Политика безбједности
интегрисаног здравственог информационог система
Републике Српске

Сектор за Информационе технологије
2018.

Садржај:

1. Политика класификације података

Сврха ове политике је да успостави стандард (у складу са стандардом ISO/IEC 27001:2005) и одреди смјернице за заштиту информација унутар интегрисаног здравственог информационог система (у даљем тексту ИЗИС) од разних пријетњи као и да обезбиједи континуитет пословања.

Ова политика се односи на све здравствене установе и кориснике ИЗИС-а. То важи и за извођаче, консултанте, привремено запослене, подизвођаче или било која трећа лица са којима здравствене установе, организације и институције у саставу ИЗИС-а имају било какву пословну сарадњу.

Информација, без обзира у којој је форми (писана, говорна, штампана или електронска) је примарно средство за пословање, које има своју вриједност и зато је неопходно да се адекватно заштити. Информације заједно са осталим средствима и компонентама (људи, процеси, здравствене установе, процедуре, услуге, хардвер, софтвер, инфраструктура, опрема…) чине ИЗИС.

Ресурсе, који припадају различитим категоријама, могуће је класификовати на разне начине. С обзиром на то да је у информатичком систему ипак најважнија сама информација, потребно је успоставити одговарајући систем класификације.

Унутар система уопштено су похрањене информације различитих вриједности за организацију: од потпуно неважних до оних кључних, па и критичних. Циљ класификације информација је осигурање њихове одговарајуће заштите.

Класификација се обично проводи с обзиром на постављене критерије (вриједност саме информације, утицај времена на њену вриједност, повезаност с појединим особама итд.). У већини систем ап тако и у ИЗИС-у уопштено је прикладан сљедећи систем класификације:

- Јавне,
- Осјетљиве,
- Повјерљиве,
- Тајне.

Јавне информације могу се понекад поистовијетити и с информацијама које не спадају у систем класификације, а односе се на оне информације чије откривање не представља никакав потенцијални ризик за кориснике те пружаоце здравствених услуга унутар ИЗИС-а. За њих обично није нужно поставити безбједоносни надзор.

Осјетљиве информације захтјевају већи ниво надзора јер њихово откривање или губитак интегритета могу изазвати одређене губитке (који не морају бити изворно материјалне природе).

Повјерљиве информације су намијењене само употреби унутар здравствених установа, Фонда. Њихово откривање може имати негативан утицај на кориснике те пружаоце здравствених услуга унутар ИЗИС-а, тако да је нужна имплементација одговарајућих безбједоносних механизама.

Тајне информације односе се на најосјетљивије податке и било какве неовлаштене активности везане уз њих могу довести до врло озбиљних посљедица за систем. Одговарајућа имплементација безбједности за овакве информације је од критичне важности.

Подаци који се колектују и чувају унутар ИЗИС-а представљају осјетљиве податке личности и могу се подјелити у неколико група:

- Демографски - административни подаци (идентификациони подаци и контакт),
- Социо-медицински подаци:
  - Медицинске информације (крвна група РХ фактор, давалац органа),
  - Социјални статус (брачни статус, занимање, заполење, итд),
- Здравствеи подаци:
  - Здравствени подаци стандардне осјетљивости,
  - Осјетљиви („скривени“) здравствени подаци.

Осјељиви подаци се идентификују на два начина:

- На нивоу дијагноза:
  - Подаци везани за ХИВ и хепатитисе,
  - Подаци у вези са менталним здрављем (психијатријом),
- Подаци везани за околности:
  - Подаци у вези са злоупотребном супстанци (дрога, алкохол и сл.),
  - Подаци везано за сексуално и породично насиље,
  - Подаци везани за алтернативни животне стилове (сексуална орјентација, филозофска убјеђења, алтернативне религије итд).

Наведене групе података су доступне надлежним здравственим радницима ако није другачије регулисано, уз обавезно праћење и контроле приступа.

Уз процјену ризика потребно је одредити како поступати с ризицима. Могући поступци укључују:

- Уграђивање одговарајућих контрола које смањују ризик,
- Свјесно и објективно прихватање ризика, удовољавајући безбједоносној политици ФЗОРС и критеријима прихватљивог ризика,
- Избјегавање ризика забранама, тј. онемогућавањем акција које узрокују ризик.

За ризике чији поступци укључују имплементацију одговарајућих контрола, те контроле морају бити одабране и имплементиране задовољавајући захтјеве дефинисане процјеном ризика.

Контроле морају осигуравати да су ризици редуцирани на прихватљив ниво узимајући у обзир:

- Ограничења и захтјеве дефинисане националним и интернационалним законима и прописима,
- Циљеви ФЗОРС,
- Оперативне потребе и ограничења,
- Цијену имплементације.

2. Политика управљања ризицима

2.1. Управљање ризицима информационих система

Независна контрола ИТ операција као и процјена функционалности ИТ сервиса и степена њихове подршке процесима организације су витални за заштиту ИТ ресурса, информација и ИТ система као и побољшање пословања. Управљање ризиком треба да обухвати цјелокупни информациони систем организације и све ИТ ресурсе. То је континуирани процес упоређивања процијењених ризика с предностима и трошковима предложених мјера у складу с пословним циљевима. Овај процес генерално обухвата:

- Процјену ризика,
- Смањивање ризика,
- Одржавање прихватљивог нивоа ризика.

Потребно је размотрити различите врсте заштитних мјера, спровести анализу и узети у обзир прихватљив ниво преосталих ризика. Заштитне мјере се бирају зависно од вјероватноће појаве нежељеног догађаја и од његовог утицаја (квантитативног и квалитативног) на информациони систем и нарушавање његове функционалности и безбједности.

2.2. Приједлог приступа и планирање:

- Планирање и идентификовање процеса и одређивање приоритета,
- Идентификовање процесних ризика и њихово документовање,
- Сагледавање и документовање процеса, кључних ризика и процеса и контрола,
- Руковођење сценарија дизајна ризика,
- Размјена информација,
- Пренос знања,
- Идентификовање недостатака и пропуста у контролама,
- Анализа постојећих политика, процедура и интерних правила, подршка и идентификовање области у којима су потребна унапређења савјетовање и израда методологије.

2.3. Процедуре приликом тестирања ИТ контрола, процедуре које ћемо спровести се базирају на сљедећим корацима:

- Разговор са запосленима одговорним за поједине процесе,
- Преглед постојећих политика, процедура и интерних правила,
- Разумјевање дизајна и имплементације контрола,
- Извршавање контрола,
- Извршавање упита и скрипти,
- Скенирање коришћењем специфичних алата,
- Ручно тестирање параметара…

2.4. Приступ спровођењу ИТ контрола ФЗОРС методологија за спровођење ИТ Контрола подразумјева три групе контрола:

2.4.1. Опште ИТ контроле (IT General Controls)

Помажу при утврђивању поузданости података генерисаних од стране ИТ система и осигуравању да системи функционишу у складу са намјеном и да је излаз поуздан. Обично укључују сљедеће области:

- Приступ програмима и подацима,
- Компјутерске операције,
- Измјене програма,
- Управљање пројектима и развој програма.

Апликативне контроле - везане су за трансакције и податке у оквиру апликативних система. Обезбјеђују потпуност и тачност података као и валидност уноса без обзира да ли су настали обрадом програма или су резултат ручног уношења података.
Основне контроле се односе на:

- Унос (улаз) података,
- Верификацију,
- Процесирање (обраду),
- Излаз контроле миграције,
- Према потреби врши се сет контрола ради провјере миграције/конверзије података.

Опште ИТ контроле - детаљи

Општи преглед организације:

- ИТ Организација,
- ИТ Стратегија, политике и процедуре,
- ИТ Лиценце и уговори.

Преглед хардверске инфраструктуре:

- Сервери,
- Радне станице,
- Мрежна опрема,
- Остала опрема.

Преглед софтвера:

- Оперативни системи,
- Базе података,
- Апликације,
- Интерфејси.

Приступ програмима и подацима:

- Функција безбједности информација,
- Формализована политика безбједности,
- Класификација и власништво над подацимаи процесима,
- Приступ трећих страна ресурсима ИС,
- Интерна ревизија и “self assesment“,
- Процеси ауторизације,
- Логичке контроле приступа,
- Контрола лозинки,
- Привилегије корисника,
- Супер корисници и администрација,
- Подјела одговорности,
- Ревизија права приступа,
- Механизми за логовање,
- Контроле за приступ мрежи,
- Антивирусна, антиспам и firewall заштита,
- Политике инсталирања софтвера и приступа интернету,
- Физичке контроле приступа.

Измјене у програмима:

- Процес управљања промјенама,
- Тестирање и контрола промјена,
- Миграција промјена у оперативни режим рада,

- Битне измјене у односу на претходну контролу.

Управљање пројектима и развој програма:

- Процес одобравања,
- Управљање пројектом и развојне методологије,
- Процес тестирања.

Компјутерске операције:

- Процедуре за бекап и опоравак,
- План континуитета пословања/План опоравка у случају несреће,
- Процедуре за управљање проблемима и Мониторинг,
- Help desk,
- Управљање инцидентима.

2.4.2. Апликативне контроле

Апликативне контроле се односе на разне контроле рада апликација и најчешће су специфичне само за конкретне системе. Могу бити угњеждене у пословне процесе употребом апликација и покривају:

- Унос (улаз) података,
- Верификацију,
- Процесирање (обраду),
- Излаз.

Ове контроле пружају гаранцију да ће апликација радити у складу са захтјевима и да је информација тачна, правовремена и потпуна. Омогућавају да контроле одмах реагују, ако се подаци не поклапају.

Примјери апликационих контрола: Контроле комплетности, Валидационе контроле, Контроле идентификације, Провјера резултата аутоматских обрада, Провјера енкрипције података у процесу преноса… У ову категорију спадају и бројне контроле самог пословног софтвера, оперативних система, инсталација и одржавања софтвера, преноса података, рада безбједносних софтвера, откривање грешака, узрока инцидената, конфигурација опреме, праћење рада системског софтвера и сл.

