Sveučilište u Zagrebu
Veterinarski fakultet

Odsjek za informatiku
Ur. broj: 034-2025-010

Zagreb, 21. studenoga 2023.

Sigurnost računalne mreže Fakulteta, procjene rizika i prijedlog radnji za poboljšanje stanja

U ovom dokumentu navodimo procjenu sigurnosti naše računalne mreže, o postojećim rizicima i mogućem unapređenju postojećeg stanja.

Mreža Veterinarskog fakulteta je postavljena tako da su na glavno čvorište mreže koje se nalazi u Knjižnici, svjetlovodnim, bakrenim i bežičnim vezama spojena podčvorišta za pojedine zgrade ili organizacijske jedinice. S obzirom da je postavljanje mreže obavljeno prije više od 20 godina, na svim čvorištima nisu poštivani isti standardi (mrežni ormarić, upravljivi preklopnik). Tijekom vremena smo, uvažavajući dostupna sredstva, pokušavali mrežu što više unaprijediti (postavljanjem novih vodova i obnavljajući dotrajale uređaje).

Mreža na kojoj se zasniva naše poslovanje sastoji se od više poslužiteljskih računala koja omogućuju osnovne funkcionalnosti računala, pristup poslovnim podacima i internetu. Podijeljena je u više segmenata (eng. *VLAN – Virtual LAN*), kako bi osjetljivi podaci bili odvojeni i sakriveni od javno dostupne mreže.

S obzirom da se u našu mrežu priključuju studenti i brojni vanjski korisnici, računala koja nisu registrirana, spajaju se u odvojeni dio mreže koji ne smanjuje kvalitetu veze, ali ograničava dostupnost pojedinih usluga.

Poslužiteljska računala su zaštićena antivirusnim programom i vatrozidom (eng. *firewall*). Prilikom nabave računala, na sva računala postavljamo antivirusni program. S CARNet-om je ugovorena usluga „Provjera ranjivosti“ kojom se ispituju moguće točke rizika na mreži u pravilnim vremenskim razmacima te nas se obavještava o uočenim rizicima, na osnovu čega s tvrtkom Pouzdani sustavi planiramo potrebna poboljšanja sigurnosti mreže.

Pohrana podataka se obavlja redovito na više lokacija u više kopija. Zbog nedostatka prostora pohranjuju se samo podaci, a ne čitava poslužiteljska računala, što može usporiti povratak poslovanja nakon incidenta.

Postojeći rizici:

1. starost poslužiteljskih računala – postojeća poslužiteljska računala su starija od 10 godina; te je s obzirom na godinu proizvodnje vrlo teško izvediva hardverska nadogradnja. Nažalost, zbog prakse proizvođača softvera, kojom se redovito ukida podrška za starije sustave te je nadogradnje sve teže obaviti te predstavljaju dodatni rizik.
2. softverski sigurnosni propusti – povezano s prethodnom točkom i teško izvedivom nadogradnjom moguća je zloporaba sigurnosnih propusta u sistemskom softveru
3. nepotpuna pokrivenost mreže upravljivim preklopnicima što otežava upravljanje računalnom mrežom
4. mogućnost spajanja neautoriziranih korisnika u mrežu, žičnu, na nezaštićenim mrežnim čvorištima, kao i bežičnu postavljanjem privatnih, loše zaštićenih, bežičnih mreža
5. nekontrolirano spajanje uređaja na mrežu kao i neautorizirano premještanje ključnih uređaja za rad mreže
6. upotreba aplikacije Ambulantni protokol koja se bazira na starom sustavu koji omogućuje previše točaka rizika (svako računalo na kojem je instalirana aplikacija, a pogotovo ona s loše odabranim i skupnim lozinkama); aplikacija zahtijeva autorizacijske postavke servera na svakom računalu, izlažući bazu podataka riziku; ne koristi se SSL protokol koji bi zaštitio podatke tijekom mrežnog prometa
7. distribucija slikovnih dijagnostičkih zapisa (RTG, UZV, CT i sl.) na temelju *file share* protokola, kojim je relativno jednostavno doći do podataka o pacijentima i vlasnicima
8. dozvola *administratorskih* ovlasti korisnicima na računalima što olakšava moguće napade
9. nemogućnost kontrole privatnih prijenosnih računala koja se spajaju u sustav bez prethodno postavljene odgovarajuće zaštite

10. korištenje javno poznatih lozinki na računalima koja koristi više korisnika
11. bežična mreža *'vef',* s javno dostupnom i poznatom lozinkom
12. računala računovodstva spojena u javnu mrežu

Prijedlog poboljšanja sigurnosnog stanja na mreži

1. Starost postojećih poslužiteljskih računala moguće je riješiti na dva načina: 1. nabavom novih poslužiteljskih računala (uz nabavu ostale podložne opreme, npr. *backup* uređaja, komunikacijskih ormara, sustava napajanja i sl), 2. prebacivanjem prioritetnih poslužiteljskih računala u tzv. oblak (eng. *cloud*). Iako zvuči kao skuplja opcija, treba obratiti pažnju na to, da pružatelj usluge *oblaka* nudi brojne pogodnosti, kao što je stalna briga o ispravnom radu opreme, nadogradnja hardvera i softvera, kvalificirana radna snaga, briga o sigurnosti podataka, pohrana podataka (kao i cjelokupnih poslužiteljskih računala) u više kopija razdvojenih prostorno (različite seizmičke zone) i vremenski (važno zbog mogućnosti kompromitiranja podataka kroz duže vremensko razdoblje). Prednost te tehnologije je i u činjenici da pružatelj usluge kroz prikladnu edukaciju svojih djelatnika i stalnu nadogradnju opreme jamči dostupnost i sigurnost podataka. S obzirom na trenutne kvalifikacije djelatnika Odsjeka, vrlo je teško očekivati suvereno vladanje novim kompleksnim tehnologijama.
2. Iako se poslužiteljska računala redovito softverski nadograđuju, starost opreme sve više ograničava hardversku nadogradnju te otvara vrata rizicima, a riješilo bi se prebacivanjem u *oblak*.
3. S obzirom na vremenski period kad je prvotno postavljena mreža na Fakultetu, koristili su se neupravljivi preklopnici koji ne omogućuju podešavanje i postizanje sigurnosnih standarda. S obzirom da su upravljivi preklopnici, koji omogućuju segmentiranje mreže kao i veću sigurnost, cijenom postali dostupni, tekućom nabavom povećali smo njihov broj. Želimo li postići dovoljnu razinu sigurnosti na tom nivou, potrebno je zamijeniti još oko 30% uređaja.

