PROCEDURA O ZAŠTITI OD ZLONAMERNOG SOFTVERA

Odgovoran za primenu procedure	Lice za bezbednost podataka Novica Krsmanović
Nosilac procedure	Rukovodilac Odseka informacionih sistema i tehnologija Novica Krsmanović
Proceduru odobrio	Direktor UDK Doc.dr Siniša Dučić

S a d r ž a j

1 SVRHA

Svrha procedure je da precizira način zaštite IKT mreže UDK od zlonamernih softvera s ciljem da se unapredi bezbednost svih resursa IKTa.

2 PREDMET I PODRUČJE PRIMENE

Ovom procedurom utvrđuju se aktivnosti, nosioci aktivnosti i odgovornosti zaposlenih koji koriste IKT sistema UDK, a u cilju zaštite od zlonamernog softvera.

Pravilnom primenom utvrđenog postupka i načina arhiviranja, UDK svodi na minimum potencijalnu izloženost šteti i problemima nastalim neadekvatnim ostavljanjem, odnosno odlaganjem osetljivih i poverljivih dokumenata i materijala.

Primenjuje se na sve zaposlene koji koriste IKT sistem UDK.

3 REFERENCE I VEZE SA DRUGIM DOKUMENTIMA

Procedura je u vezi sa dokumentima:

- Akt o bezbednosti IKT sistema Univerzitetske dečje klinike;
- Uputstvo o bezbednosti informaciono - komunikacionog sistema Univerzitetske dečje klinike;
- PR.BZB 01 Procedura za rad Odseka informacionih sistema I tehnologija
- PR.BZB 02 Procedura o instalaciji i konfiguraciji sistema;
- PR.BZB 03 Procedura pristupa mreži i mrežnim uređajima;
- PR.BZB 07 Procedura za VPN pristup;
- PR.BZB 08 Procedura edukacije zaposlenih iz oblasti bezbednosti IKT sistema.

4 DEFINICIJE I SKRAĆENICE

UDK – Univerzitetska dečja klinika;

OJ - Organizaciona jedinica UDK;

Odsek informacionih sistema i tehnologija – sastavni deo Službe investicionog tehničkog održavanja, pomoćnih poslova, bezbednosti i zaštite na radu;

IKT sistem - informaciono-komunikacioni sistem UDK u smislu tehnološko-organizacione celine koja obuhvata:

1. elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije;
2. uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada elektronskih podataka korišćenjem računarskog programa;
3. elektronske podatke koji se čuvaju, obrađuju, pretražuju ili prenose pomoću sredstava iz tač. 1. i 2. a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;
4. organizacionu strukturu putem koje se upravlja IKT sistemom;

BIS Heliant (informacioni sistem) je deo IKT sistema UDK koji je namenjen planskom prikupljanju, skladištenju, obradi i razmeni informacija / podataka o pacijentima i lečenju, kao i informacija koje su značajne za poslovne procese UDK, a na način takav da su informacije dostupne i upotrebljive svima koji su ovlašćeni da ih koriste

Informaciona bezbednost predstavlja skup mera koje omogućavaju da elektronski podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti tajnost, integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi IKT sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica;

Administrator IKT - zaposleni Odseka informacionih sistema i tehnologija kome je dozvoljeno administriranje IKT, IS i BIS;

Lice zaduženo za bezbednost podataka - zaposleni UDK, lice koje se bavi poslovima informacione bezbednosti;

Korisnik - zaposleni UDK koji ima pristup IKT sistemu radi obavljanja svojih poslovnih aktivnosti;

Mobilni uređaj - prenosivi računar, tablet, SMART mobilni telefon, PDA *(Personal Digital Assistant)* i sl. koji se povezuje sa UDK IKT mrežom;

Medijum – disk, USB memorija, prenosivi hard disk, CD, DVD, kao i ostali predmeti i komponente koji imaju mogućnost čuvanja i prenosa podataka;

Radna stanica je personalni računar sačinjen od hardverskih i softverskih komponenti sa monitorom, tastaturom i mišem, namenjena obavljanju poslovnih aktivnosti.

5 ODGOVORNOSTI

Svaki zaposleni je dužan da se ponaša u skladu sa procedurom i u skladu sa svojim zaduženjima će snositi odgovornost.

Saradnici UDK su dužni da se ponašaju u skladu sa ugovorom i u skladu sa njim će snositi odgovornost.

Obaveza rukovodioca svake organizacione jedinice UDK je da sve zaposlene upozna sa procedurom i kao i sve novozaposlene, bilo da su u stalnom ili radnom odnosu na određeno vreme.

Za kontrolu sprovođenja procedure odgovorni su rukovodilac Odseka informacionih sistema i tehnologija i administrator IKT.

6 OPIS PROCEDURE

Zlonamerni softver (engl. *malware*) je namenski osmišljen program koji ima za cilj da naruši bezbednost IKT sistema i podataka koji se nalaze u njemu. Ovi programi mogu napraviti višestruku štetu i to:

1. mogu oštetiti server, računar ili mobilni uređaj;
2. mogu značajno kompromitovati poverljivost, integritet ili dostupnost podataka;
3. mogu zloupotrebiti aplikacije ili operativne sisteme radnih jedinica IKT sistema;
4. mogu na neki indirektan način, sa odloženim vremenskim periodom poremete, uspore, ugroze ili u potpunosti onemoguće rad korisnika tj. zaposlenih.