2.5. Провјера миграције података и система према потреби врши се сљедећи сет контрола ради провјере миграције/конверзије података:

- Утврђивање обима и процеса миграције као и укључених кадрова и власника података,
- Провјера постојања јасне идентификације свих података које треба мигрирати,

- Процјена контрола које треба да утврде да ли постоји одговарајуће вођење и извршење,
- Процјена да ли су мигрирани подаци тачни и релевантни,
- Процјена комплетности мигрираних података,
- Провјера безбједности података и заштите од намјерне или случајне измјене током миграције,
- Утврђивање да ли су подаци добро мапирани,
- Преглед и процјена излазних критеријума,
- Провјера да ли је нови систем дизајниран да омогући функционалност апликативних контрола.

2.6. Примјер резултата једног пројекта:

- Опис спроведених корака,
- Сажет приказ ваше ИТ организације као и хардверске и софтверске инфраструктуре,
- Налази, идентификовани ризици и препоруке за спроведене контроле,
- Наше разумјевање изазова,
- Приоритети за рјешавање,
- Процјењен број мјесеци за реализацију,
- Оквирна динамика,
- Приједлог рјешења,
- Оквирни износ инвестиција,
- Предности и недостаци за могуће опције,
- Преглед најзначајнијих налаза и препорука за ИТ безбједност,
- Унапређене интерне процедуре.

3. Политика контроле приступа

3.1. Контрола приступа у складу с пословним захтјевима

Приступ информацијама, јединицама за обраду информација и пословним процесима треба бити контролисан на темељу захтјева пословања и система безбједности.

3.2. Политика контроле приступа

Права приступа сваког појединца или групе кориснике требају бити јасно дефинисана у политици контроле приступа.

Политика контроле приступа треба обухватити:

- Захтјеве безбједности појединачних пословних апликација,
- Идентификацију свих информација везаних уз пословне апликације,
- Политику за ширење и ауторизацију информација (класификација),
- Конзистентност контроле приступа с политиком класификације информација у разним системима,
- Релевантне законе и уговорене обавезе које се односе на заштиту приступа,
- Стандардизоване профиле приступа за уобичајене категорије послова,
- Управљање правима приступа.

3.3. Контрола приступа мрежи

Контрола приступа мрежним сервисима (интерним и екстерним) нужна је како би се спријечило компромитовање безбједности од стране корисника који имају приступ мрежи и мрежним ресурсима. Безбједност мрежних сервиса потребно је провести кроз:

- Осигурање одговарајућих окружења,
- Осигурање механизама за провјеру вјеродостојности корисника и опреме,
- Контролу корисничког приступа до информационих сервиса.

Један од корака успостављања безбједности приступа мрежи је у дефинисању политике према којој корисници смију приступити само оним сервисима за која имају уређена права приступа. Уколико корисник нема дефинисана права приступа, приступ сервису је забрањен. Како би забрана или дозвола приступа била могућа, потребно је имплементирати квалитетне контроле идентификације и ауторизације, те дефинисати процедуре за заштиту приступа мрежи мрежним сервисима.

Дефинисање прописаног пута од терминала до сервиса безбједоносна је контрола која спрјечава злонамјерног корисника да искористи неауторизовани приступ апликацијама и уређајима за обраду података. Дефинисањем прописаног пута кориснику се не допушта бирање пута од терминала до сервиса, тј. могуће је бирати само прописане. Принцип ове контроле је да се на сваком чвору унапријед одреде допуштене руте.

Примјери прописаних рута:

- Додјела сталних линија,
- Аутоматско спајање улаза на одређене апликације,
- Лимитирање опција у менијима за одређену групу корисника,
- Све врсте активних контрола.

3.4. Контрола приступа оперативном систему (ОС)

Како би спријечили неовлаштени приступ рачунарским ресурсима, потребно је успоставити безбједносне механизме и унутар самог ОС.

Тиме се:

- Провјерава идентитет сваког овлашћеног корисника,
- Провјерава се локација терминала,
- Биљеже успјешни и неуспјешни приступи систему,
- Осигурава примјерен начин провјере вјеродостојности (квалитетне лозинке и сл.),
- Ограничава вријеме повезивања корисника (ако је потребно).

За контролу приступа ОС потребно је успоставити:

3.4.1. Аутоматску идентификацију терминала

Ова техника се користи и нужна је уколико се комуникација иницира с одређене локације или с одређеног терминала, како би се осигурала безбједност идентификатора терминала потребно је терминал физички заштитити

3.4.2. Процедуре пријаве терминала

Приступ до информационих ресурса треба бити омогућен само након успјешне пријаве у систем, процедура мора бити таква да:

- Даје минималан број информација неауторизованом кориснику,
- не смије приказивати системске или апликационе идентификаторе све док се пријава успјешно не изведе,
- Мора приказивати обавијештења и упозорења да рачунару смију приступити само овлаштени корисници,
- Не смије приказивати помоћне поруке,
- Не смије назначити који дио података је нетачан,
- Мора ограничити број неуспјешних пријава,
- Треба биљежити неуспјешне пријаве,
- Треба дефинисати максимално и минимално вријеме извођења пријаве,
- Након успјешне пријаве треба приказати податке (датум и вријеме) задње успјешне пријаве и детаље о неуспјешним покушајима пријаве од задње успјешне.

3.4.3. Идентификација и провјера вјеродостојности корисника

Сви корисници морају имати јединствен идентификатор за своју личну употребу како би се накнадно активности могле повезати с појединим корисником. Из корисничког имена не смије бити могуће открити информације о нивоу корисникових привилегија.

3.4.4. Систем управљања лозинкама

Употреба лозинки најчешћи је облик начина доказивања идентитета, стога је потребно осигурати квалитетан, интерактиван начин осигуравања квалитете лозинки.

Систем управљања лозинки треба:

- Наметати коришћење индивидуалних лозинки ради утврђивања одговорности (уколико је лозинка додијељена кориснику, приликом прве пријаве на систем потребно је лозинку промијенити),
- Наметати избор квалитетних лозинки,
- Наметати промјене лозинки,
- Спријечити коришћење већ коришћених лозинки (систем памти лозинке),
- Не приказивати лозинку на екрану приликом уноса лозинке,
- Похранити лозинке у криптованом облику, користећи алгоритме за једносмјерну енкрипцију, одвојене од апликацијских података.

3.4.5. Вријеме неактивности терминала

Терминале пријављене на систем који нису коришћени одређено вријеме, нпр. 5 мин, потребно је аутоматски одјавити. Вријеме неактивности дефинише се према ризичности локације (могућности приступа терминалу). Осим одјаве потребно је обрисати екран терминала, затворити све апликацијске и мрежне везе.

3.5. Праћење приступа и коришћење система

Активности у систему треба пратити и документовати ради правовременог уочавања одступања од политике контроле приступа и ради пружања доказа у случају безбједоносног инцидента.

3.6. Биљежење догађаја

Потребно је биљежити активности над системом те сакупљене информације чувати одређени временски период како би се осигурала подршка у случају инцидента и омогућило праћење система.

Информације које је потребно сакупити биљежењем догађаја:

- Корисничка имена,
- Датуме времена пријаве и одјаве из система,
- Ако је могуће идентитет рачунара (терминала) с којег је направљена пријава,
- Записе о успјешним и неуспјешним покушајима приступа систему,
- Записе о успјешним и неуспјешним покушајима приступа подацима и ресурсима.

3.7. Праћење употребе система

Како би се осигурало да корисници извршавају само оне активности за које су овлаштени, нужно је успоставити поступак за праћење употребе јединица за обраду података. Ниво праћења појединих јединица треба утврдити кроз процјену ризика.

Подручја о којима је потребно водити рачуна су:

- Овлашћени приступ (корисничка имена, датум и вријеме догађаја, типови догађаја, датотеке којима је приступано, коришћени програми),
- Привилеговане активности,
- Неовлашћени покушаји приступа,
- Системска упозорења и грешке.

Резултате добијене праћењем потребно је редовно прегледати и анализирати. Учесталост прегледа зависи о постојећим ризицима.

Факторе ризика које треба размотрити су:

- Критичност апликација,
- Вриједност, осјетљивост и критичност информација,
- Искуства о злоупотребама, неовлашћеним упадима и сл.

Посебну пажњу треба обратити на безбједност дневника записа о догађајима. Приликом додјеле одговорности за преглед дневника потребно је раздвојити улоге корисника које обављају преглед и оних чије се активности прате. Такође је потребно омогућити филтрирање логова, из разлога што дневници садрже велику количину информација од које је већина небитна за праћење безбједности.

Дневнике записа потребно је заштитити од активности као што су:

- Искључивање система за биљежење,
- Измјене типа забиљежених информација,
- Измјена или брисање података,
- Спријечити могућност прекида надзирања због недостатка простора на диску и сл.

Све набројане контроле не би имале очекивани учинак уколико није обављена синхронизација рачунарских сатова. Дневници догађаја често служе као доказ у судским или дисциплинским поступцима, стога непрецизни подаци могу угрозити кредибилитет

доказа. Сатове на рачунарима или комуникационим уређајима потребно је подесити на дефинсани стандард, нпр. локално стандардно вријеме, те морају постојати механизми који ће провјеравати и исправљати варијације.

3.8. Примјена норме у безбједносној политици

Због великог броја корисника ИСФЗОРС контрола приступа изузетно је важан безбједносни механизам којем је циљ спријечити, детектовати и документовати сваки покушај неовлашћеног приступа, било да се ради о хардверу или софтверу.

Како би контрола приступа као безбједоносни механизам био што квалитетније спроведен, потребно је осмислити прикладне методе идентификације, ауторизације али и методе заштите система од непажљивих корисника.

