STRATEGIJA UPRAVLJANJA INFORMACIJAMA

U

J.U. OPĆA BOLNICA „PRIM DR ABDULAH NAKAŠ“

Septembar, 2018. godine

Sadržaj

1. Uvod

Sigurnosna politika informacionih tehnologija je usko vezana sa Strategiju upravljanja informacionim tehnologijama u Općoj bolnici „Prim dr Abdulah Nakaš". Ova politika se odnosi na standardne i sigurnosne procedure koje se odnose na zaštitu ličnih podataka pacijenata, korisnika usluga te podataka koji se odnose na podatke potrebne za upravljanje bolnicom.

Sigurnosna politika je dokument koji definira skup pravila, smjernica i prijedloga o ponašanju prilikom rukovanja informacijskim sistemom u bolnici i mjerama koje je potrebno poduzeti u konkretnim situacijama. To su mjere koje moraju biti sadržane u organizacijskom i tehničkom dijelu upravljanja informacijskim sistemom bolnice odnosno Bolničkim informacionim sistemom na nivou Kantona Sarajevu koji se koristi za rad sa pacijentima ove Ustanove.

Bolnica treba da ispoštuje akreditaciiske standarde sukladno sa preporukama AKAZ-a pod brojem 6.14.

6.14. Postoji dokumentirana sigurnosna politika informacijskog sistema bolnice.

Sama sigurnosna politika je vezana za politiku razvoja informacionog društva BIH iz 2004. godine, te strategiju primjene informaciono komunikacione tehnologije u zdravstvu Kantona Sarajevo te Strategiju upravljanja informacionim tehnologijama u Općoj bolnici „Prim dr Abdulah Nakaš".

Radi boljeg razumijevanja svrhe ovog dokumenta i toga šta je njegova zadaća potrebno je dati osnovna pojašnjena samog naziva koji je definiran u projektnom zadatku, a to je "Sigurnosna politika informacionih tehnologija u općoj bolnici „Prim dr Abdulah Nakaš".

Informacijski sistemi i podaci koje oni sadrže često su vrlo bitni za poslovanje institucija koje ih koriste. Povećanjem uporabe elektroničkih informacija u poslovanju povećava se i zabrinutost oko sigurnosti sistema i podataka koji su u njemu pohranjeni. Da bi se podaci i informacijski sistemi kvalitetno zaštitili važno je osmisliti i provesti politiku sigurnosti.

Adekvatna razmjena informacija na nivou Opće bolnice „Prim. dr. Abdulah Nakaš" je preduslov za pružanje kvalitetne i efikasne zdravstvene zaštite. Informacione tehnologije predstavljaju danas jedan od prioriteta u oblasti zdravstvenog menadžmenta. Istovremeno, kvalitet zdravstvene zaštite je prepoznat kao jedna od najvažnijih karakteristika sistema zdravstvene zaštite. Stalno unapređenje kvaliteta rada i sigurnosti pacijenata je sastavni dio svakodnevnih aktivnosti zdravstvenih radnika i zdravstvenih saradnika. Informacione tehnologije igraju značajnu ulogu u strategiji razvoja Opće bolnice „Prim. dr. Abdulah Nakaš". Razmjena informacija igra ključnu ulogu u procesu rada kako medicinskih tako i nemedicinskih službi. Svaki dan se unutar Bolnice generira velika količina

informacija. Informacije se trenutno pohranjuju na serverima Bolnice te najvećim dijelom na serverima BIS-a na koje se pohranjuju informacije o pacijentima koji dolaze na liječenje u našu ustanovu.

2. Što je sigurnosna politika

Svaki informacijski sistem sadrži podatke kojima se služe njegovi korisnici i koji služe kako bi korisnicima bilo omogućeno korištenje sistemom. Budući da takvi podaci često ne smiju biti javno dostupni, tj. moraju biti tajni, ne smiju biti mijenjani bez odobrenja i ne smiju biti nedostupni korisnicima, važno je provesti određene korake sigurnosti kako bi navedeni uvjeti uvijek bili zadovoljeni.

Sigurnosna politika je skup pravila, smjernica i postupaka koji definiraju na koji način informacijski sistem učiniti sigurnim i kako zaštititi njegove tehnološke i informacijske vrijednosti. Ona govori korisnicima što smiju raditi, što ne smiju raditi, što moraju raditi i koja je njihova odgovornost. Politikom ne određujemo na koji način zaštiti informacijski sistem već samo što zaštititi. Svakodnevnim razvojem tehnologija otkrivaju se i nove metode kojima je moguće ugroziti sistem. Stoga definiranje općenite sigurnosne politike za informacijske sisteme nije moguće i jednom napisana politika mora se redovito pregledavati, mijenjati i nadopunjavati kada se za tim ukaže potreba.

Sigurnosnom politikom definirana su pravila koja se odnose na:

- Svu računalnu opremu institucije (hardware i software)
- Osobe odgovorne za administraciju informacijskog sistema
- Sve zaposlenike i korisnike sistema, odnosno osobe koje imaju pravo pristupa
- Vanjske saradnike (npr. ovlaštene djelatnike zadužene za održavanje sistema)

Sigurnosnom politikom obuhvaćaju se široka područja sigurnosnih mjera, ali nisu svi dijelovi politike potrebni pojedinim skupinama korisnika. Na primjer, zaposlenici koji koriste sistem ne trebaju znati dio politike koji se odnosi na sigurnost tehničke opreme. Stoga se sigurnosna politika može, a i preporučljivo je, podijeliti u više dijelova.

Sigurnosna politika Opće bolnici „Prim dr Abdulah Nakaš". se odnosi na sve njezine zaposlenike, pacijente i osobe koje su prisutne po drugim dužnostima, obvezama i razlozima u prostorima bolnice. Sigurnosna politika se odnosi na sudionike odgojno obrazovnog procesa i one koji nisu dio tog sistema, a nalaze se u prostorima bolnice.

Ovo se odnosi i na osobe koje rade u drugim zdravstvenim ustanovama Kantona Sarajevo koje imaju pristup informacijama koje se generiraju u toku radnog procesa Bolnice. Naime, ljekari u Domovima zdravlja KS i UKC Sarajevo mogu pristupiti nalazima i dokumentima koji su generirani u našoj Ustanovi. Također,

medicinsko osoblje naše ustanove ima pristup podacima i dokumentima koji su generirani u drugim zdravstvenim ustanovama u Kantonu Sarajevo i trebaju da se ponašaju odgovorno prema navedenim dokumentima.

Korisnici, kojima je sigurnosna politika namijenjena, često nemaju strpljenja čitati mnoštva stranica teksta. Isti korisnici imaju vrlo mala znanja o tehnologijama koje se koriste pri radu. Zbog toga je nužno definirati sigurnosnu politiku tako da bude kratka i jasna, napisana na način da ju korisnici mogu razumjeti. Politiku napisanu opširno i stručnim jezikom obični korisnik ne razumije i površno ju ili nikako analizira, pa je stoga ne može niti primijeniti.

Nakon definiranja sigurnosne politike bitno je osigurati da se pravila koja su definirana sigurnosnom politikom provode i poštuju. Kako bi to bilo postignuto bitno je svakom korisniku sistema dati na znanje da je sigurnosna politika uvedena i upoznati ga s njegovim dužnostima. Postoji više načina kako korisnike upoznati sa sigurnosnom politikom, npr. dijeljenjem dokumenta politike ili objavljivanjem sigurnosne politike na web stranicama bolnice.

