Pravilnik o provjeri ranjivosti mrežnih resursa informacijskog sustava

SADRŽAJ

POPIS PRILOGA
Prilog 1
Prilog 2
Prilog 3

NAPOMENA:

Gore navedeni vezani dokumenti kojih je vlasnik Opća bolnica Varaždin su iz razloga jednostavnosti korištenja izrađeni kao zasebni dokumenti a smatraju se sastavnim dijelom ovog dokumenta. Isti su dostupni osoblju u skladu sa distribucijom pojedinog dokumenta te putem Intranet portala na način da se nalaze u istoj radnoj mapi gdje i ovaj priručnik.

VEZANI DOKUMENTI	
1	Politika sigurnosti informacijskog sustava
2	Pravilnik o upravljanju mrežnom infrastrukturom
3	Metodologija upravljanja rizicima informacijskog sustava

NAPOMENA:

Gore navedeni vezani dokumenti su izrađeni kao zasebni dokumenti nužni za pravilno razumijevanje sadržaja ovog dokumenta ali se ne smatraju njegovim sastavnim dijelom. Isti su dostupni osoblju putem Intranet portala.

Distribucija dokumenta

Broj kopije	Mjesto/lokacija/radno mjesto	Format	Količina	Datum	Potpis
	OPĆA BOLNICA VARAŽDIN				
1	Uprava	Tiskana kopija	1		
N/A	Odjel za informatiku	Digitalna kopija	N/A		
N/A	N/A	Digitalna kopija	N/A		

Revizija dokumenta

Redni broj	Datum	Reviziju izradio	Reviziju odobrio	Naziv i broj poglavlja koje se mijenja/opis revizije
1	16.11.2022.	D. Uremović	D. Poljak	Cijelo izdanje

1. Namjena

Ovim Pravilnikom o provjeri ranjivosti mrežnih resursa informacijskog sustava Opće bolnice Varaždin (u nastavku: OBV ili Bolnica) omogućava se ostvarenje sljedećih ciljeva:

- veća razina zaštite OBV-ovih zaposlenika, sustava i infrastrukture,
- identifikacija i smanjivanje rizika za OBV-ove mrežne resurse informacijskog sustava (npr. poslužitelje, mrežnu opremu, baze podataka) na prihvatljivu razinu,
- upravljanje konfiguracijama mrežnih resursa IS-a u skladu s dobrim svjetskim sigurnosnim praksama.

2. Opseg

S obzirom na sadržaj ovog pravilnika, propisana pravila odnose se na djelatnike OBV-a i vanjske partnere koji upravljanju sigurnosnim politikama resursa informacijskog sustava (uprava, Informatika, VSIS) te na one koji provode te politike (skrbnici mrežnih resursa).

Pravilnik se odnosi na fizičke ili virtualne resurse informacijskog sustava OBV-a koji su spojeni na mrežnu infrastrukturu, primjerice poslužitelje, mrežnu opremu, sustave za upravljanje bazama podataka i „out-of-the-box" aplikacijama odnosno na njihove operativne sustave. Upravljanje rizicima ostalih tipove informacijske imovine obuhvaćeno je Metodologijom upravljanja rizicima informacijskog sustava.

3. Nadležnosti i odgovornosti

Voditelj sigurnosti informacijskog sustava (VSIS) je odgovoran za razvoj i ažuriranje ovog Pravilnika. Također je odgovoran za izradu plana skeniranja ranjivosti, analize rezultata skeniranja i predlaganja opcija za uklanjanje neprihvatljivih rizika.

Skrbnici mrežnih resursa informacijskog sustava (administratori sustava) su odgovorni za primjenu sigurnosnih mjera za umanjivanje rizika u dogovoru s voditeljem sigurnosti informacijskog sustava te u skladu s procedurom za upravljanje promjenama u informacijskom sustavu. Također pomažu VSIS-u u interpretaciji rezultata skeniranja te predlaganju mjera za umanjivanje rizika.

Rukovoditelj Odjela za informatiku odgovoran je za implementaciju eventualnih tehničkih procedura vezane uz ovaj Pravilnik.

4. Planiranje provjera ranjivosti

Skeniranja mrežnih resursa za provjeru ranjivosti se trebaju raditi na kvartalnoj osnovi. Ažurirani katalog informacijske imovine će se koristiti za planiranje skeniranja.

Plan skeniranja se izrađuje na godišnjoj osnovi, a ovisi o sljedećim kriterijima mrežnih resursa:

- Podržavaju rad kritičnih funkcija informacijskog sustava,
- Sadrže visoko osjetljive podatke odnosno informacije,
- Nisu bili duže vremena uključeni u skeniranje ranjivosti,
- Podliježu posebnim uredbama i regulativi odnosno zahtjevima Uprave.