Контролу приступа угрубо можемо подијелити на:

- Контрола приступа софтверу,
- Контрола приступа опреми.

Контрола приступа софтверу темељи се на унапријед одређеним правилима. Став струке је да се права приступа не додјељују директно корисницима, већ да се она дефиншу кроз корисничке групе.

Због свакодневних потреба за новим групама немогуће је унапријед одредити све групе. Једино је важно да се свака створена група документује на јединственом мјесту које одреди одговорна особа.

Документација треба да садржи:

- Назив групе,
- Права приступа,
- Идентификација особе која је отворила групу,
- Датум и вријеме настанка групе,
- Рок трајања.

Права приступа појединим ресурсима треба бити садржана (документована), а документација треба да садржи сљедеће детаље:

- ИД - идентификација права приступа,
- Право приступа - читање, писање, извршавање,
- Идентификација особе која је створила запис,
- Вријеме и датум настанка записа.

Контрола приступа има задатак заштити систем у максималној мјери од непажљивих корисника и злонамјерних особа. Непажљиви корисници сматрају се они који на било који

начин, не придржавајући се политике безбједности, несвјесно помажу хакерима у злонамјерним радњама. Неки примјери су остављање рачунара пријављеног на систем без надзора, откривање корисничких имена и сл. Хакери уколико дођу у посјед пријављеног рачунара могу направити велику штету или искористити такав рачунар за прикупљање информација потребних за обављање злонамјерних радњи. Такође одавање било којих информација, чак и корисничког имена, хакерима увелике олакшава поступак напада на систем.
Како би се заштитили од непажљивих корисника потребно је имплементирати безбједносне контроле као што су:

- Аутоматска одјава са система уколико је рачунар неактиван 15 мин,
- Аутоматска одјава са система уколико је терминал неактиван 3 мин,
- Блокирање корисничког налога уколико се 3 пута узастопно унесе криво корисничко име и лозинка,
- „Присиљавање“ корисника на редовно мијењање лозинке, сваких 40 - 180 дана,
- Допуштање бирања само лозинки које задовољавају правила безбједносне политике итд.

Контрола приступа хардверу има идентичну сврху као и контрола приступа софтверу. Важно је осигурати приступ опреми само оним особама које за то имају потребу. Приступ опреми пружа се кроз давање овлаштења приступа просторијама у којима се опрема налази.

Правила приступа требају задовољавати сљедеће тачке:

- Опрема треба бити смјештена у одговарајућим просторијама, што је опрема осјетљивија, вреднија, садржи важније податке, то просторија треба бити под већим степеном заштите,
- Просторије у којима се налази осјетљива опрема требају бити означене одређеном ознаком која указује на „осјетљивост“ просторије,
- Приступ таквим просторијама треба бити омогућен путем идентификационих картица како би се могло проводити надзирање приступа; уколико из техничких разлога није могуће користити идентификационе картице, потребно је користити други безбједоносни механизам (кључ и слично),
- Потребно је обезбједити континуиран видеонадзор,
- Права приступа појединим просторијама треба бити документован.

Надзирање и безбједносне контроле не могу пружити 100% заштиту. Хакери ће увијек тражити пропусте и евентуалне „рупе у одбрани“ како би постигли свој циљ. Надзирање је безбједоносна контрола чија је сврха биљежити све поступке унутар ИС. Ова контрола врло је важна како би се на вријеме уочиле неправилности унутар система (обављање недопуштених радњи, напади, припреме напада и сл.).

Надзирање ИС ФЗОРС треба садржати сљедеће информације:

- Корисничка имена,

- Датуме времена пријаве у и одјаве из система,
- Ако је могуће идентитет рачунара с којег је направљена пријава,
- Записе о успјешним и неуспјешним покушајима приступа систему,
- Записе о успјешним и неуспјешним покушајима приступа подацима и ресурсима.

У данашње вријеме рад на преносним (мобилним) рачунарима све је учесталије, како због практичности тако и због пословних потреба. Чест је случај да корисници на састанке или на едукацију доносе своје преносне рачунаре помоћу којих се спајају на интерну мрежу и њима се користе. Овакав начин пословања сигурно има својих предности, али које захтјева додатне контроле на подручју безбједности.

Додатне безбједносне контроле требале би спријечити (отежати) све нападе који могу бити почињени због отварања права приступа с мобилних рачунала.

Наведене контроле првенствено требају обухватити:

- Начини заштите од малициозних програма,
- Начини и права приступа,
- Постављање безбједносне баријере.

Заштита од малициозних програма треба осигурати да мобилни рачунари не могу угрозити ИС зато што се на њему налази малициозни програм.

Осим заштите од малициозних програма потребно је дефинисати начине приступа треће стране ресурсима ФЗОРС. Начини приступа могу бити:

- Приступ web апликацијама,
- Приступ интернет провајдерима,
- Приступ искључиво одређеним директоријима и сл.

Дефинисањем начина приступа могуће је осигурати потребну функционалност без инсталирања, доградње и контроле мобилног рачунара корисника. Сва контрола саобраћаја одвија се путем безбједносне баријере и на страни провајдера.

У случају када није могуће једноставно одредити потребе корисника (нпр. само приступ web апликацијама), нужно је провести контроле којима ће се осигурати безбједност система. Наведене контроле првенствено укључују провјеру приликом спајања на систем да ли је на рачунару инсталиран потребан антивирусни софтвер, те превентивна контрола која укључује квалитетно додијељена права приступа.

Главна одговорна особа дужна је осигурати потребан антивирусни софтвер који је нужно имати инсталирано за спајање на ИС, те ажурирану базу с подацима о вирусима уколико се ажурирање базе не ради аутоматски приликом пријаве на систем.

Осим „техничких“ контрола безбједности, кориснике је потребно упознати с њиховим дужностима и одговорностима, те наведено документовати потписивањем Уговора о придржавању безбједосних правила.

<u>Напомена:</u> Ову политику у сажетом облику имате на крају овог документа као Прилог за кориснике.

4. E-mail политика

Електронска пошта дио је свакодневне комуникације, пословне и приватне. Комуницирањем e-mailom у установи, захтијева да се размотре сви аспекти електронске комуникације с обзиром на могуће посљедице.

Протокол који се користи за пренос електронске поште, SMTP или Simple Mail Transport Protocol није од самог почетка дизајниран да буде сигуран. Додатне проблеме понекад изазивају и корисници, који нису посве свјесни замки при коришћењу e-maila.

4.1. Откривање информација

Поруке намијењене једној особи, једноставно се могу прослиједити другима, нпр. на mailing листу. То се може догодити:

- (Зло)намјерно, с циљем да се нашкоди другој особи или ФЗОРС,
- Немаром судионика (радника), који не тражи дозволу за прослијеђивање поруке,
- Случајном грешком, на примјер нехотичним кликом мишем на погрешну икону (Reply All умјесто Reply).

Пословне дописе који садрже осјетљиве информације треба означити као повјерљиве, како бисмо примаоца обавезали на дискрецију.

У случају безбједносног инцидента, истрага може довести до откривања садржаја порука које су замишљене као приватна комуникација. ФЗОРС се обавезује чувати повјерљивост таквих порука, али то не може гарантовати ако поруке буду третиране као доказни материјал у истрази или у могућем судском процесу.

4.2. Радна етика

Велика количина порука које треба свакодневно прочитати може вам одузети знатан дио радног времена. Стога ограничите број приватних и забавних порука.

Ланчане поруке које људи шаљу познаницима могу садржавати лажне информације или бити дио преваре, с намјером да се корисницима извуче новац ("помозите болеснику којем треба операција", "отворите рачун како би избјегли предсједник могао извући новац из

нестабилне афричке државе"...). Овакве поруке треба игнорисати и брисати из mail клијента.

Spam, слање нежељених комерцијалних порука, све више оптерећује промет на Интернету, те одузима вријеме, чак и ако бришете такве порука без читања. Сервиси ће углавном филтрирати spam на клијенту електронске поште, али је обавеза корисника да сами не шаљу такве поруке.

4.3. Повреда ауторских права

Свака порука електронске поште може се сматрати ауторским дјелом, стога она припада особи која ју је послала. Стога за прослијеђивање туђе поруке морате тражити дозволу њезиног аутора.

Прилози (документи) који се шаљу уз електронске поруке могу садржавати ауторски заштићене информације. Примајући и шаљући такве садржаје можете изложити тужби не само себе, већ и ФЗОРС.

Због свега набројаног коришћење електронске поште сматра се ризичном дјелатношћу, те се корисници обавезују на придржавање одређених правила:

- Запосленицима се отвара кориснички рачун ради обављања посла,
- Приватне поруке дозвољене су у умјереној количини, уколико то не омета рад,
- Пишући поруке, будите свјесни да не представљате само себе, већ и ФЗОРС за коју радите,
- Придржавајте се етикете, правила пристојног понашања на Интернету, службену e-mail адресу немојте користити за слање увредљивих, омаловажавајућих порука, или за сексуално узнемиравање,
- Није дозвољено слање ланчаних порука којима се оптерећују мрежни ресурси и људима одузима радно вријеме,
- Свака написана порука сматра се документом, те на тај начин подлијеже прописима о ауторском праву и интелектуалном власништву. Немате право поруке коју су послане вама лично прослиједити даље без дозволе аутора, односно пошиљаоца,
- Све поруке прегледаће аутоматски апликација која открива вирусе. Ако порука задржи вирус, неће бити испоручена, а пошиљаоц и примаоц ће бити о томе обавијештени. Порука ће провести одређено вријеме у карантину. Након одређеног времена, обично мјесец дана, порука се брише из карантина како би се ослободио простор на диску,
- ФЗОРС задржава право филтрирања порука с намјером да се заустави spam,
- У случају истраге узроковане могућим безбједносним инцидентом, безбједносни тим може прегледати комплетан садржај диска, па тиме и e-mail поруке,
- Поруке које су дио пословног процеса треба архивирати и чувати прописани временски период као и документе на папиру.