4. Neautorizirani pristup mreži se može spriječiti ugradnjom javno dostupne mrežne opreme u komunikacijske ormariće, osigurane ključem. Svakako bi trebalo spriječiti korisnike da samoinicijativno spajaju mrežne i slične uređaje u sustav, jer postavljanjem neodgovarajućih postavki mogu znatno unazaditi sigurnost te dovesti do nedostupnosti mreže, što se redovito događa.
5. Nekontrolirano spajanje ključnih uređaja za rad mreže i njihovo neautorizirano premještanje moguće je spriječiti na isti način kao u prethodnoj točki.
6. Svjesni važnosti i osjetljivosti podataka koji se vode kroz aplikaciju Ambulantni protokol, predlažemo dva rješenja: 1. kodiranje aplikacije u nekom suvremenom programskom jeziku, možda kao mrežno dostupne aplikacije koja bi omogućila funkcionalnost bez obzira na platformu (Windows, macOS, iOS, Android i sl.), 2. prebacivanje u *oblak* zbog dostupnosti, sigurnosti i pohrane. Dodatno bi važno bilo aplikaciju odvojiti od javno dostupne mreže i omogućiti samo na računalima u ambulantama. Radi dostupnosti kliničkih podataka u ostalim prostorima Fakulteta, dio podataka bi se mogao odvojiti (povezanost s vlasnikom) i tim podacima omogućiti vidljivost na ostatku mreže, ali samo kroz prilagođenu programsku aplikaciju (time bi se ostvarila sigurnost podataka vlasnika, a radi učinkovitosti omogućio pristup putem mobilnih uređaja).
7. Dostupnost slikovnih dijagnostičkih podataka temeljiti, u suradnji s dobavljačem opreme, na nekom sigurnijem protokolu uz striktno poštivanje sigurnosnih standarda. Kao i u prethodnoj točki, bilo bi potrebno navedene funkcionalnosti odvojiti od javno dostupne mreže i omogućiti samo na računalima u ambulantama.
8. Potrebno bi bilo, barem na novonabavljenim računalima isključiti administratorske ovlasti, uz mogućnost ako korisnik želi instalirati dodatne aplikacije, da to učine djelatnici Odsjeka. Osim toga, po inzistiranju korisnika, ostaviti mogućnost dodjele administratorskih ovlasti na računalu uz uvjet da preuzme brigu o održavanju računala prema utvrđenim pravilima (dokumentacija za sustav kvalitete Odsjeka).
9. S obzirom da prijenosna računala koja se povremeno spajaju u mrežu predstavljaju velik rizik, trebalo bi zahtijevati njihovu provjeru s predočenim rezultatima priznatog

antivirusnog testa. Osim toga, kontrola takvog pristupa djelomično bi se riješila i obnavljanjem mrežnih preklopnika.

10. Problem javno dostupnih lozinki bi se riješio njihovom periodičkom izmjenom (jednom tjedno), a dostupnost lozinke bi se mogla osigurati putem mrežne stranice, nakon autentifikacije AAI identitetom.
11. Problem javno dostupne lozinke za bežičnu mrežu *vef* riješio bi se periodičkom izmjenom lozinke (jednom tjedno), a dostupnost lozinke bi se mogla osigurati putem mrežne stranice, nakon autentifikacije AAI identitetom.
12. Računala računovodstva se nalaze u javnoj mreži. Postigli bismo puno veću sigurnost ako bi ta računala bila odvojena u posebnu mrežu, izoliranu od javne. To bi se moglo postići bez utjecaja na brzinu i funkcionalnost mreže, bez intervencije u postojeći radni proces. Veliki dio računovodstvenih podataka se vodi i pohranjuje u vanjskim sustavima, a pristupa im se putem spomenutih sigurnih veza. Osim računovodstva, preporučljivo bi bilo odvajanje mrežnog prometa između postojećih organizacijskih jedinica, što bi značajno smanjilo rizik širenja prijetnji.

Izdvojeno, trebalo bi usvojiti plan izrade sigurnosnih kopija podataka i njihovog povratka, pri čemu bi svaki odjel trebao surađivati s Odsjekom za informatiku u svrhu određivanja podataka koji se obrađuju, načina njihove obrade i čuvanja.

Podaci o studentima nisu posebno navedeni zato jer se vode u sustavu SRCE-a (aplikacija ISVU), uz napomenu da se u referadama Fakulteta podaci o studentima ne bi smjeli pohranjivati na prenosive medije (USB *flash* pohrana i USB diskovi).

Dio predloženih radnji već je opisan u Pravilniku o sigurnosnoj politici i sigurnosti informacijskoga sustava Veterinarskoga fakulteta Sveučilišta u Zagrebu kao i u dokumentaciji sustava kvalitete (radne upute Odsjeka).

Voditelj Odsjeka za informatiku

mr. sc. Alen Hrastnik, dr. med. vet.