Ova vrsta softvera, zlonamerni softver se najčešće ubacuje u ceo IKT sistem ili neki njegov deo tajno, skriveno tako da korisnik ne može da prepozna tu vrstu aktivnosti.

Zlonamerni softver podrazumeva sve maliciozne kodove, a to mogu biti: virusi, trojanci, „crvi“ ili engl. *spyware, adware, nagware, backdoors, exploits, rootkits, keyloggers* itd.

U cilju zaštite IKT sistema od zlonamernog softvera, UDK u kontinuitetu primenjuje i unapređuje mere za prevenciju i rano otkrivanje zlonamernih kodova i tu spadaju:

1. praćenje i kontrola podataka;
2. softvera i hardvera;
3. sprečavanje i otkrivanje napada zlonamernim softverom;
4. kao i oporavak IKT sistema nakon napada zlonamernog softvera.

Zaštita svih IKT resursa, prevashodno podataka i sredstava za obradu podataka od zlonamernog softvera u UDK se zasniva na:

1. edukaciji zaposlenih;
2. zaštiti na nivou hardvera;
3. zaštiti na nivou softvera;

4. kontroli pristupa i
5. upravljanju zahtevanim i potrebnim promenama.

6.1 Edukacija zaposlenih

Proces rada sistem administratora IKT sistema se sastoji iz operativnih aktivnosti koje obezbeđuju kvalitetan nadzor, otkrivanje rizika, procenu rizika i preduzimanje mera za zaštitu IKT sistema. Takođe, administrator IKT periodično i prema potrebi informiše ovlašćeno Lice za bezbednost podataka o bezbednosti IKT sistema. Kroz timski rad učestvuje u procesu širenja svesti zaštite podataka svih zaposlenih u UDK.

Lice za bezbednost podataka UDK periodično organizuje edukaciju svih zaposlenih, dok svim novozaposlenima odmah po zasnivanju radnog odnosa organizuje obaveznu edukaciju o bezbednosti podataka.

6.2 Zaštita na nivou hardvera

Obaveza sistem administratora IKT u saradnji sa informatičarima Odseka informacionih sistema i tehnologija je zaštita na nivou hardvera, koju sprovodi na sledeće načine:

- koristi sve bezbednosne mere koje postojeći hardver omogućava;
- redovno ažurira upravljački softver i obezbeđuje potrebne licence za rad hardvera;
- osigurava pravilno priključivanje uređaja na IKT sistem UDK u skladu sa PR.BZB 14 Procedurom uključivanja i isključivanja servera;
- instalacijom i konfiguracijom sistema isključivo od strane Administratora IKT u skladu sa PR.BZB 02 Procedura o instalaciji i konfiguraciji sistema;
- da obezbedi u potpunosti primenu procedure PR.BZB 03 Procedura pristupa mreži i mrežnim uređajima, odnosno da onemogući priključivanje uređaja od strane bilo kog drugog lica;
- da VPN konekciju koriste isključivo uređaji koji su u vlasništvu UDK u skladu sa PR.BZB 07 Procedurom za VPN pristup. Preko VPN se omogućava i pristup IKT resursima UDK saradnicima (lica koja nisu stalno zaposlena u UDK). Potrebno je da vodi evidenciju njihovih elemenata IKTa putem kojih pristupaju, kao i lokaciju pristupa.

6.3 Zaštita na nivou softvera

U IKTu UDK se koristi nekoliko softverskih rešenja za bezbednost podataka po specifičnim oblastima i prema procenjenoj vrsti napada:

- antivirus-zaštita servera i radnih stanica, laptopa *(Sophos*),
- zaštita od napada sa Interneta *(Sophos firewall*),
- zaštita elektronske pošte *(open source*),
- zaštita bežične konekcije *(provajder).*

Odgovorno lice Odseka, a naročito Administrator IKTa kontinuirano prati sve pretnje i primenjuje adekvatnu zaštitu. Adminsitrator vodi evidenicju, analizira i izveštava rukovodioca Odseka o bezbednosnim propustima IKT sistema UDK sa tehničko-tehnološkog aspekta. Maksimalna zaštita se postiže redovnim ažuriranjem softvera i pravovremenim obezbeđivanjem potrebnih licenci. U tom smislu, UDK planski nabavlja licencirane softvere i operativne sisteme u skladu sa finansijskim sredstvima. Trenutno od 350 radnih stanica, 100 radnih stanica ima licenciran OP sistem i to *Windows Microsoft operating systems. Office paket (Microsoft Office)* sa licencom ima samo nekoliko radnih stanica.