4.4. Процедура за додјелу e-mail адресе

При запошљавању новог радника, руководилац затражи од администратора отварање корисничког налога електронске поште.

При престанку радног односа, руководилац је дужан најкасније у року од седам дана затражити затварање корисничког налога.

4.5. На кога се односе правила коришћења e-maila

Правила за коришћење e-maila односе се на све раднике ФЗОРС.

4.6. Непридржавање

Против корисника који не поштују ова правила ФЗОРС може покренути дисциплински поступак. У случају поновљених тежих прекршаја, кориснику се може затворити кориснички налог и ускратити право коришћења сервиса електронске поште.

Напомена: Ову политику у сажетом облику имате на крају овог документа као Прилог за кориснике.

5. Политика енкрипције

Осигурање система база података је важан задатак за ФЗОРС. ФЗОРС чува повјерљиве податке онда мора примјенити и задовољити многе законе и безбједносне стандарде.

Улога криптографије као елемента безбједности система база података долази до изражаја када се наруше елементи заштите као што је рецимо контрола приступа. Основни циљ криптографије јесте учинити податке неразумљивим и тешким за дешифровање неовлаштеним лицима, а који су успјели да дођу до њих након заобилажења свих осталих механизама заштите. Често се у литератури може наћи тврдња да је криптографија последња линија одбране база података.

Савремене криптографске методе везане су за криптографске алгоритме. Сваки криптографски алгоритам обухвата пар трансформација података, које се називају шифровање и дешифровање. Шифровање (енкрипција) је процедура која трансформише оригиналну информацију отворени текст у шифроване податке шифрат или криптограм. Обрнут процес, дешифровање (декрипција), реконструише отворени текст на основу шифрата.

Главни циљеви криптографије или безбједносних захтјева су повјерљивост, расположивост, интегритет, аутентификација, ауторизација те непорецивост. Прва три захтјева су основни безбједносни захтјеви.

- Повјерљивост или тајност осигурава да садржај информације буде приступачан само овлаштеним корисницима (корисницима којима је намијењена),
- Расположивост осигурава да информације буду на располагању овлаштеним корисницима,
- Интегритет осигурава да информације у систему могу мијењати само за то овлаштени корисници, односно осигурава непромјењивост података,
- Аутентификација је поступак провјере идентификације односно утврђивање вјеродостојности корисничког идентитета,
- Ауторизација је поступак који обухваћа аутентификацију и провјеру провјеру права приступа,
- Непорецивост представља заштиту од оповргавања, а то значи онемогућавање негирања претходно почињеног дијела од стране корисника.

Сви безбједносни захтјеви осим расположивости рјешавају криптовање.

Постоје три опште категорије криптографских алгоритама:

- Симетрични,
- Асиметрични,
- Хешинг (Hashing) алгоритми.

Сваки криптографски алгоритам има своје предности и своје недостатке. Неки системи користе комбинацију ових алгоритама и на тај начин искоришћавају њихове јаче стране. Такве криптографске системе називамо хибридним системима.

Симетрични алгоритми

Користе исти кључ и за шифровање и за дешифровање података. Еквивалентна имена за симетричне алгоритме су: цонвентионал, сецрет кеу, цлассицал и привате кеу алгоритам. Као што и само име говори, код оваквих алгоритама кључеви морају бити сакривени или тајни. Ако се деси да до кључа дођу стране које нису укључене у комуникацију, безбједност података је смањена или потпуно елиминисана. Другим ријечима, свако ко посједује тај дијељени тајни кључ има могућност читања (и писања) шифрованих порука.

Асиметрични алгоритми

За разлику од алгоритама са тајним кључем гдје се користи један дијељени кључ, асиметрични алгоритми користе два кључа. Један од кључева је јавни, а други приватни. Ови алгоритми се називају и алгоритми са јавним кључем, а њихов принцип рада је сљедећи: на основу тајног кључа који задаје прималац, генерише се јавни кључ. Јавни кључ се даје страни која шаље шифроване податке примаоцу. Помоћу њега, пошиљалац шифрира информацију коју жели да пошаље и такву шаље примаоцу. Кад шифрат стигне

примаоцу он га дешифрује помоћу свог тајног кључа. Значи, тајни кључ има само прималац, а јавни кључ може имати било ко, пошто се он користи само за шифровање, а не и за дешифровање. Предност овог начина шифровања је у томе што не постоји брига у случају да неко пресретне јавни кључ, јер помоћу њега може само да шифрује податке.

Хешинг (Hashing) алгоритми

Криптографске функције за сажимање - хеш (eng. hash) функције се сврставају у криптографске алгоритме без кључа. Hash function означава функцију која компресује низ података произвољне дужине у низ података фиксне дужине. Хеш функције се користе код заштите интегритета података и раде на сљедећем принципу; када нови податак пристигне он се хешира и онда се се пореди са хеш вриједности оригинала. Ако подаци нису корумпирани или измијењени вриједности ће бити идентичне, а ако су подаци били измијењени, хеш вриједности биће различите. Примјер коришћења hashing је провјера password-a између радне станице и сервера. Коришћењем ове технике информација никада не „путује“ кроз мрежу у облику отвореног текста, па нема опасности од пресретања.

5.1. Методологија енкрипције

С обзиром на податке који се криптују и на нивоу на којем се криптовање обавља, постоје различите врсте енкрипције које су примјенљиве у заштити система база података:

- Енкрипција за заштиту података током преноса (eng. data-in-motion),
- Енкрипција за заштиту података током мировања (eng. data-at-rest),
  - Енкрипција на нивоу програмског интерфејса, тј. енкрипција на нивоу апликације (eng. aplication - layer encryption), енкрипција на нивоу базе података (eng. database-layer-encryption),
  - Енкрипција фајла (eng. file-based encryption),
  - Транспарентна енкрипција.

У зависности од алата који се користи енкрипција је:

- Енкрипција на нивоу софтвера,
- Енкрипција на нивоу хардвера.

Софтверска енкрипција се користи да означи процес шифровања података у самом процесору, а ако се подаци шифрују помоћу хардвера прикључених на рачунар онда се ради о хардверској енкрипцији. Иако је хардверска енкрипција бржа у односу на софтверску енкрипцију, она може бити недоступна, па се стога користи софтверска енкрипција.

5.2. Дигитални потпис

Дигитални потпис мора имати сва особине личног потписа, а то су сљедеће особине:

- Лични потпис је аутентичан, а то значи да га може издати само потписник лично,
- Лични потпис могуће је провјерити поређењем с претходним потписима,
- Лични потпис изражава ауторство или слагање са садржајем документа и његов је неодвојиви дио,
- Лични потпис се неможе порећи.

Ове особине не значе да се лични потпис не може кривотворити, али постоје методе с којим се може с великом сигурношћу утврдити да ли је он кривотворен.

Документе у дигиталном облику лако је мијењати, а да би они имали правну или неку другу вриједност потребно им је осигурати аутентичност. Та аутентичност се осигурава дигиталним потписивањем документа. Дигитални потпис је у основи функција компресије дигиталног документа и приватног кључа потписника. Вјеродостојност потписаног документа се обавља употребом садржаја документа и јавног кључа потписника.

5.3. Дигитални цертификат

Дигитални сертификат је дигитално потписани документ који повезује јавни кључ с особом којој припада (власником јавног кључа). Уведен је из тог разлога што судионици у комуникацији, да би уопште могли комуницирати, морају на неки начин дознати кључеве својих партнера. Осим тога, морају бити увјерени да партнери нису особе који се лажно представљају. Сертификат се дигитално потписује из тог разлога што се осигурава његов интегритет, који гарантује потписник. Потписник дигиталног цертификата назива се сертификацијски центар (eng. Certification Authority - CA). Цертификацијски центар (ЦА) је тијело којој сви корисници сертификата вјерују и чији јавни кључ, који се користи за провјеру потписа на сертификату, мора бити поуздано исправан.

6. Политика приступа интернету

Коришћење Интернета у свакодневном пословању данас је нужност. Осим што доноси бројне предности, приступ Интернету доноси и бројне потенцијалне проблеме ако се правилно не надзире приступ непожељним или забрањеним страницама (вируси и други Malware), цурење информација, phishing и social engineering, смањење продуктивности…

Због разних пријетњи које “вребају” кориснике Интернета, у ФЗОРС све чешће се примјењују рјешења задужена за безбједност и надзор приступа Интернету. Таква рјешења морају задовољавати сљедеће функционалности:

- Анти-Вирус/Анти-Malware,

- Firewall,
- Надзор HTTPS саобраћаја,
- URL Filtering - ограничавање приступа појединим web страницама према категоријама (нпр. друштвене мреже, порнографија, коцкање и сл.),
- Надзор осталих Интернет апликација (chat, FTP, Torrent…),
- Управљање правима приступа и извјештавање о начину коришћења - по кориснику, добу дана, апликацији, садржају…,
- Превенција губитка ("цурења") информација - Data Loss Prevention.

Од рјешења за безбједност и надзор приступа Интернету данас се очекује да у себи имају већ уграђене основне политике, како би увођење у рад било што брже и једноставније. Редовно ажурирање Анти-Вирус, Анти-Malware и других дефиниција, као и базе непожељних URL-ова подразумијева се, док се данас све више траже напредније могућности, као што је надзор HTTPS (енкриптованог) саобраћаја, надзор садржаја који се измјењује путем WebMail-а, социјалних мрежа (Web 2.0), chat-апликација и сл., надзор Интернетског саобраћаја на мобилним уређајима,…

Осим експлицитних забрана које такви системи могу наметнути корисницима, могуће их је користити и као надзорне системе који само обавјештавају администраторе у случају сумњивих акција, односно помоћу система за извјештавање добити увид у начин коришћења Интернета од стране крајњих корисника.

<u>Напомена:</u> Ову политику у сажетом облику имате на крају овог документа као Прилог за кориснике.