Prije pokretanja postupka skeniranja potrebno je dobiti odobrenje skrbnika resursa kako bi se smanjila mogućnost negativnog utjecaja izvršavanja skeniranja na rad resursa odnosno poslovnih procesa OBV-a.

Svi poslužitelji i mrežna oprema bi se trebali skenirati minimalno jednom godišnje, nevezano uz kriterije za planiranje skeniranja.

5. Izvršavanje provjere ranjivosti

Provjere ranjivosti se trebaju izvršavati upotrebom specijaliziranih automatiziranih softverskih rješenja koja imaju mogućnost provjere i rangiranja ranjivosti prema CVSS shemi. VSIS mora odobriti upotrebu takvog alata prije korištenja.

Skeniranje ranjivosti se mora obavljati u vrijeme u kojem je moguće očekivati najmanje moguće negativne efekte na mrežne resurse odnosno informacijski sustav u cjelini (npr. tijekom noćnih sati).

Skeniranje s pokušajima iskorištavanja ranjivosti (engl. intrusive scans) se ne smiju provoditi kako bi se smanjila mogućnost negativnih efekata skeniranja. Ovakva skeniranja mogu biti dio posebno ugovorenih poslova penetracijskog testiranja sustava.

Skeniranja bi po mogućnosti trebalo raditi s dodijeljenim privilegiranim pravima na mrežne resurse kako bi se otkrilo što više poznatih ranjivosti.

Rezultati skeniranja sadrže visoko osjetljive podatke (ranjivosti) o mrežnim resursima te se moraju označiti kao „Osjetljivi“. Upravljanje takvom vrstom dokumenata propisano je Pravilnikom o klasifikaciji podataka.

6. Analiza rezultata i implementacija kontrola

VSIS, zajedno sa skrbnicima mrežnih resursa informacijskog sustava će pregledati rezultate skeniranja ranjivosti i propisati mjere za smanjivanje ranjivosti sukladno prepoznatim rizicima. Preporuke ne moraju nužno biti jednake onima koje sami softverski alati za provjeru ranjivosti predlažu.

Preporuke za smanjivanje ranjivosti potrebno je provesti u skladu s važećim Postupkom za upravljanje promjenama u informacijskom sustavu. Ove preporuke sadrže listu ranjivosti, visinu sigurnosnog rizika, opis ranjivosti, opis preporuke, rokove za implementaciju mjera te odgovorne osobe.

Rokovi za implementaciju mjera za smanjivanje ranjivosti određuju se u skladu s kriterijima u tablici niže:

Kritičnost	Opis	Očekivani rok
Kritično (Critical)	Kritične ranjivosti imaju CVSS ocjenu od 8.0 pa naviše. Lako ih je moguće iskoristiti uz pomoć javnih alata za iskorištavanje ranjivosti.	30 dana
Visoko (High)	Visoko opasne ranjivosti imaju CVSS ocjenu od 8.0 pa naviše, ali nisu jednostavne za iskorištavanje od strane zlonamjernih osoba.	90 dana
Srednje (Medium)	Srednje opasne ranjivosti imaju ocjenu CVSS od 6.0 do 8.0.	180 dana
Nisko (Low)	Nisko rangirane ranjivosti imaju CVSS ocjenu od 4.0 do 6.0. S obzirom na rizičnost te mogućnosti mitigacije ranjivosti nisu uvijek lake za otklanjanje.	360 dana
Informacija (Information)	Ranjivosti koje su procijenjene kao one "informativnog" karaktera imaju CVSS ocjenu nižu od 4.0. Ovakve ranjivosti nije potrebno otklanjati, ali se i mogu, u skladu s raspoloživim resursima.	Nije propisano

7. Izvješćivanje

VSIS izrađuje godišnje izvješće o provjeri ranjivosti mrežnih resursa informacijskog sustava koje može biti i poglavlje u godišnjem izvješću o radu VSIS-a. Izvješće se šalje ISMS odboru na usvajanje.

Izvješće o provjeri ranjivosti sadrži:

- Sumarni prikaz pronađenih ranjivosti na mrežnim resursima,
- Opseg provjere ranjivosti,
- Broj provedenih skeniranja,
- Statističke podatke o pronađenim ranjivostima i predloženim kontrolama za smanjivanje rizika,
- Preporuke za unaprijeđene procesa, ukoliko je potrebno.

8. Nepridržavanje

Svako nepridržavanje ovog pravilnika i ostalih sigurnosnih politika, zakona, općih akata i drugih dokumenata može biti sankcionirano sukladno zakonskim propisima i internim aktima OBV.

9. Završne i prijelazne odredbe

Pravilnik stupa na snagu i primjenjuje se danom njegovog donošenja.

KLASA: 011-02/23-01/15

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

Dr. sc. Damir Poljak, mag.soc.geront.