Sigurnosna politika kao dokument je jedan od važnijih dijelova sistema koji definira elemente upravljanje i rada sistemom. Politikom upravljamo sigurnošću informacijskih sistema.

Sigurnosna politika je važna za uobičajeno, redovito i kvalitetno funkcioniranje sistema.

Svrha politike sigurnosti je:

1. definirati prihvatljive načina ponašanja
2. definirati neprihvatljive načine ponašanja
3. jasno raspodijeliti zadatke
4. jasno raspodijeliti odgovornosti
5. propisati smjernice i pravila ponašanja tijekom korištenja informacijskog sistema
6. propisati sankcije u slučaju nepridržavanja smjernica sigurnosne politike.

Glavni zadatak sigurnosne politike je osigurati tri jedinstvena svojstva informacija:

- povjerljivost (tajnost),
- integritet,
- dostupnost.

3. Povjerljivost

Povjerljivost je zaštita podatka koje sadrži sistem od neovlaštenog pristupa. Iako je opće mišljenje da je ovaj tip zaštite od najveće važnosti za državne institucije i vojsku jer svoje planove i mogućnosti moraju čuvati tajno od mogućih neprijatelja, ono također može biti značajno za kompanije koje imaju potrebu zaštititi poslovne planove i informacijske vrijednosti od konkurencije ili da bi zaštitili podatke od neovlaštenog pristupa. Ključni aspekt povjerljivosti je identifikacija korisnika i provjera autentičnosti.

Identifikacija je proces prijave korisnika na sistem, pri čemu sistem zna da takav korisnik postoji. Na primjer, korisnik A želi se prijaviti na sistem. Sistem provjeri da li je korisnik A prijavljen na sistem, i ako je, tada slijedi proces provjere autentičnosti. Provjera autentičnosti je proces kojim sistem želi biti siguran da je korisnik koji se prijavljuje pod imenom A upravo osoba A. Postoji više načina provjere autentičnosti. Najrašireniji je unos lozinke, ali se i sve više razvija tehnička oprema koja jedinstvene ljudske osobine, poput otiska prsta ili mrežnice oka pretvara u digitalne signale koji služe za autentifikaciju. Na primjer, kako bi sistem provjerio da li je korisnik koji se pokušava prijaviti kao osoba A upravo ta osoba, može pri prijavi tražiti od korisnika A određenu lozinku koju zna samo osoba A. Ako korisnik A pošalje upravo tu lozinku, sistem zna da je korisnik upravo osoba A. U suprotnom, korisnik nije osoba A te mu sistem ne dozvoljava korištenje sistema.

U Općoj Bolnici se vrši autorizacija korisnika prilikom pristupa računaru. Tom prilikom korisnik unosi korisničko ime Odsjeka ili vlastito korisničko ime. Za pristup Bolničkom informacionom sistemu svi ovlašteni korisnici imaju svoje korisničko ime i lozinku te su potpisali dokument kojim garantuju da neće odavati drugim korisnicima svoje podatke za pristup BIS-u.

Povjerljivost može biti narušena na nekoliko načina. Navedene su najčešće prijetnje povjerljivosti:

- Hakeri
- Lažno predstavljanje
- Neovlaštena aktivnost
- Nezaštićeno preuzimanje podataka
- Lokalna mreža (eng. LAN – Local Area Network)
- Trojanski konji

Hakeri. Hakeri su osobe koje koriste sigurnosne slabosti sistema na način da se neovlašteno koriste sistemom. Mnogi hakeri, osim sigurnosnih slabosti sistema, koriste i metode otkrivanja lozinki ovlaštenih korisnika. Naime, lozinke koje su riječi koje se nalaze u rječniku ili često korištene lozinke, iskusnijim hakerima pomoću programske podrške vrlo lako je otkriti. Otkrivanjem lozinke korisnika haker se prijavljuje na sistem kao ovlašteni korisnik i vrlo jednostavno obavlja kopiranje,

brisanje ili mijenjanje podataka, ili ih kopiraju na lokacije s kojih su dostupni određenom krugu ljudi ili čak svim korisnicima Interneta. Iz tih razloga aktivnost hakera predstavlja veliku opasnost povjerljivosti informacija.

Lažno predstavljanje. Lažno predstavljanje je prijetnja u kojoj korisnik koji ima ovlasti pristupa sistemu preko lozinke dobivene ili nabavljene na bilo koji drugi način od drugog korisnika čime dobiva mogućnost pristupa podacima dodijeljene drugom korisniku. Lažno predstavljanje je čest slučaj u kompanijama koje dozvoljavaju korisnicima da razmjenjuju lozinke.

Neovlaštena aktivnost. Ovaj tip aktivnosti događa se kad ovlašteni korisnik sistema koristi podatke za koje nema ovlasti. Nedovoljna kontrola pristupa i zaštita podataka omogućuju neovlašten pristup, što može ugroziti njihovu povjerljivost.

Kopiranje podataka na nezaštićene lokacije. Kopiranje podataka može ugroziti njihovu povjerljivost ukoliko se podaci kopiraju na sistem s nedovoljnom sigurnosnom zaštitom. Primjer ove vrste prijetnje je kopiranje podataka sistema na lokacije sistema koje nemaju adekvatnu razinu zaštite. Ukoliko do kopiranih podataka pristup imaju ostali ovlašteni korisnici sistema njihova je tajnost ugrožena.

Lokalna mreža. Lokalna mreža predstavlja prijetnju jer podaci koji putuju mrežom mogu biti dohvaćeni u svakom čvoru mreže. Kako bi se izbjegla ova vrsta prijetnje svi tajni podaci koji bi smjeli biti dostupni samo u određenim čvorovima moraju biti kriptirani kako bi njihova povjerljivost ostala neupitna.

Trojanski konji. Trojanski konji su vrsta aplikacije koje mogu izazvati vrlo velike štete sistemima. Primjer trojanskog konja je aplikacija instalirana na računalo sistema nakon što ga nesvjesno pokrene ovlašteni korisnik, te je tako programirana da kopira podatke na nezaštićene dijelove sistema. Jednom pokrenut, trojanski konj ostaje aktivan na sistemu i konstantno obavlja programirane zadatke.

4. Integritet

Integritet predstavlja zaštitu podataka od namjernog ili slučajnog neovlaštenog mijenjanja. Dodatni element integriteta jest zaštita procesa ili programa kako bi se onemogućilo neovlašteno mijenjanje podataka. Glavni zahtjev komercijalnih i državnih institucija jest osigurati integritet podataka kako bi se izbjegle zlouporabe i greške. To je imperativ kako korisnici ne bi mogli mijenjati podatke na način da ih izbrišu, promjene ili učine ključne podatke nesigurnima. Svi zaposlenici, mogu koristiti informacijski sistem Bolnice pod uvjetima i pravilima koji su propisani za određeni dio informacijskog sistema ili tehničke opreme ovisno o nivou pristupa informacijama koja je određena od strane menadžera BIS-a te pristupati serverima Bolnice ovisno o nivou autorizacije koju određuje direktor Bolnice uz saradnju sa Odsjekom za informaciono – komunikacijske tehnologije.