7. Политика креденцијала за аутентикацију

Циљ ове политике је спријечити неовлаштени приступ информационим системима (ИС).

Потребно је успоставити процедуре за контролу додјеле права приступа ИС. Те процедуре требају обухватити све стадије у животном циклусу корисничког приступа, од почетне регистрације новог корисника до коначног одјављивања корисника којем више није потребан приступ систему и услугама.

7.1. Регистрација корисника

Мора постојати формална регистрација и одјава корисника ради добијања права приступа вишекорисничким ИС и сервисима.

Приступ треба контролисати кроз процес регистрације корисника, који укључује:

- Коришћење једноставних корисничких имена, како би се кориснике могло повезати с њиховим активностима и учините одговорне,

- Провјера овлашћења корисника за коришћење ИС или сервиса,
- Провјера да дозвољени ниво приступа одговара пословним потребама и да је у складу с политиком безбједности,
- Осигурање да даваоц услуге не дозволи приступ док није проведен ауторизацијски поступак,
- Одржавање пописа свих корисника регистрованих за коришћење сервиса,
- Тренутно укидање права корисника,
- Повремене провјере корисничких имена и рачуна.

7.2. Управљање привилегијама

Додјела и коришћење привилегија треба бити ограничена и строго контролисана.

Потребно је размотрити:

- Идентификовати привилегије и кориснике којима их треба додијелити,
- Привилегије треба додјељивати појединцима на темељу потреба и ситуација,
- Ниво привилегије мора бити минимална потребна за функционисање,
- Биљежење свих додијељених привилегија,
- Додјељивање привилегија под новим корисничким именом.

7.3. Управљање корисничким лозинкама

Расподјелу лозинки треба контролисати кроз формални процес управљања лозинкама који укључује:

- Захтијевати од корисника да потпишу изјаву у којој се обавезују да ће чувати лозинке повјерљивима,
- Захтијевати да се лозинке просљеђују корисницима на безбједан начин,
- Употребу електронске поште или треће стране треба избјегавати,
- Лозинке се не смију похрањивати на рачунару у незаштићеном облику.

Треба спријечити неовлашћени приступ корисника, повећати свијест корисника о властитој одговорности око коришћења лозинки и безбједности опреме коју користе.

Корисници се приликом употребе лозинки морају придржавати безбједносног упутства које је дефинисано политиком безбједности. Они морају бити свјесни да се лозинком потврђује њихов идентитет, омогућавајући тиме право приступа до јединица и сервиса за обраду података.

Корисници су дужни:

- Чувати повјерљивост лозинки,
- Не биљежити лозинке на папир,

- Лозинке се не смију одавати другим корисницима, чак ни администраторима, одговорним особама и сл.,
- Корисници не смију мијењати лозинке уколико сумњају на неправилности у раду сервиса (примјер phishing, социјални инжењеринг и сл.),
- Бирати квалитетне лозинке, дуге минимално 6 знакова, да нису везане уз имена, датуме, телефонске бројеве и сл.,
- Лозинке морају садржавати и бројеве и слова, ако је могуће и специјалне знакове,
- Избјегавати поновну употребу старих лозинки,
- Избјегавати лозинке које већ користе на другим системима,
- Редовно мијењати лозинке итд.

Осим одговорности над употребом лозинки, корисници су дужни на одговарајући начин заштитити опрему када нису у њезиној близини. Сви корисници морају бити свјесни својих одговорности над заштитом неосигуране опреме, које првенствено укључује:

- Корисници уколико се удаљавају од рачунара за вријеме радног времена, обавезно морају осигурати рачунар примјереним безбједносним механизмима (CTRL + ALT + DEL - Lock, screen saveri с лозинком и сл.),
- Приликом гашења рачунара нужно је одјавити се са система; не само угасити терминал или рачунар,
- Осигурати рачунар и терминале од неовлашћеног коришћења, посебно када нису у употреби.

<u>Напомена:</u> Ову политику у сажетом облику имате на крају овог документа као Прилог за кориснике.

8. Политика физичке безбједности

Циљ ове политике је спријечити неовлашћени приступ, наношење штете пословним просторијама и информацијама.

Критичне и осјетљиве пословне објекте за обраду информација треба поставити у безбједном подручју, заштићене према класификацији (осјетљивост и важности објекта који се штити). Физичка заштита подручја састоји се од ограђивања (најчешће зидовима и протупровалним - протупожарним вратима) и контролом приступа (ући могу само овлашћене особе, снимање просторија итд.).

8.1. Подручје физичке заштите

Безбједносне баријере попут зидова или картицом контролисани улази у просторије требају служити за заштиту оних дијелова ФЗОРС који садрже повјерљиве информације и опрему.

Сљедеће смјернице морају бити размотрене и по потреби имплементиране гдје постоји потреба за физичком заштитом:

- Безбједносна подручја морају бити строго означена; јачина и опсег заштите зависи о процјени ризика, вриједности и осјетљивости имовине које то подручје садржи,
- Контролним механизмима потребно је спријечити сваки покушај неовлашћеног приступа,
- Врата на улазима у заштићена подручја морају бити отпорна на пожаре, поплаве, пробијања итд.,
- Сви улази у заштићена подручја требају бити надгледана и снимана помоћу камера,
- Главни улази у безбједносна подручја морају имати чувара који контролише ко улази, шта се уноси, те по потреби може интервенисати,
- Сви контроли механизми морају бити периодично прегледавани како би се на вријеме уочили недостаци заштите или покушаји неовлашћеног приступа итд.

8.2. Физичка контрола уласка

Безбједносна подручја морају бити заштићена одговарајућим контролама уласка како би се осигурало да могућност уласка имају само овлашћене особе.

Потребно је проучити сљедеће ставке:

- Датум и вријеме уласка и одлазак особе мора бити забиљежен,
- Све активности корисника морају бити надгледане, осим уколико посебним одредницама није другачије дефинисано,
- Приступ безбједносним подручјима требају имати само овлашћене особе чији рад зависи о опреми и информацијама из тог подручја,
- Приступ подручјима треба бити дефинисан према подручјима, а не према „класификацији“ запосленог,
- Права приступа требају бити периодично прегледавана и ажурирана.

8.3. Безбједност опреме

Циљ је спријечити губитке, штету или компромитовање имовине и прекид пословних активности.

Опрема треба бити заштићена од пријетњи и опасности из околине. Заштита опреме је неопходна како би се смањио ризик неовлашћеног приступа подацима, те како не би дошло до губљења и оштећења имовине.

8.4. Смјештај и заштита опреме

Сљедеће смјернице треба узети у обзир при заштити опреме:

- Опрема мора бити смјештена тако да је непотребни приступ опреми минималан,
- Јединице за обраду података морају бити смјештене тако да је смањена могућност проматрања неовлашћеним корисницима (на примјер, постављање монитора под таквим углом да само особа за рачунаром види слику),
- Контроле је потребно имплементирти тако да минимализирају ризик од потенцијалних пријетњи, примјер: крађа, пожар, дим, вода, вибрације, радијације итд.,
- Да ли је допуштено јести, пити, пушити у близини опреме,
- Услови окружја (температура, влага) који могу утицати на рад јединица за обраду информација, требају бити под надзором,
- Не дозвољавати складиштење друге опреме или материјалакоји не припадају ИТ инфраструктури.

8.5. Безбједност инсталација

Јединице за обраду података морају бити заштићене од грешака које могу настати нестанком електричне енергије, поплавама из водоводних инсталација, одводом отпадних вода, грijањем/хлађењем итд. Све наведене инсталације морају бити правовремено прегледане и тестиране како би се на вријеме уочиле и исправиле грешке у раду.

Јединице за непрестано напајање (УПС - eng. uninterruptible power supply) неопходне су у случају нестанка електричне енергије. Такве јединице временски врло кратко могу напајати јединице за обраду података, поготово уколико је систем велики. Зато је важно размотрити уградњу генератора чија је могућност напајања далеко већа од обичних јединица за непрестано напајање.

Нестанак електричне енергије, поплаву, пожар или било коју другу пријетњу битно је алармирати звучним и свјетлосним сигналима како би се правовремено подузеле прописане акције у случају незгоде. Опскрба водом мора бити редовно контролисана како исправност уређаја за гашење пожара не би била упитна. Телекомуникацијска опрема мора бити инсталирана на начин да евентуалан прекид везе не утиче на комплетан прекид комуникације.

8.6. Безбједност код каблирања

Каблови за напајање електричном енергијом и телекомуникацијски каблови морају бити адекватно заштићени од оштећења, прекида или прикључења неовлашћених корисника на мрежу.

Прије каблирања мора бити размотрено сљедеће:

- Каблови за напајање јединица за обраду података, уколико је могуће, морају бити положени подземно; алтернатива је адекватна физичка заштита,
- Исто вриједи и за телекомуникацијске каблове,

- Каблови за напајање морају бити раздвојени од телекомуникацијских како би се избјегле сметње,
- Означавање каблова посебним идентификацијским ознакама спријечити ће грешке у спајању, такође ознаке је потребно документовати.

8.7. Одржавање опреме

Одржавање опреме треба бити редовно и обављено од стране стручњака како би се осигурала исправност, тј. непрекидни рад.

При одржавању опреме треба се придржавати сљедећег:

- Одржавање опреме мора бити у складу с препорукама произвођача, у одређеним временским интервалима и по заданим спецификацијама,
- Само овлаштене особе смију сервисирати опрему,
- Прије сервисирања опреме потребно је имплементирати одговарајуће безбједносне контроле уколико за тим постоји потреба, те је потребно обрисати повјерљиве информације (потребе за овакви мјерама настају уколико сервисирање извршавају ванјски партнери или трећа страна).