6.4 Kontrola pristupa

Da bi održali bezbednost sistema, potrebno je sprovoditi proveru sadržaja dokumenata, elektronske pošte, mobilnih uređaja, eksternih memorija i medija (CD, DVD). Ova provera se odnosi na prepoznavanje sumnjivih aktivnosti. Ukoliko se uoči neka nepravilnost, posumnja na

potencijalnu bezbednosnu pretnju, potebno je postupati po procedurama ili izjavama odgovornosti (PR.BZB 03 Procedura pristupa mreži i mrežnim uređajima, PR.BZB 05 Procedura o pravima pristupa IKT sistemu, PR.BZB 07 Procedura za VPN pristup; PR.BZB 10 Procedura za bezbedno upravljanje prenosnim nosačima podataka, PR.BZB 17 Procedura o bezbednosti razmene ePoruka, PR.BZB 18 Procedura o korišćenju mobilnih uređaja).

6.5 Upravljanje zahtevanim i potrebnim promenama

Administrator IKT je u obavezi da u slučaju bilo kakve bezbednosne pretnje u IKT sistemu UDK primeni sve raspoložive tehničko-tehnološke mere. To se odnosi na aktivni kontinuirani monitoring, postupanja prema softveru i hardveru u skladu sa definisanim preformansama kao i preduzimanje svih mera za pravilno korišćenje i rad svih resursa IKT sistema.

U slučaju otkrivanja ili sumnje na napad od strane zlonamernog softvera, Administrator IKT sprovodi sve mere zaštite koje su mu na raspolaganju za specifične oblasti sistema IKT (server, radna stanica, laptop, eMail a u skladu sa procedurama).

U slučaju otkrivanja ili sumnje na postojanje zlonamernog softvera, a u zavisnosti od mesta otkrivanja, potrebno je:

- Ako je zlonamerni softver otkriven na radnoj stanici ili nekom od medijuma, potrebno je isključiti ga sa mreže, „očistiti“ od zlonamernog softvera. Zaposlenom / korisniku koji u svom radu koristi datu radnu stanicu treba ukazati koje zaštitne mere treba da preduzme. Događaj treba evidentirati i prikazati kroz redovni periodični izveštaj o bezbednosti IKT. Radnu stanicu treba vratiti Korisniku i priključiti na mrežu tek posle provere i testiranja bezbednosti. Ako je predmet napada bio neki od mobilnih uređaja, vrši se provera i eventalno čišćenje svih uređaja sa kojim je on bio u kontaktu. Obaveštava se Lice zaduženo sa bezbednost podataka;
- Ako je zlonamerni softver pokrenut putem mejla: tada se radna stanica „očisti“, *mail* sa kog je upućen zlonamerni softver se stavlja na *black* listu; zaposlenom / korisniku se ukazuje na to koje zaštitne mere treba da preduzme; događaj se evidentira. Obaveštava se Lice zaduženo sa bezbednost podataka;
- Ako je zlonamerni softver aktiviran preko poznatih ili sumnjivih kompromitovanih *web* sajtova: potrebno je očistiti radnu stanicu; Korisnicima / Zaposlenima onemogućiti pristup tim veb sajtovima (dodati ga u listu *block* adresa) a događaj evidentirati. U slučaju dokazane zloupotrebe interneta od strane korisnika, Odsek informacionih sistema i tehnologija može korisniku ukinuti pristup internetu. Obaveštava se Lice zaduženo sa bezbednost podataka i postupa u skladu sa Pravilnikom o ponašanju zaposlenih UDK.

Odsek informacionih sistema i tehnologija planira da u nastupajućem periodu izradi planove;

1. Plan kontinuiteta poslovanja u vanrednim uslovima i
2. Plan oporavka od napada zlonamernim softverom, uključujući sve neophodne rezervne kopije podataka i softvera kao i mehanizme za oporavak.

Odsek za informacione sisteme i tehnologije planira da samostalno ili uz pomoć odgovarajućih vendora sprovodi oporavak od napada zlonamernim softverom.

Korisnik IKT sistema ne sme svesno (namerno) da uradi nijednu radnju koja bi dovela do ranjivosti i napada na sistem. Korisnik svoje aktivnosti na IKT sistemu treba da sprovodi u skladu sa PR.BZB 05 Procedurom o pravima pristupa IKT sistemu. U suprotnom, pokreću se mere i postupci definisani Pravilnikom o ponašanju zaposlenih UDK.

Rukovodilac Odseka informacionih sistema i tehnologija je u obavezi da redovno tj. jednom u 6 meseci informiše o stanju bezbednosti IKTa ovlašćeno Lice za bezbednost podataka UDK. U slučaju evidentiranja zlonamernog softvera neophodno je da odmah obavesti Lice za bezbednost podataka UDK.

Lice zaduženo za bezbednost podataka evidentira informacije o zlonamernom softveru i u skladu sa svojim ovlašćenjima preduzima eventualne mere.

7 PRAVNI OSNOV

- Zakon o informacionoj bezbednosti („Sl.glasnik RS", br. 6/2016, 94/2017);
- Zakon o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva („Sl.glasnik RS", broj 123/2014, 106/2015, 105/2017, 25/2019);
- Zakon o zaštiti podataka o ličnosti („Sl.glasnik RS", br. 87/2018).