Pravila vrijede za sve jednako i moraju se provoditi na način kako je propisano unutarnjim pravilima Bolnice, zakonima i sigurnosnom politikom.

Ključni elementi za postizanje integriteta podataka su identifikacija i provjera autentičnosti korisnika. Budući integritet ovisi o kontroli pristupa, važno je pozitivno i jedinstveno utvrditi identičnost svih korisnika prijavljenih na sistem.

Čuvanje osobnih korisnički podataka:

- Korisnički podaci su tajni.
- Svako je vlasnik svojih korisničkih podataka i dužan ih je čuvati.

Zabranjeno je ustupanje osobnih korisničkih podataka bilo kojoj drugoj osobi bez obzira na razlog.

Nakon korištenja određenog dijela informacijskog sistema, opremu je potrebno vratiti u stanje u kojem je zatečena prije korištenja. Nakon radnog vremena računalnu opremu je potrebno isključiti na pravilan način.

Svi zaposlenici koji koriste računalnu/mrežnu opremu dužni su se educirati, ukoliko ne znaju rukovati spomenutom opremom, kako bi njome mogli na ispravan način rukovati.

Na računalima nije dozvoljeno korištenje memorija koje nisu očišćene od virusa i drugih malicioznih programa.

Na računalima se ne smiju pohranjivati osobne datoteke koje nisu potrebne za radni proces u Bolnici. Sve datoteke koje više nisu potrebni se moraju ukloniti. Svaka osoba koja koristi resurse, dužna je nepotrebne datoteke ukloniti.

Gubitak podataka se mora prijaviti administratoru Odsjeka za informaciono komunikacijske tehnologije Bolnice koji će izdati nove podatke.

4.1. Zaštita integriteta

Kao i povjerljivost, integritet može biti ugrožen od hakera, lažnog predstavljanja, neovlaštenih aktivnosti i nedozvoljenih programa (virusi, trojanski konji) jer sve navedene aktivnosti mogu dovesti do neovlaštenog mijenjanja podataka.

Osnovni principi za kontrolu integriteta:

- dodjeljivanje pristupa na temelju potreba
- razdvajanje obaveza
- rotiranje obaveza.

Dodjeljivanje pristupa na temelju potreba. Korisnici bi trebali dobiti pristup samo onim podacima koji su im potrebni kako bi mogli obavljati zadane poslove.

Korisnikov pristup ključnim podacima trebao bi biti dodatno ograničen kvalitetno definiranim transakcijama koje osiguravaju da korisnik podatke može mijenjati u strogo kontroliranim uvjetima kako bi se sačuvao integritet podataka. Bitan element kvalitetno definiranih transakcija je bilježenje podataka o mijenjanju podataka (ko, kada i koje podatke) kako bi se moglo utvrditi da li su podaci ispravno mijenjani od ovlaštene osobe. Kako bi bila djelotvorna, transakcije bi trebale dopuštati izmjenu podataka samo od unaprijed odabranih programa. Odabrani programi moraju biti ispitani kako bi se izbjegla neovlaštena aktivnost.

Kako bi korisnici mogli uspješno koristiti sistem, privilegija pristupa mora biti razumno raspodijeljena kako bi se omogućila potrebna operativna fleksibilnost. Dodjeljivanje pristupa na temelju potreba ima zadaću osigurati maksimalnu kontrolu uz minimalno ograničavanje korisnika.

5. Dostupnost

Dostupnost je garancija ovlaštenim korisnicima sistema da će im sistem biti raspoloživ u svakom trenutku kad za njim imaju potrebu. Dva su najčešća uzroka neraspoloživosti sistema.

Sigurnosne mjere kojima osiguravamo dostupnost dijelimo na:

- Fizičke
- Tehničke
- Administrativne

Fizičke mjere uključuju kontrolu pristupa koja sprječava neovlaštenim osobama pristup sklopovlju informacijskog sistema, protupožarnim sistemima, sistemima za kontrolu temperature prostorija itd.

Tehničke mjere sprječavaju nefunkcioniranje sistema koje uzrokuje kvar opreme raznim mjerama poput zrcaljenja diskova, tj. više diskova sadrži iste informacije – ako se jedan pokvari, njegovu funkciju preuzima drugi. Jedna od mjera je konstantna provjera rada aplikacija – ako aplikacija ne izvršava zadatke ona se automatski ponovno pokreće. Tehničke mjere također sadrže mehanizme oporavka nakon nestanka struje (automatski se pokreće sekundarno napajanje), automatsko kreiranje kopija podataka itd.

Administrativne mjere uključuju kontrolu pristupa, kontrolu izvršavanja procedura i educiranje korisnika. Odgovarajuća osposobljenost programera i sigurnosnih stručnjaka također je bitan faktor dostupnosti sistema. Na primjer, ostane li prilikom kontrole sistema baza podataka zaključana, korisnici se ne mogu koristiti podacima koje ona sadrži, tj. sistem postaje nedostupan.

6. Norme i reference

Danas je sigurnost informacijskih sistema jedna od najaktualnijih tema u informatičkim krugovima. Budući da je sigurnost najslabija karika informacijskih sistema u njen razvoj se uključuje sve više stručnjaka, koji svakim danom definiraju nove norme kojima predlažu način zaštite informacijskih sistema.

ISO/IEC 17799:2005 je internacionalna norma za sigurnost informacijskih sistema. Razvijena je od strane internacionalne organizacije za norme (eng. ISO – the International Organization for Standardization) i internacionalnog elektrotehničkog odbora (eng. IEC - the International Electrotechnical Commission

7. Sigurnost informacijskih sistema

Kao što je navedeno u prethodnim poglavljima, sigurnost informacijskih sistema može biti ugrožena na više načina. Možemo ih podijeliti na one koje mogu ugroziti sistem izvana i one koje sistem ugrožavaju iznutra.

Da bi spriječili mogućnost obavljanja ovakvih neželjenih radnji, potrebno je uvesti odgovarajuće mjere. Mjerama poput educiranja zaposlenika smanjuje se vjerojatnost njihove pogreške kojima bi mogli ugroziti integritet i sigurnost sistema. Smještajem opreme na kojima se čuvaju podaci u posebnu prostoriju, propisima kojima se određuje tko joj smije pristupiti, kontroliranjem uvjeta u takvoj prostoriji kao što su temperatura i vlaga, postižemo duži radni vijek opreme a time i pouzdaniji rad sistema. Uvođenjem kontrole pristupa podacima i definiranjem sankcija onima koji se ne pridržavaju propisanih pravila suzbijamo zlouporabu sistema od strane zaposlenika.

Najrjeđi, ali napadi koji najčešće uzrokuju najveće štete su napadi "izvana". Oni sudjeluju u vrlo malom postotku, a cilj im je pribavljanje informacija, njihovo mijenjanje ili uništavanje. Sistem se od takvih napada brani kontrolom prometa s Interneta prema sistemu i obrnuto, sprečavanjem instaliranja programa u operacijski sistem ili kriptiranjem podataka. Uvođenjem ovakvih mjera u informacijskim sistemima podižemo njegov stupanj sigurnosti, a mogućnost obavljanja neželjenih radnji svodimo na minimum.