8.8. Примјена норме у безбједносној политици

Због великог броја људи који користе ресурсе ФЗОРС и релативно лаког приступа појединаца просторијама ФЗОРС политика физичке заштите овдје је врло битна. Како би се спријечиле незаконите радње злонамјерних корисника, али и случајне погрешке радника, приступ просторијама које садрже осјетљиву опрему (сервер, базе података и сл.) мора бит строго контролисан. Нужно је омогућити приступ искључиво овлаштеним особама који за приступом имају потребу због природе обављања посла. Свим осталим корисницима приступ мора бити строго забрањен. Осим просторија велика пажња мора се посветити безбједности каблова. Сви каблови (напајање, комуникацијски и сл.) морају бити физички заштићени и одвојени од неовлаштених корисника. Сву опрему коју физички није могуће смјестити у „безбједне“ просторије мора бити заштићена од неовлаштених корисника на начин да се постави у безбједносне ормариће. Посебну пажњу треба посветити одржавању опреме, те контролисању да ли постоји назнаке злонамјерних радњи – оштећење, крађа, мијењање опреме и сл.

8.9. Административне и безбједносне зоне

За физичку заштиту утврђене су двије врсте физички заштићених подручја:

- Административне зоне,
- Безбједносне зоне.

8.9.1. Административне зоне

- Административна зона 1. (Сервер сала) - Сви појединци стално имају пратњу и подлијежу додатним контролама, а који нису овлаштене особе који припадају Сектору за ИТ ФЗОРС,
- Административна зона 2. (Пасивна и активна опрема) - Приступ са или без пратње одобрава се само појединцима које је прописно од стране Сектора за ИТ,
- Административна зона 3. (Персонални рачунар, преносни рачунар, мобилни уређаји...) - Приступ без пратње одобрава се само појединцима који су прошли безбједносну провјеру и који су посебно овлаштени за улазак у подручје на темељу нужности приступа подацима.

8.9.2. Безбједносне зоне

- Безбједносна зона 1. (Сервер сала) - Сви појединци стално имају пратњу и подлијежу додатним контролама, а који нису овлаштене особе који припадају Сектору за ИТ ФЗОРС,
- Безбједносна зона 2. (Објекти и просторије) - Успоставља се правило кроз који се надзиру сви уласци и изласци помоћу система препознавања особа,
- Безбједносна зона 3. (Подручје изван објеката, улази, паркинг...) - Успоставља се правило које омогућује провјеру појединаца, а ако је могуће и возила.

9. Политика удаљеног приступа

Врло често се налазимо у ситуацији када нам је потребно да приступимо удаљеном рачунару корисника мреже ФЗОРС коме је потребна помоћ или асистенција, а због чињенице да сте се једноставно налазили предалеко то нисмо могли. Да би рјешили проблем географске удаљености и немогућности да физички будемо за жељеним рачунаром користе се различити програми и сервиси за удаљени приступ и управљање рачунарима.

Ти алати морају бити дизајнирани да раде преко LAN-а, WAN-а или интернета, без потребе за подешавањем фиревалл-а, а такође је потребно да посједује комплетно рјешење за удаљено управљање и подршку.

Окружење:

- Повезивање преко TCP/IP протокола,
- Комуникација преко ЛАН-а, WAH-а, интернета, ISDN-а или мобилне мреже,
- Подршка за различите оперативне системе,
- Једноставна комуникација између рачунара.

Удаљена контрола:

- Надгледање, контрола екрана, тастатуре и миша радне станице, без обзира на резолуцију, мрежни протокол или оперативни систем,
- Оптимизовање квалитета слике када се контролише радна станица преко споре конекције,
- Интерактивни преглед свих повезаних радних станица,
- Удаљена контрола више система одједном или прелазак са једне радне станице на другу,
- Могућност дијељења контроле корисницима,
- Текстуална и аудио комуникација између два или више рачунара,
- Смањење екрана.

Алати за подршку:

- Подржава пренос датотека (File Transfer),
- Нуди могућност цхат-а и аудио комуникације,
- Удаљено покретање команди,
- Удаљено искључивање, поновно покретање и логовање/одлоговање на клијентском рачунару,
- Подршка за експорт/импорт адресара софтвера за удаљени приступ,
- Подршка за конфигурацију привилегија и администрацију софтвера за удаљену контролу,
- Праћење и прављење логова удаљених конекција.

Безбједност:

- Интеграција са Active Directory-m,
- Коришћења заштите удаљене контроле (најмање са 256-битном) енкрипцијом.

10. Безбједносна политика сервера

Заштита сервера један је од најбитнијих изазова у данашњем ИТ-у. Администратори морају одређивати и проводити безбједоносна правила која пружају робусну заштиту, а истовремено су довољно флексибилна да подржавају потребе повезивости све већег броја интерних и екстерних корисника, разних уређаја, конфигурација система и врста мрежних веза.

У зависности од локације, безбједносне пријетње могу бити сљедеће:

- Неовлашћен приступ повјерљивим подацима,
- Губљење или уништавање података,

- Злонамјерне измјене података,
- Софтверске грешке,
- Проблеми у раду апликација,
- Проблеми у раду база података,
- Проблеми у раду ОС сервера.

Шта је све потребно имати, и који су то предуслови за безбједан рад сервера:

- Сервер сала,
- Ормар (рек),
- Извор континуираног напајања (УПС, генератори),
- Извор континуираног хлађења (климатизација),
- Систем противпожарне дојаве и заштите.

Заштита на нивоу хардвера:

- Редундација различитих компоненти сервера (напајања, дискова, процесора, меморије, интерфејса ...),
- Стораге систем дискова и траке за бацкуп (система, база, апликација, фајлова...),
- Disaster recovery систем на удаљеној локацији.

Безбједност на нивоу софтвера:

- Backup (оперативних система, база, апликација, фајлова...),
- Редовно ажурирање ОС са безбједоносним печевима, односно закрпама,
- Забрана коришћења неауторизованог и непровјереног софтвера,
- АВ заштита,
- "Пуштање" само неопходних сервиса.

11. Безбједносна политика мрежних уређаја

Класификација мрежних уређаја врши се искључиво на основу нивоа на којима ти уређаји функционишу, односно пакете ког протокола контролишу и на ком слоју врше преглед њиховог заглавља. На основу тога планира се и безбједосна политика мрежних уређаја.

Најважнији механизми превенције напада на уређаје другог слоја је правилно конфигурисање портова за одређену врсту филтрирања. Одговарајућа промјена мода у коме се порт налази.

Напредније технике подразумијевају постављање додатних безбједносних механизама.

Први је постављање филтера да би се обезбиједило приступање порту са одређеном MAC адресом.

Друга опција је да се одреди максималан број физичких адреса које се могу додијелити порту. Обавезна употреба листи за контролу приступа (ACL). Употреба криптографских алгоритама, сертификата и других механизама шифровања порука.
Ограничавање приступа неовлашћеним особама у просторије гдје се налази мрежна опрема. Правилно конфигурисање и руковање мрежном опремом. Чување лозинки које се налазе на мрежним уређајима. Честе промјене лозинки.

12. ДМЗ политика

За управљање ДМЗ-ом треба дефинисати не само ДМЗ елементе, већ и уређаје који ће се налазити у ДМЗ, стандарде и захтјеве за све уређаје, конекције и саобраћај који се односи на ДМЗ, као и на слојеве статичке конфигурације firewall-а и мрежног саобраћаја кроз firewall. Због комплексности типичног ДМЗ окружења, типично је потребно дефинисати три шира стандарда за све што је везано за ДМЗ:

- Одговорности власника,
- Захтјеве за безбједносним конфигурисањем,
- Функционалне захтјеве и захтјеве за контролом промјена.

12.1. Одговорност власника

ДМЗ је вјероватно најкомплекснији мрежни сегмент у цјелој LAN (WAN) мрежи. Због тога је критично дефинисати не само улогу - ко је одговоран за неки систем или апликацију, већ и које су му одговорности. Кључни захтјеви укључују сљедеће:

- Комплетну документацију о ресурсима у систему управљања,
- Одговарајуће називе за све адресибилне мрежне интерфејсе,
- Тренутан приступ систему у складу са политиком надзора,
- Потпуно слагање са политиком управљања и контролом промјена,
- 24/7 листу особа за контакт у случају да се систему мора приступити ван радног времена.

12.2. Захтјеви за безбједносним конфигурисањем

ДМЗ мора бити безбједнији од било ког другог система у интерној мрежи, зато што ДМЗ систем може дозволити непознатом кориснику приступ ресурсима. Због тога је потребно дефинисати сљедеће конфигурационе захтјеве:

- Сви системи се морају редовно ажурирати са новим безбједносним закрпама,
- Сви системи и све апликације морају бити одобрене од одјељења за заштиту,

- Сав непотребан софтвер и сервиси морају бити или деинсталирани или искључени ако је могуће,
- Приступ сервисима мора бити ограничен кроз логичку контролу приступа употребом ACL/ACM и прокси сервера гдје год је то могуће,
- Све удаљене администрације морају се обављати преко безбједних канала,
- Сви системи се морају надгледати и сви догађаји морају бити уписани у одговарајуће логове,
- Треба забранити администрацију са спољашње стране (Интернета),
- Све везе између дистрибуираних система биће одобрене само, ако за то постоји валидан пословни разлог и ако не постоји другачије рјешење.

12.3. Функционални захтеви и захтеви за контролом промјена

Операционални, функционални захтјеви дефинишу шта се мора урадити сваког дана у циљу одржавања система. Кључан елемент операционалних захтјева је да се обезбједи да сви системи буду у складу са политиком управљања промјенама и да све промјене конфигурација морају бити ауторизоване од стране сектора за ИТ.

13. VPN политика

Виртуелне приватне мреже (VPN) засноване на технологији Интернета користе се у случајевима када је потребно повезати више удаљених рачунарских мрежа. При томе подаци пролазе виртуелним „тунелом“ кроз Интернет. VPN се најчешће интегрише у склопу firewall-a, те тако на једном мјесту уједињава заштиту мреже од спољњих упада и заштиту података који иду кроз тунел.

