanja promenama. Za ispravke koje su niskog rizika i redovne, standardna promena može biti definisana u okviru procesa upravljanja promenama tako da dozvolimo da se to desi sa što manje administracije.

7.1.5 Procena ranjivosti

- Pored redovne primene vendora koji isporučuje ažuriranja softvera, kompanija će sprovesti procenu ranjivosti najmanje dva puta godišnje. Fokus procene ranjivosti treba da se rukovodi prema najnovijoj proceni rizika.

- Svrha ove procene je da identifikuje postojeće slabosti u sistemima u kojima mogu biti iskorišćene od strane napadača. To mogu biti poznate softverske ranjivosti za koje nisu urađene zakrpe, kao i konfiguracione greške koje treba da budu razmotrene.

- Procena može biti izvedena u kompaniji, od strane eksterne kompanije, ili kombinacija oba načina, a kao minimum treba da obuhvati:

- Procenu bezbednosti svih ruta u unutrašnjoj mreži kompanije (od Interneta)
- Web serveri
- Poslovno kritični serveri na internoj mreži
- Izbor tipičnih korisničkih računara

- Ako sredstva dozvoljavaju, dodatne oblasti treba proceniti kao što je ranjivost zaposlenih na phishing napade.

- Nije politika ove organizacije da pokušava da iskoristi slabosti zaposlenih, ali ovu vrstu penetracionog testa može da naruči kao potrebnu koristeći spoljne stručne resurse kao deo pažljivo planirane vežbe obavljene izvan redovnog radnog vremena.

7.1.6 Ojačavanje konfiguracije

- Dalje akcije koje treba preduzeti da se smanji broj i obim ranjivosti unutar sistema kompanije je ojačavanje konfiguracije servera i drugih uređaja. To podrazumeva zatvaranje usluga i protokola koji nisu potrebni, tako da je polje napada suženo.

- Ove aktivnosti ojačavanja treba sprovesti u skladu sa smernicama vendora i pod kontrolom procesa upravljanja promenama.

7.1.7 Trening podizanja svesnosti

Kao rezultat procene ugroženosti može biti neophodno da se povećaju napori obukom podizanja svesnosti o bezbednosti za zaposlene i osoblje pod ugovorom. Ova obuka treba da objasni prirodu ranjivosti i šta se može učiniti da se one smanje.

8. ODGOVORNOSTI I OVLAŠĆENJA

Potrebno je čuvati zapis o svakoj aktivnosti koja je preuzeta. Proces upravljanja tehničkim ranjivostima mora se redovno pratiti, proveravati i ocenjivati, kako bi se osigurala efikasnost i efektivnost.
ISMS Menadžer je odgovoran za sprovođenje ove politike u saradnji sa IT podrškom kao i za nadzor nad njihovim radom u vezi sa planiranjem i organizovanjem aktivnosti. Za kontrolu primene politike ovlašćen je Direktor.

9. ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje tehničkim ranjivostima 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.