Kako bi se postigla maksimalna sigurnost sistema, potrebno je obratiti pažnju na:

- Fizičku sigurnost
- Sigurnosne mjere za osoblje
- Sigurnost komunikacija
- Operacijsku sigurnost

Fizička sigurnost. Osnova fizičke sigurnosti je zaštita fizičkog dijela informatičke infrastrukture, zgrade u kojoj je ona smještena, medija za pohranu podataka i komunikacijske opreme. Mjere fizičke sigurnosti obuhvaćaju sve obrambene mjere poduzete u svrhu zaštite računarske infrastrukture od prirodnih nepogoda, problema u okolini, nezgoda i namjernih oštećenja.

Fizičku sigurnost sistema mogu ugroziti prirodne nepogode poput požara, poplava, udara groma ili potresa, prijetnje iz okoline poput zagrijavanja, hlađenja ili električne energije, zatim korisnici sistema ili osobe koje sistemu nemaju pravo pristupa.

Sigurnosne mjere za osoblje. Najveće prijetnje informacijskim sistemima su ljudi koji s njim imaju vezu, kroz svakodnevni rad ili kroz povremeno održavanje. Neke osobe nisu dovoljno kvalificirane za određeni posao te se može dogoditi da takva osoba slučajno uništi podatke te ugrozi informacijski sistem. Ugrožavanje sistema je također moguće namjernim radnjama korisnika sistema, bilo radi zadovoljstva, osobne koristi ili nekog drugog razloga.

Sigurnost komunikacija. Komunikacija između računala doprinosi povećanju snage sistema, brzini obrade podataka, dostupnosti, ali što više računala komunicira sa drugim računalima to je organizacija u kojoj se ona nalaze ranjivija.

Komunikaciju mrežom možemo učiniti sigurnijom kontrolom pristupa, kriptiranjem podataka koji putuju mrežom, zaštitom vatrenim zidovima (eng. firewall) i ostalim mjerama fizičke zaštite. Kontrola pristupa je bitan faktor u ostvarivanju računarske sigurnosti u mrežnom okružju. Mnogi računalni sistemi koriste lozinke u smislu osiguravanja kontrole pristupa, svako tko zna ispravnu lozinku ima dozvoljen pristup računalnom sistemu. Stoga je bitno da lozinku poznaju samo ovlašteni korisnici. Kako bi kontrola pristupa imala svoj smisao, korisnici se moraju pridržavati osnovnih pravila pri čuvanju lozinke dok su ih administratori dužni tehnički ugraditi u sve sisteme koji to omogućavaju.

Pravila za korištenje lozinki

1. Minimalna dužina lozinke

Kratku lozinku lakše je probiti. Stoga neka minimalna dužina lozinke bude šest znakova, ali preporučujemo korištenje još dužih lozinki.

2. Riječi iz rječnika

Ne koristiti ih, jer hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih lozinki (tzv. dictionary attack).

3. Izmiješati mala i velika slova s brojevima

Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je lozinka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova. Koristiti i specijalne znakove ako su dopušteni u sistemu (npr. $).

4. Imena bliskih osoba, ljubimaca, datumi

Ne treba koristiti takve lozinke jer se lako otkriju socijalnim inženjeringom.

5. Tajnost lozinke

Korisnici su odgovorni za svoju lozinku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sistema. Hakeri nastoje izmamiti lozinke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja probleme i bez poznavanja korisničkih lozinki.

7. Čuvanje lozinke

Lozinke se ne ostavljaju na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama itd. Korisnik je odgovoran za tajnost svoje lozinke, te mora naći način da je sakrije. Ukoliko korisnik zaboravi lozinku, administrator će mu omogućiti da unese novu. Nikada lozinku čuvati u blizini računala ili terminala

8. Administriranje lozinki

Ukoliko sistem dopušta na računalima koja spadaju u zonu visokog rizika administratori su dužni konfigurirati sistem na taj način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave. Prilikom provjere sistema, sigurnosni tim može ispitati jesu li korisničke lozinke u skladu s navedenim pravilima.

Osim ovih pravila, moguće je definirati dodatna pravila koje kontrolira sistem.

Operacijska sigurnost. Operacijska sigurnost uključuje dva aspekta sigurnosti informacijskih sistema. Prvi se odnosi na povećanje svijesti među potencijalnim žrtvama, a drugi predstavlja načine na koji se računalni kriminalci mogu spriječiti u počinjenju djela.

Povećanje svijesti postiže se tako da kad god je to moguće zaposlenici budu uključeni u sigurnosni program te ih po potrebi educirati na koji način je sigurnost ugrožena i kako svi dijele rizik i odgovornost. Jednom kada se analiziraju rizici sistema, potrebno je odrediti količinu informacija koja će se podijeliti sa zaposlenicima. Jasno je da povjerljive informacije neće biti dostupne svima, već samo malom broju osoba kojima su one nužne za obavljanje poslova. Općenito gledajući, operacijska sigurnost ne može postojati i biti dostatna sama sebi. Jedini način na koji ona može postojati jest uključivanje operacijske sigurnosti u programe ostalih načina zaštite sistema.

8. Korisnici usluga

Korisnici usluga su osobe koje se koriste sistemom u svome radu (proizvode dokumente, unose podatke, koriste se informacijama) ali ne odgovaraju za instalaciju računalnih programa, njihov ispravan rad niti za ispravan i neprekidan rad računala

odnosno mreže. Unatoč tomu, svaki korisnik ima određene dužnosti prema davatelju usluga.

Svaki korisnik dužan je pridržavati se pravila prihvatljivog ponašanja, što znači da se ne smije koristiti računalom za djelatnosti koje nisu u skladu sa zakonom i pravilima sigurnosne politike, birati kvalitetnu lozinku i povremeno je mijenjati, prijavljivati sigurnosne incidente.

Korisnici koji proizvode podatke dužni su brinuti o njihovoj sigurnosti (dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, stoga treba osigurati njihovo čuvanje i ograničiti pristup samo ovlaštenim osobama.

9. Administrator računala

Da bi se osigurao nesmetan rad sistema, potrebno je administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti. Svako računalo mora imati imenovanog administratora, koji je odgovoran za instalaciju i konfiguraciju programske podrške. Ako korisnici žele sami administrirati računala, moraju imati dopuštenje odgovornih osoba nakon čega i za njih vrijede sva pravila za administriranje računala. Davanje ovakvih dopuštenja može se dati samo u uz saglasnost direktora Bolnice na prijedlog odgovorne osobe Odsjeka za IKT nakon što ova služba razmotri pismeni zahtjev korisnika.

Računala je potrebno konfigurirati na taj način da budu zaštićena od svih napada izvana i iznutra, što se osigurava pravovremenim instaliranjem zakrpi po preporukama proizvođača programske podrške, listama pristupa, filtriranjem prometa i drugim sredstvima.

Administratori računala dužni su svakodnevno pratiti rad sistema i čitati dnevničke zapise. Zadaća administratora je i nadgledanje rada korisnika, kako bi se otkrile neovlaštene aktivnosti. Bilo kakve incidente administratori su dužni prijaviti odgovornoj osobi Odsjeka za IKT.