Безбједност је један од основних захтјева за VPN мреже. Њу угрожава велики број напада, који се могу сврстати у већи број група као што су:

- Напади аутентификације,
- Криптографски напади,
- Напади интегритета,
- Фалсификовање сервера,
- Фалсификовање пакета,
- Напади ускраћивања услуга,
- Пасивни мониторинг.

Постоји много разлога за увођење корпоративне VPN мреже. Неки од најзначајнијих свакако су:

- VPN мрежа омогућује приступ ресурсима ФЗОРС, што је основни предуслов за развој интерне мреже (Интранет) и даљинског приступа. На овај начин ФЗОРС је у могућности да себи, тако и здравсвеним установама пружи сет апликација и сервиса

чиме ће се значајно допринјети повећању продуктивности и побољшању односа са клијентима, партнерима и добављачима,
- VPN мрежа обезбјеђује највиши ниво безбједности података, што омогућава несметан пренос осјетљивих података преко Интернета, или кроз потпуно приватну IP мрежу, при чему само ауторизовани корисници има право приступа,
- Осим тога, VPN мрежа представља мудро и економски исплативо рјешење. Обезбјеђује једнак ниво безбједности као изнајмљивање посебне приватне линије, уз знатно ниже трошкове.

VPN технологија мора осигурати ове захтјеве:

- Управљање IP адресама - VPN је задужен за додјељивање клијентских адреса унутар приватне мреже,
- Механизми управљања кључевима - VPN мора осигурати генерисање и освјежавање кључева између клијента и сервера,
- Подршку за разне протоколе - VPN мора подржавати стандардне протоколе који се користе у јавним мрежама (IP, IPX,...).

Врло су важни и безбједносни захтјеви:

- Право приступа - VPN осигурава провјеру идентитета корисника и допушта VPN приступ само регистрованим корисницима. Такође, мора осигурати могућност праћења догађаја (engl. logging),
- Аутентикација и ауторизација - VPN мора осигурати провјеру да подаци који долазе стварно долазе с извориштa с којег тврде да долазе и да особа која тврди да је пошиљалац података то стварно и јесте,
- Интегритет података - VPN мора осигурати провјеру јесу ли подаци путем промјењени. За то се најчешће користи MD5 алгоритам,
- Повјерљивост (тајност, криптировања) - VPN мора осигурати криптовање података тако да их нико, осим клијента односно сервера не може прочитати. То се постиже разним алгоритмима, а неки од њих су DES, RSA, Diffie-Hellman...

Врсте VPN мрежа су:

- Интранет VPN - Користи се за повезивање више локација унутар једне организације. За пренос података се користи интернет,
- Екстранет VPN - Користи се за повезивање различитих организација (нпр. фирме и пословних партнера). За пренос података се користи интернет,
- Удаљени приступ - Повезује удаљене кориснике с локалном мрежом ФЗОРС.

VPN се може подјелити по типу тунеловања који користи:

- Стални - Траже одређену појасну ширину чак и када се канал не користи па нису финансијски исплативи,
- Привремени - Успостављају се када клијент затражи спајање на VPN и нестају када се веза прекине.

14. Екстранет политика

14.1. Изолација

Уз помоћ firewall опреме одржавати три зоне:

- Приватну,
- Јавну,
- ДМЗ зону.

Циљ ове стратегије је изоловати системе са различитим безбједносним нивоима приступа од стране јавне мреже. Увијек водити рачуна да је екстранет мрежи дозвољен приступ само одобреном сету информација.

14.2. Јака аутентификација

Кључна компонента екстранет политике је јака аутентификација. Гдје је могуће пожељно је користити двоструку аутентификацију или дигиталне сертификате.

14.3. Контрола нивоа приступа

Администратори морају креирати ACL како би се сваком екстранет клијенту ограничио приступ само дозвољеним ресурсима.

14.4. Енкрипција

Обавезно коришћење VPN технологије која обезбјеђује јаку енкрипцију података који се преносе несигурном мрежом. VPN рјешење и алгоритам за енкрипцију одређују одговорни у ИТ сектору.

15. Безбједносна политика бежичне комуникације и мобилних уређаја

Циљ ове политике је забрана приступа приватној мрежи ФЗОРС путем несигурних механизама бежичне комуникације. Само бежични системи који задовољавају критеријуме дефинисане овом политиком или су одобрени од стране одговорних из ИТ сектора, имају право успостављања бежичне конекције на мрежу ФЗОРС.

Све бежичне приступне тачке повезане на приватну мрежу ФЗОРС морају бити регистроване и одобрене од стране одговорних из ИТ сектора.Ове приступне тачке су предмет периодичних тестова пенетрације, провјера рањивости и морају укључивати снажне механзме аутентификације.

Сви рачунари који користе бежични приступ морају користити VPN тунел и морају поштовати правила дефинисана у склопу "Политике удаљеног приступа".

Сви уређаји који користе бежични приступ морају подржавати хардверско адресирање (нпр. MAC адреса) путем којег је уређаје могуће регистровати и пратити.

SSID - Сервисни идентификатор приступне тачке – ће бити конфигурисан тако да не садржи информације помоћу којих је могуће идентификовати ФЗОРС.

ИТ сектор је одговоран за креирање процедура и конфигурације приступних тачака, пружање подршке и савјета, те верификацију приступних тачака.

16. Безбједоносна политика радних станица

Циљ ове политике је дефинисање стандарда који морају бити поштовани при инсталацији радних станица које су у валсништву ФЗОРС, те да допринесе непрекидном раду сервиса и рачунарске опреме ФЗОРС.

Лозинке за приступ уређајима морају бити дефинисане и одржаване у складу са поглављем "Политика контроле приступа".

Анти-вирусне политике морају бити у складу са поглављем "Анти-вирус политика".

Све радне станице и лаптоп рачунари требају имати подешен screensaver (лозинком заштићен) који се активира максимално након 5 минута неактивности. Алтернатива овом је обавезна одјава са система или закључавање приступа.

Преносиве медије, USB меморије и др. потребно је увијек скенирати прије њихове употребе.

Коришћење преносивих медија, USB меморија, CD/DVD-RW, или других меморија за физички пренос података мора бити одобрено од стране одговорних у ИТ сектору.

Сервиси и апликације чије функционисање није неопходно не требају се инсталирати или морају бити искључени. Несигурни сервиси и протоколи морају бити замијењени безбиједним еквивалентима, кад год они постоје.

За сваку радну станицу потребно је документовати локацију и особу за контакт, основне хардверске карактеристике, верзију оперативног система, основне функције и апликације.

Сви догадјаји везани за безбједност морају бити логовани и пријављени одговорнима у ИТ сектору, који ће на основу тога преузети одговарајуће кораке.

Посљедње безбједносне закрпе морају у што краћем року бити инсталиране на систем. Посљедње безбједносне закрпе не морају бити инсталиране у случају када би то изазвало проблеме у функционисању сервиса или апликација који су у продукцији.

Потребно је увијек користити принцип "најмањег потребног права приступа" за обављање било које функције. Не користити root или администраторски налог, ако се операција може извршити помоћу непривилегованог налога.

Ако је технички изводљиво, за удаљени и привилеговани приступ морају се користити безбједни канали.

Хардвер, руковање и начин употребе хардвера, оперативни систем, сервиси и апликације морају бити одобрени од стране одговорних из ИТ сектора.

Све измјене конфигурације радних станица које су у продукцији морају бити у складу са овим документом.

<u>Напомена:</u> Ову политику у сажетом облику имате на крају овог документа као Прилог за кориснике.

17. Безбједносна политика провјере рањивости

Правовремено проналажење рањивости значи да се оне могу анализирати и уклонити. Редовне провјере овог типа смањују могућност успјешног напада и компромитације података извана или изнутра.

Провјера рањивости мора укључивати преглед свих сегмената ИТ система (радне станице, мрежна опрема, мрежни штампачи, оперативни системи, web апликације) и проналажење рањивости у било којем дијелу система.

Сам поступак провјере рањивости, односно скенирања мреже, проводи се помоћу одговарајућег алата који бирају одговорни из ИТ сектора уз писану сагласност генералног директора. Након скенирања мреже обавља се анализа добијенх резултата након чега се генерише извјештај који садржи цијели низ информација о пронађеним рањивостима, те начинима њиховог уклањања.

Одговорни из ИТ сектора такође дефинишу колико често је потребно вршити провјеру рањивости.

18. Политика одговора на безбједносне инциденте

18.1. Пријаве инцидента

Сваки запосленик дужан је пријавити безбједносне инциденте попут успореног рада сервиса, немогућности приступа, губитка или неовлашћене измјене података, појаве вируса и сл.

Одговорна лица би требало да израде и одржавају контакт листу особа којима се јављају проблеми у раду рачунара и сервиса као и образац за пријаву инцидента.

Сваки инцидент се документује. Уз образац за пријаву инцидента, документација садржи и образац са описом инцидента и подузетих мјера при рјешавању проблема.

Извјештаји о инцидентима сматрају се повјерљивим документима, спремају се на безбједно мјесто и чувају као би могли послужити за статистичке обраде којима је циљ установити најчешће пропусте ради њиховог спречавања али исто тако и као доказни материјал у случају већих безбједносних пропуста.

18.2. Процедуре за рјешавање инцидента

Администартори смију пратити корисничке процесе. Ако постоји сумња да се рачунар користи на недозвољен начин може се излистати садржај корисничког директорија, али не смије се провјеравати садржај корисничких докумената, e-mailova и сл.

У случају озбиљнијег безбједносног инцидента поштују се сљедећа правила:

- Истрагу спроводе двије одговорне особе,
- Информациони систем на коме је дошло до безбједносног инцидента потребно је сачувати у затеченом стању тј. потребно је спријечити измјене које би отежале или онемогућиле да се утврди узрок инцидента,
- Направити копију затеченог стања,
- Документовати сваки корак и на крају написати извјештај о безбједносном инциденту,
- Извештаји о инцидентима сматрају се повјерљивим документима и чувају се на тај начин да им приступају само овлаштене особе.