10. Upravitelj mreže

Ustanove čiji se sistemi sastoje od velikog broja računala i razgranatih mreža mogu imati velike probleme pri uspostavi sigurnosti ako se ne zna točan broj mrežnih priključaka i umreženih uređaja, uključujući prenosiva i ručna računala. Kako bi se osiguralo da su u svakom trenutku takvi podaci dostupni, potrebno je odrediti osobu koja će biti odgovorna za upravljanje mrežom, konfiguriranje uređaja, dodjeljivanje adresa itd. Ovi poslovi su isključivo u nadležnosti odgovornih osoba Odsjeka za IKT.

Osobe koje vrše preinake na mreži to moraju raditi isključivo u dogovoru sa odgovornim osobama Odsjeka za IKT bez obzira da li se radi o uposlenicima Bolnice ili vanjskim saradnicima koji su angažirani na poslovima nadogradnje mreže.

Ukoliko je podržan rad na daljinu, na primjer kada je djelatnicima dopušteno izvan radnog mjesta (putem Interneta ili bežičnog pristupa sistemu ustanove) ažuriranje podataka, potrebno je donošenje posebnog pravilnika kojega se moraju svi pridržavati. Pravilnikom se definiraju postupci kojima bi se spriječilo ugrožavanje informacijskog sistema ustanove. Povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se nalazi u ustanovi.

Ustanova je također obavezna odrediti pravila spajanja gostujućih računala na vlastiti sistem, kako bi se onemogućilo da takva računala budu izvor zaraze (virusa, crva, trojanskih konja), kako bi se onemogućilo presretanje prometa ili prikupljanja informacija, te da namjernim ili slučajnim destruktivnim radnjama ne bi ugrozili sistem. Jedan od načina rješenja problema je da se gostujuća računala mogu spojiti na određenim priključnim tačkama, s kojih nije moguće pristupiti računalima kompanije.

11. Instaliranje i licenciranje programske podrške

Korištenje ilegalne programske podrške nezakonito je i predstavlja povredu autorskih prava. Kako bi se ustanova zaštitila od materijalne i javne štete nastale korištenjem ilegalne programske podrške, potrebno je provoditi kontrolu da li su programi instalirani na računalima sistema licencirani. Da bi se takva kontrola što kvalitetnije provodila, bitno je odrediti odgovornu osobu koja je zadužena za instaliranje, održavanje i licenciranje programske podrške na svim računalima sistema. Korisnik koji ima potrebu za nekim programom, dužan je za nabavu i instalaciju programa obratiti se odgovornoj osobi.

Sve korisnike potrebno je također obavezati na pridržavanje autorskih prava, na primjer potpisivanjem izjave da je upoznat sa pravilima prihvatljivog korištenja. U slučaju eventualnog kršenja zakona, ustanova svu odgovornost prebacuje na nesavjesnog korisnika.

12. Politika postupanje u slučaju incidenta

Iako je moguće uložiti velika sredstva i angažirati najbolje stručnjake za definiranje i implementiranje sigurnosti u sistem, danas je nemoguće informacijski sistem učiniti potpuno sigurnim. Veliki propust u organizaciji sigurnosti napravljen je ako se ta činjenica ignorira. Kako bi se postigla najveća moguća sigurnost sistema, bitno je shvatiti da je svaki sistem ranjiv i da bilo koji može postati metom napada. Sistemi koji imaju kvalitetno definiranu strategiju u slučaju napada, eventualni napad

neće izazvati veće probleme. Sistemi koji takvu strategiju nemaju, u slučaju napada mogu pretrpjeti velike štete.

U slučaju da se napad na sistem ipak dogodi, važno je što prije sistem dovesti u stanje prije napada. Kako bi se to postiglo, bitno je odrediti osobu ili oformiti stručni tim koji će djelovati u slučaju napada. Da bi osoba ili tim mogao kvalitetno reagirati, potrebno je definirati pravila na koji način će se obnavljanje sistema provoditi. Kako bi se oporavak uspješno realizirao, potrebno je ustanoviti kako je sistem napadnut, koji dijelovi sistema su napadnuti i što je cilj napada. Ustanoviti na koji način je sistem napadnut vrlo je važno kako bi se izbjegli budući napadi i ispravili sigurnosni propusti. Kako bi stanje sistema bilo identično stanju sistema neposredno prije napada, bitno je otkriti što je sve promijenjeno u sistemu. Također je bitno saznati da li je, na primjer, mijenjanje podataka bio cilj napada, ili je ono samo maska stvarnog cilja.

Ako su sistemi napadnuti s ciljem mijenjanja ili brisanja podataka, korištenjem sigurnosnih kopija relativno je lako sistem osposobiti za daljnji rad. U slučaju krađe podataka ili nekom drugom zlouporabom napada vrlo je bitno pravnim postupcima reagirati kako bi se Bolnica zaštitila od daljnjih materijalnih i drugih šteta. Osoba koja namjerno uzrokuje kvar računarske mreže, računala ili bilo kojeg dijela informacijskog sistema, snosi troškove njihovog popravka. Drugačije je moguće postupati u slučaju kada je to tako dokazano i moguće. Sva postupanja se moraju voditi u skladu s važećim zakonima, pravilnicima Bolnice i ostalim propisima.

13. Korištenje elektroničke pošte (eng. e-mail)

Budući da danas poslovanje mnogih modernih kompanija ovisi o elektroničkoj pošti, sigurnosna politika mora osigurati da je kompaniji poznat u koje je svrhe njezini zaposlenici koriste. Također trebaju biti svjesni da elektronička pošta ima istu „težinu" kao i obično pismo poslano s potpisom tvrtke.

Zaposlenici moraju biti svjesni da kompanija omogućava korištenje elektroničke pošte samo za potrebe obavljanja posla. Mnoge kompanije trenutno dopuštaju zaposlenicima slanje i primanje privatne pošte korištenjem njenih sistema. U takvim okolnostima, zaposlenici moraju znati da je to dozvola koja ne smije biti zloupotrijebljena, niti brojem poslanih mail-ova niti trošenjem previše vremena za čitanje i pisanje privatne pošte. Korištenjem sistema za privatne potrebe mora biti dopušteno od osobe koja za to ima ovlasti.

Da bi zaštitili bilo kakvu zloupotrebu korištenja elektroničke pošte, mora postojati sistem za nadzor koji u bilo kojem trenutku bez prethodne obavijesti korisnika može pregledati sadržaj mail-a. Stoga je bitno korisnike i zaposlenike pravovremeno obavijestiti da korištenjem sistema za elektroničku poštu kompanije ne smiju očekivati nikakvu privatnost i da bi svu poštu koju šalju ili primaju mogla pročitati odgovorna osoba.

Sigurnosna politika mora definirati preventivne mjere kako bi zaštitila informacijski sistem kompanije, a koji bi mogao ugroziti sadržaj elektroničke pošte ili njoj dodana datoteka. Takva pravila su na primjer:

- Niti jedan program, datoteka, podatak ili dokument koji bi mogao narušiti sigurnosnu politiku, zakon, licenca prava ili dozvole kopiranja ne smiju se slati elektroničkom poštom
- Neprikladno korištenje sistema za poštu može rezultirati disciplinskim mjerama. Neprikladno korištenje podrazumijeva širenje tekstova, programa ili bilo kojih drugih datoteka koje bi moglo ugroziti politiku kompanije
- Korisnici su odgovorni da svaku datoteku primljenu s mail-om provjere od virusa i sadržaja.
- Primljena pošta koja krši politiku mora se smjesta prijaviti osobama odgovornima za sigurnost
- Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primajući i šaljući takve sadržaje možete izložiti tužbi ne samo sebe, već i Gradsku i sveučilišnu knjižnicu Osijek.

Zbog svega nabrojanog, korištenje elektroničke pošte smatra se rizičnom djelatnošću, te su korisnici obvezni pridržavati se sljedećih pravila:

- Svaki zaposlenik ima svoju mail adresu oblika: ime.prezime@obs.ba koju je dobio na korištenje tijekom vremena zaposlenja. To je službena mail adresa Bolnice i svi zaposlenici su dužni provjeravati svoju elektroničku poštu.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa redoviti rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.
- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i ustanovu za koju radite.
- Pridržavajte se etike i pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, za seksualno ili bilo koje drugo uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi a ljudima oduzima radno vrijeme.
- Svaka napisana poruka smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Nemate pravo poruke koju su poslane vama osobno proslijediti dalje bez dozvole autora, odnosno pošiljatelja.
- Sve poruke pregledati će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.

- Administrator sistema zadržava pravo konfiguriranja sistema na način da ne obavještava pošiljatelja i primatelja o otkrivenom virusu u poruci ukoliko se ustanovi da se radi o tzv. virusima koji lažiraju adresu.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.
- Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

14. Procedura za dodjelu e-mail adrese

Pri zapošljavanju novog uposlenika, šef organizacione jedinice zatraži od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa.

Pri prestanku radnog odnosa, šef organizacione jedinice je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa.

Ako zaposlenik nakon odlaska u mirovinu zatraži nastavak korištenja korisničkog računa to mu se, uz suglasnost Direktora može odobriti.

15. Pravilnik o antivirusnoj zaštiti

Virusi i crvi predstavljaju opasnost za informacijske sisteme jer ugrožavaju funkcioniranje mreže i povjerljivost podataka.

Nove generacije virusa su izuzetno složene i opasne, sposobne da prikriju svoju nazočnost, presreću unos podataka na tipkovnici. Informacije poput lozinki ili povjerljivih dokumenata mogu poslati svome tvorcu nekamo na Internet, te otvoriti kriptiran kanal do vašeg računala, kako bi nad njim kontrolu preuzeli hackeri.

Stoga je zaštita od virusa obaveza administratora računala i svakog korisnika.

Zaštita od virusa je obavezna i treba da se provodi na nekoliko nivoa:

- na poslužiteljima elektroničke pošte
- na internim poslužiteljima, gdje se stavlja centralna instalacija
- na svakom osobnom računalu korisnika.

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju sa centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju prethodno obavijestiti administratore sistema.

Nepridržavanje

Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu, te na taj način izazove štetu, bit će kažnjen.

16. Sigurnosne kopije podataka

Za sve podatke koje informacijski sistem sadrži postoji opasnost da budu izgubljeni. Kako bi sistem u slučaju gubitka podataka mogao dalje funkcionirati važno je da te podatke na neki način vratimo. Najlakši način, a često i jedini, je taj da sva programska podrška i podaci budu kopirani na alternativni medij koji treba čuvati u sigurnim uvjetima. Na takav način podatke uvijek imamo zapisane na više mjesta. Ako se na jednom mediju unište (pokvari se disk), promijene ili obrišu (napad na sistem „iznutra" ili „izvana"), vrlo lako kopiranjem s alternativnog medija možemo opet doći do njih i vratiti sistem u funkciju.

Koliko često treba raditi sigurnosne kopije podataka, mora biti određeno u politici, a ono je razmjerno s važnosti da te podatke vratimo u slučaju njihova gubitka. Važne podatke koji se mijenjanju svakodnevno trebamo kopirati na alternativni medij što češće, dok se „statični" podaci, koji se rijetko mijenjaju, kopiraju rjeđe, na primjer kada dođe do mijenjanja podataka.

17. Pristup sistemu vanjskim suradnicima

Iako mnoge kompanije imaju svoje interno odjeljenje za održavanje opreme, postoje situacije kada se pristup sistemu mora dopustiti osobama iz drugih firmi zbog servisiranja, održavanja, konzultacija ili obuke. Bitno je da u tom slučaju u ugovorima s vanjskim tvrtkama donesemo odredbe kojima se vanjski partneri obvezuju na poštivanje sigurnosnih pravila. Ako se podaci mogu klasificirati kao tajna, potrebno ih je privremeno ukloniti sa sistema prije nego osoblje koje nije zaposleno u kompaniji dobije pristup sistemu za obavljanje posla.

18. Kontrola pristupa Internetu

Mnogo tvrtki pruža svojim zaposlenicima mogućnost pristupa Internetu. Iako je takav Internet obično namijenjen u svrhe poslovanja, osoba odgovorna za sigurnost mora osigurati da politika jasno savjetuje korisnike, tj. osoblje na koji način pristupiti Internetu, ne samo zbog povećanja propusnosti mreže već i zbog sprječavanja

ilegalnih radnji. Politika mora jasno naglasiti da je upotreba Interneta isključivo u svrhe poslovanja.

Bolnica također pruža usluge pristupa internetu preko bežične Wi Fi mreže koja radi odvojeno od kablovske mreže za pacijente i posjetioce Bolnice, uz poštovanje svih sigurnosnih protokola.

19. Fizička sigurnost sistema

Kako bi informacijski sistem bio potpuno siguran, bitno je osigurati kvalitetnu fizičku zaštitu sistema. Fizičkom zaštitom sistema želi se spriječiti bilo kakvo fizičko djelovanje na sistem koje bi moglo ugroziti povjerljivost, dostupnost i integritet podataka.

Fizičku sigurnost sistema mogu ugroziti ljudi i prirodni procesi. Prirodni procesi, kao što su potresi, poplave ili požari, javljaju se u malom postotku ali uzrokuju vrlo velike štete. Iz tih razloga opremu poput poslužitelja ili diskovnih jedinica na kojima su pohranjeni važni podaci potrebno je smjestiti u posebne prostorije. U takvim prostorijama nužno je ugraditi alarmne sisteme u slučaju požara ili poplave, kako bi se eventualni rizici na vrijeme uočili.

Oprema neophodna za rad sistema također treba biti zaštićena od mogućeg nestanka električne energije, tj. potrebno je osigurati alternativne izvore energije (akumulatori i generatori) koji bi pri takvom kvaru omogućili daljnji rad. Vrlo je važno dodatno osigurati sistem napajanja od prenapona, kako bi se spriječio kvar opreme od strujnih udara.

Vrlo je bitno je odrediti odgovornu osobu koja će brinuti o ključnim pitanjima kao što su dobivanje dozvola za pristup prostoriji ili njeno održavanje, te prostoriju držati pod strogim nadzorom.

20. Sigurnost radnog računala

Velika prijetnja sigurnosti sistema može nastati ako zaposlenik ostavi nezaštićeno računalo, bez nadzora prijavljeno na sistem. Takvo računalo tada može doći u ruke osobi koja nema ovlasti pristupa i koristiti ga u neprihvatljive svrhe. Zbog toga korisnici moraju biti svjesni da pri napuštanju radnog mjesta moraju osigurati da se niko drugi ne može služiti računalom pod njihovom identifikacijskom oznakom kojom su prijavljeni na sistem. To se može postići privremenim odjavljivanjem sa sistema ili korištenjem određenih programa koji za rad traže unos lozinke. Iz sličnih razloga, ako je moguće, potrebno je omogućiti da korisnik na sistem može biti prijavljen samo jednom. Time se sprječava da se korisnik prijavi istovremeno na više terminala, tj. ostane prijavljen na jednom od terminala i tako omogući drugim osobama korištenje sistema.

21. Prihvatljiva i neprihvatljiva ponašanja

Svaka zloupotreba dostupnih informacija spada u neprihvatljivo ponašanje i treba biti sankcionirana na odgovarajući način.

Pretpostavka sigurnog informacijskog sistema temelji se na ljudima koji se koriste informacijskim sistemom i to isključivo na načine koji su sigurni za cjelokupni sistem. Tehnologija ne može sama osigurati najvišu razinu sigurnosti, te zbog toga svi moraju imati svoju ulogu te ju savjesno i redovito izvršavati. Važno je uvesti sve potrebne mjere za očuvanje sigurnosti. Prije svega, to je moguće kroz definiranje sigurnosne politike, krovnog dokumenta za održavanje sigurnosti informacijskog sistema. Uloga sigurnosne politike je određivanje prihvatljivog i neprihvatljivog načina ponašanja, što joj je i primarna uloga, a cilj je zaštititi vrijednosti informacijskog sistema, opremu, programsku podršku i podatke.

Po definiciji pojmova vrijedi sljedeće:

-Povjerljivost se temelji na pretpostavci da se podaci čuvaju u skladu s propisanim zakonima, pravilnicima i drugim propisima u ustanovi

- Integritet se temelji na pretpostavci da su svi podaci cjeloviti i očuvani od vanjskih utjecaja koji mogu integritet narušiti

- Dostupnost se temelji na pretpostavci da su svi podaci dostupni samo onim osobama koje imaju pravo pristupa određenim podacima.

Prihvatljivo ponašanje

Informaciona sistem Bolnice, BIS i mreža računara stoje korisnicima na raspolaganju radi:

- obavljanja posla, - pregleda pacijenata, zakazivanja pregleda, kreiranja dnevnih, mjesečnih i godišnjih izvještaja, učenja, podučavanja, istraživanja, usavršavanja u struci,

- drugih razloga koje menadžment Bolnice daje suglasnost, pismeno ili usmeno

Sva prava korisnici su dužni ostvarivati poštujući potrebe i prava ostalih korisnika informacijskog sistema. Svako korištenje informacijskog sistema je prihvatljivo korištenje, ako se ne krše smjernice i pravila, te ako nisu narušena tuđa prava. Prihvatljiva ponašanja definirana su politikom sigurnosti.

Neprihvatljivo ponašanje

Neprihvatljivo ponašanje je svako ponašanje koje nije dopušteno ovim smjernicama ili pravilnikom. Neprihvatljivo je stvaranje ili prijenos datoteka (osim eventualno u okviru znanstvenog istraživanja):

- materijala koji je napravljen da bi izazvao neugodnosti, neprilike ili širio strahove,

- uvredljivog i ponižavajućeg materijala

- distribuiranje autorski zaštićenih djela bez dozvole vlasnika prava

- korištenje računarske mreže Opće Bolnice „Prim. dr. Abdulah Nakaš" na takav način da ometa korištenje drugim korisnicima

- širenje, virusa, trojanaca, crva i ostalog zlođudnog softvera,

- slanje neželjenih masovnih poruka

- preuzimanje tuđeg identiteta,

- provaljivanje na računala koristeći sigurnosne propuste u softveru

- traženje sigurnosnih propusta na umreženim računalima bez dozvole vlasnika opreme

- izvršavanje napada uskraćivanjem resursa (Denial of Service)

- korumpiranje ili uništavanje podataka drugih korisnika

- povreda privatnosti drugih korisnika

- uništavanje tuđih podataka

- neovlašteno korištenje tuđih radova

- kopiranje ili instaliranje softvera za koje ne postoji licenca

- drugih načina kršenja koji nisu u skladu s općeprihvaćenim normama i standardima

22. Raspodjela zadataka

Zadaci tijekom nadzora pridržavanja smjernica i pravila sigurnosti Opće Bolnice "Prim. dr. Abdulah Nakaš" raspodijeljene su na sljedeći način:

- Odgovorne osobe Odsjeka za IT: preuzimaju prijave o mogućem kršenju smjernica i pravila ponašanja tijekom korištenja informacijskog sistema, redovito održava dijelove informacijskog sistema, kreira izvješća o obavljenim aktivnostima provedenim na temelju dobivenih prijava, redovito održava dijelove informacijskog sistema

- Ljekari: preuzima prijave o mogućem kršenju smjernica i pravila ponašanja tijekom korištenja informacijskog sistema

-Glavni medicinski tehničar Bolnice treba da vodi računa o provođenju ove politike, učestvuje u procesu davanja ovlasti za pristup informacionom sistemu Bolnice i BIS-u, ostvaruje kontakte sa odgovornim osobama Odjeka i MEDIT-a ukoliko je potrebno da se novom zaposleniku dodjele ovlasti vezane za pristup informacionom sistemu Bolnice i BIS-u.

- Medicinski tehničari: prijavljuju incidente na propisan način, definiraju pravila ponašanja i korištenja računarske opreme, u skladu s propisanim pravilnicima i politikom sigurnosti Bolnice. Dužni su upozoriti druge osobe koje se nalaze u Bolnici ukoliko primijete da se radi o ugrožavanju sigurnosti informacijskog sistema

- Ostali zaposlenici: prijavljuju incidente na propisan način

- Pacijenti: prijavljuju incidente na propisan način

- Druge osobe u Bolnici: prijavljuju incidente na propisan način

Odgovorna osoba Odsjeka za informaciono komunikacijske tehnologije, Menadžment Bolnice, ostali zaposlenici Bolnice mogu koristiti računalnu opremu za čiju upotrebu imaju dodijeljenu ovlast.

23. PACS sistem

Bolnica ima pristup PACS sistemu (Picture Archiving and Communication System – Sistem za pohranu i distribuciju snimaka) u okviru ovlasti koje su date medicinkom osoblju od strane viših instanci na nivou Kantona Sarajevo.

Pristup Sistemu korisnici imaju preko IMPAX-a preko kojih ovlašteni korisnici mogu pristupati radiološkim snimcima pohranjenim u Sistemu.

Osim gore navedenog načina, moguće je pristupiti preko BIS-a preko opcije radiološki snimci pacijenta unutar Medicinskog kartona pacijenta ukoliko korisnik ima pristup BIS-u i ovlaštenja da otvara pohranjene snimke.

24. Elektronske zdravstvene kartice

Pacijenti koji imaju elektronske zdravstvene kartice se korištenjem JMBG-a i bar koda mogu prijaviti u sistem. Na odgovarajućim punktovima su postavljeni čitači bar koda.

Izdavanje kartica je u nadležnosti Zavoda za zdravstveno osiguranje kantona.

25. Literatura:

1. http://www.marketmakers.ba/bundles/websitenews/gallery/files/15/1492083973Studija_razvoja_IT_sektora_u_Kantonu_Sarajevo.pdf
2. http://www.healthcareitnews.com/news/5-tips-creating-strategic-plan-it
3. http://www.obsm.rs/obsm/wp-content/uploads/2011/07/Strateski-plan-2015-2020.pdf

Dodatak:

26. Standard 2.5.2- Naputci pri pisanju sigurnosne politike

Pri definiranju sigurnosne politike, važno je obratiti pozornost na slijedeće naputke:

Na koga se politika odnosi. Vrlo bitno je jasno i nedvosmisleno odrediti na koga se odnosi definirana sigurnosna politika i tko je se treba pridržavati. Ako se izričito ne naglasi, moguće je da sigurnosna politika bude ignorirana od strane onih kojima je namijenjena.

Politika mora biti primjenjiva. Napisana sigurnosna politika mora biti primjenjiva u smislu da se ne krše moralna ili kulturološka načela, da politika ne sprječava obavljanje svakodnevnih poslova ili da se odnosi na nepostojeće činjenice. Kršenje osnovnih ljudskih prava može dovesti do razdraženosti korisnika sistema i uzrokovati suprotan učinak. Definiranje pravila o nepostojećim činjenicama, na primjer odnos korisnika prema nepostojećoj opremi, može kod korisnika izazvati ne razumijevanje i odbacivanje politike. Stoga je vrlo važno politiku redovito pregledavati i po potrebi izmjenjivati ili nadopunjavati.

Upoznati korisnike s politikom. Pri prvom donošenju sigurnosne politike velik broj korisnika vjerojatno neće znati što je zapravo sigurnosna politika i čemu ona služi. Stoga je bitno odrediti vremenski period u kojem će korisnici moći proučiti politiku, imati mogućnost postaviti pitanja o dijelovima koje ne razumiju, dati svoju kritiku ili moguće prijedloge izmjena. Stupanjem na snagu politike u trenutku njenog donošenja mnogi korisnici zbog needuciranosti možda ne bi znali o čemu se radi, niti bi se konzultirali sa stručnim osobljem kako ne bi ostavili negativan dojam, te ju ne bi ni primjenjivali.

Politika mora biti kratka. Sigurnosna politika koja se odnosi na korisnike sistema mora biti kratka. Korisnici nemaju strpljenja čitati desetke stranica tekstova o mogućnostima napada i eventualnim rizicima. Važno je jasno, nedvosmisleno, vrlo kratko i običnim riječima napisati čega se moraju pridržavati, što smiju odnosno ne smiju raditi. Sigurnosna politika koja je namijenjena administratorima informacijskih sistema ne treba biti kratko napisana, štoviše, preporučljivo je da ona bude što detaljnija i obuhvaća što više činjenica.

Uskladiti politiku s ostalim dokumentima. Važno je definiranu sigurnosnu politiku prikazati kao i svaki drugi važan dokument u vlasništvu kompanije. Način na koji je ona otisnuta na papiru ili prikazana na Internetu, upućuje na to koliko je pažnje posvećeno sigurnosnoj politici. Dodavanjem logotipa kompanije s uredno napisanom sigurnosnom politikom vidljiv je značaj dokumenta te će mu korisnici pristupiti ozbiljno. U suprotnom korisnik može shvatiti da to nije važan dokument budući mu ni odgovorni ne posvećuju pažnju te će ga ignorirati.

Izbor riječi. Izbor riječi također je važan za interpretaciju sigurnosne politike. Korištenjem riječi poput „morate" ili „trebate" dajemo puno ozbiljniju poruku od one ako se koriste riječi „trebali biste" ili „možete".

Podrška. Važno je osigurati da korisnici informacijskog sistema u svakom trenutku imaju odgovarajuću podršku. Nerazumijevanje politike u bilo kojem smislu može uzrokovati neželjene posljedice, stoga je bitno korisnicima osigurati kontakt osobu kojoj se mogu obratiti u vezi bilo kakvih nejasnoća. Također je važno da postoji osoba kako bi korisnik mogao prijaviti uočene nepravilnosti.

Odgovornost korisnika. U svakoj sigurnosnoj politici bitno je naglasiti koje su posljedice i tko je odgovoran za eventualne propuste. Naglaskom da je svaki korisnik odgovoran za nepridržavanje pravila definiranih sigurnosnom politikom i da će za to biti sankcioniran, prisiljava korisnike na razumijevanje politike i njezino pridržavanje.

Odgovorna osoba. Svaki informacijski sistem treba imati glavnu i odgovornu osobu o pitanju sigurnosti sistema. Jedan od značajnih problema u sigurnosti je neznanje o tome tko je za što odgovoran. Strogim određivanjem granica odgovornosti pojedinih osoba i određivanjem glavnog odgovornog napravljen je velik korak k cjelokupnoj sigurnosti informacijskog sistema.

Kontrola poštivanja politike. Nakon definiranja sigurnosne politike vrlo važno je da je se korisnici i pridržavaju. Stoga je bitno provesti nekoliko koraka kako bi bili u to sigurni. Jedan od njih je kontroliranje korisnika. Korisnici se mogu kontrolirati na više načina, kratkim testovima s pitanjima koja se odnose na sigurnosnu politiku i tajnom kontrolom korisnika.

Ažuriranje sigurnosne politike. Jednom definirana sigurnosna politika zbog raznih razloga nakon nekog vremena može postati neprimjenjiva. Zbog svoje neprimjenjivosti može izgubiti funkciju stoga je bitno konstantno politiku ažurirati, mijenjati ili izbrisati neprimjenjive dijelove i po potrebi dodati nova pravila. Kako zbog odgađanja ažuriranja politika ne bi izgubila funkciju, važno je odrediti najveći vremenski interval koji može proteći bez ažuriranja sigurnosne politike. Intervali koji se najčešće određuju su između šest mjeseci i godine dana.

Nekoliko je tema koje bi se trebale uzeti u obzir pri ažuriranju sigurnosne politike:

- Politika mora biti važeća. Sva pravila koja se odnose na nepostojeću opremu (npr. naknadno isključenu iz sistema)moraju biti uklonjena. (Primjer: pravila koja se odnose na floppy diskovne ulazno-izlazne jedinice, koje više ne postoje u sistemu, moraju biti uklonjena iz politike)

- Dogodila se promjena u procesima sistema (Primjer: Politika kontrole virusa provodi se samo kontrolom floopy disketa, a floopy jedinice više ne postoje u sistemu, važno je da se ta pravila uklone iz politike)
- Uvedena je nova tehnologija od zadnje kontrole politike
- Korisnici sistema su prešli na korištenje ručnog računala (*eng. PDA - Personal Digital Asistents*)

Datum zadnjeg ažuriranja. U svakoj sigurnosnoj politici mora biti naznačeno od kojeg se datuma primjenjuje i kojeg datuma je napravljena zadnja izmjena. Ovaj podatak je vrlo bitan kako se ne bi dogodilo da odgađanjem ažuriranja politika zastari.

Broj: 24-160/18

Sarajevo, 25.09.2018. godine

Predsjednik Upravnog odbora

Dr. Sead Željo