<u>Напомена:</u> Ову политику у сажетом облику имате на крају овог документа као Прилог за кориснике.

19. Безбједоносна политика мобилних уређаја

Било који мобилни уређај који се користи за приступ пословним подацима, на пословну имрежу мора бити спојен VPN тунелом. Свака особа, апликација и уређај који се повезује на пословну мрежу мора се аутентификовати као корисник чији је приступ одобрен од стране одговорних у ИТ сектору.

Корисници мобилних уређаја не могу приступити повјерљивим и осјетљивим подацима.

Одговорни из ИТ сектора имају овлаштење да погледају, модификују, направе резервне копије и по потреби обришу пословне податке са мобилних уређаја.

Одговарајући антивирусни софtwаре мора бити инсталиран на свим мобилним уређајима који приступају пословној мрежи.

Како би се смањила могућност да се угрозе приватни подаци корисника мобилних уређаја потребно је строго одвојити приватне од пословних података.

<u>Напомена:</u> Ову политику у сажетом облику имате на крају овог документа као Прилог за кориснике.

20. Безбједоносна Анти-Вирус политика

Циљ ове политике је заштитити интегритет софтвера и информација.

Мјере заштите потребне су како би се спријечила и на вријеме уочила употреба малициозног софтвера. Софтвер и објекти за обраду информација су рањиви, и као такве треба их заштитити од злоћудних софтвера као што су вируси, мрежни црви, логичке бомбе итд. Кориснике треба упознати с опасностима употребе неодобреног или злоћудног софтвера а администратори би требали, уколико постоје могућности, подстаћи имплементацију контрола које детектују и спрјечавају употребу таквог софтвера.

20.1. Контроле против малициозног софтвера

Циљ је имплементирати контролне механизме који превентивно дјелују на пријетње малициозног софтвера и развити процедуре које осигуравају свјесност корисника.

Сљедеће контролне механизме потребно је узети у обзир:

- Формална политика која захтјева у складу са софтверским лиценцама и која забрањује употребу неауторизованог софтвера,
- Мора бити успостављена формална политика која се односи на ризике везане уз набавку софтвера и датотека с ванjских мрежа или с неког другог медија. У тој политици треба бити назначено које је заштитне мјере потребно подузети,
- Потребна је инсталација и редовно ажурирање антивирусних програма,

- Потребно је редовно проводити провјеру софтвера и података који подржавају критичне пословне процесе. Постојање било каквих неодобрених датотека мора се формално истражити,
- Провјера на злоћудни софтвер свих датотека на електронским медијима несигурног или неауторизованог поријекла,
- Провјера на злоћудни софтвер свих датотека набављених преко несигурних мрежа,
- Провјера на злоћудни софтвер свих e-mail додатака (фајлова у atachment-u),
- План опоравка и континуалног пословања у случају напада малициозног софтвера,
- Израда безбједносних копија свих неопходних података.

Прилог за кориснике

Прилог за кориснике је осмишљен као кратак водич Политике ФЗОРС за раднике ФЗОРС и њихово упознавање са безбједносним политикама. За детаљније информисање потребно је прочитати цијели документ.

Политика класификације информација односно података

Класификација се обично проводи с обзиром на постављене критеријуме (вриједност саме информације, утицај времена на њену вриједност, повезаност с појединим особама итд.). У већини организација, па тако и у ФЗОРС уопштено је прикладан сљедећи систем класификације:

- Јавне (Информације чије откривање не представља никакав потенцијални ризик за ФЗОРС),
- Осјетљиве (Захтијевају већи ниво надзора јер њихово откривање или губитак интегритета могу изазвати одређене губитке, који не морају бити изворно материјалне природе),
- Повјерљиве (Намијењене су само употреби унутар ФЗОРС. Њихово откривање може имати негативан утицај на организацију или њене запослене.),
- Тајне (Односе се на најосјетљивије податке и било какве неовлашћене активности везане уз њих могу довести до врло озбиљних посљедица за организацију.).

Политика контроле приступа

Контрола приступа има задатак заштити систем у максималној мјери од непажљивих корисника и злонамјерних особа. Непажљиви корисници сматрају се они који на било који начин, не придржавајући се политике безбједности, несвјесно помажу хакерима у злонамјерним радњама.

Како би се заштитили од непажљивих корисника потребно је имплементирати безбједносне контроле као што су:

- Аутоматска одјава са система уколико је рачунар неактиван 15 мин,
- Аутоматска одјава са система уколико је терминал неактиван 3 мин,
- Блокирање корисничког налога уколико се 3 пута узастопно унесе криво корисничко име и лозинка,
- „Присиљавање“ корисника на редовно мијењање лозинке, сваких 40 - 180 дана,
- Допуштање бирање само лозинки које задовољавају правила безбједносне политике итд.

Осим „техничких“ контрола безбједности, кориснике је потребно упознати с њиховим дужностима и одговорностима, те наведено документовати потписивањем Уговора о придржавању безбједосних правила.

E-mail политика

Корисници се обавезују на придржавање одређених правила:

- Запосленицима се отвара кориснички рачун ради обављања посла,
- Приватне поруке дозвољене су у умјереној количини, уколико то не омета рад,
- Пишући поруке, будите свјесни да не представљате само себе, већ и ФЗОРС за коју радите,
- Придржавајте се етике, правила пристојног понашања на Интернету, службену e-mail адресу немојте користити за слање увредљивих, омаловажавајућих порука, или за сексуално узнемиравање,
- Није дозвољено слање ланчаних порука којима се оптерећују мрежни ресурси и људима одузима радно вријеме,
- Свака написана порука сматра се документом, те на тај начин подлијеже прописима о ауторском праву и интелектуалном власништву. Немате право поруке коју су послане вама лично прослиједити даље без дозволе аутора, односно пошиљаоца,
- Све поруке прегледаће аутоматски апликација која открива вирусе. Ако порука задржи вирус, неће бити испоручена, а пошиљаоц и примаоц ће бити о томе обавијештени. Порука ће провести одређено вријеме у карантину. Након одређеног времена, обично мјесец дана, порука се брише из карантина како би се ослободио простор на диску,
- ФЗОРС задржава право филтрирања порука с намјером да се заустави spam,
- У случају истраге узроковане могућим безбједносним инцидентом, безбједносни тим може прегледати комплетан садржај диска, па тиме и e-mail поруке,
- Поруке које су дио пословног процеса треба архивирати и чувати прописани временски период као и документе на папиру,
- Ланчане поруке које људи шаљу познаницима могу садржавати лажне информације или бити дио преваре, с намјером да се корисницима извуче новац ("помозите болеснику којем треба операција", "отворите рачун како би избјегли предсједник могао извући новац из нестабилне афричке државе"...). Овакве поруке треба игнорисати и брисати из mail клијента.

Политика приступа интернету

Због разних пријетњи које “вребају” кориснике Интернета, у ФЗОРС морају задовољавати сљедеће функционалности:

- Анти-Вирус/Анти-Malware,
- Firewall,
- Надзор HTTPS саобраћаја,

- URL Filtering - ограничавање приступа појединим web страницама према категоријама (нпр. друштвене мреже, порнографија, коцкање и сл.),
- Надзор осталих Интернет апликација (Chat, FTP, Torrent…),
- Управљање правима приступа и извјештавање о начину коришћења - по кориснику, добу дана, апликацији, садржају…,
- Превенција губитка ("цурења") информација - Data Loss Prevention.

Политика креденцијала за аутентикацију

Циљ ове политике је спријечити неовлашћени приступ информационим системима (ИС).

Корисници су дужни:

- Чувати повјерљивост лозинки,
- Не биљежити лозинке на папир,
- Лозинке се не смију одавати другим корисницима, чак ни администраторима, одговорним особама и сл.,
- Корисници не смију мијењати лозинке уколико сумњају на неправилности у раду сервиса (примјер phishing, социјални инжењеринг и сл.),
- Бирати квалитетне лозинке, дуге минимално 6 знакова, да нису везане уз имена, датуме, телефонске бројеве и сл.,
- Лозинке морају садржавати и бројеве и слова, ако је могуће и специјалне знакове,
- Избјегавати поновну употребу старих лозинки,
- Избјегавати лозинке које већ користе на другим системима,
- Редовно мијењати лозинке итд.

Осим одговорности над употребом лозинки, корисници су дужни на одговарајући начин заштитити опрему када нису у њезиној близини. Сви корисници морају бити свјесни својих одговорности над заштитом неосигуране опреме, које првенствено укључује:

- Корисници уколико се удаљавају од рачунара за вријеме радног времена, обавезно морају осигурати рачунар примјереним безбједносним механизмима (CTRL + ALT + DEL - Lock, screen saveri с лозинком и сл.),
- Приликом гашења рачунара нужно је одјавити се са система; не само угасити терминал или рачунар,
- Осигурају рачунар и терминале од неовлаштеног кориштења, посебно када нису у употреби.

Безбједоносна политика радних станица

Све радне станице и лаптоп рачунари требају имати подешен screensaver (лозинком заштићен) који се активира максимално након 5 минута неактивности. Алтернатива овом је обавезна одјава са система или закључавање приступа.

Преносиве медије, USB меморије и др. потребно је увијек скенирати прије њихове употребе.

Коришћење преносивих медија, USB меморија, CD/DVD-RW, или других меморија за физички пренос података мора бити одобрено од стране одговорних у ИТ сектору.

Сервиси и апликације чије функционисање није неопходно не требају се инсталирати или морају бити искључени. Несигурни сервиси и протоколи морају бити замијењени безбиједним еквивалентима, кад год они постоје.

Хардвер, руковање и начин употребе хардвера, оперативни систем, сервиси и апликације морају бити одобрени од стране одговорних из ИТ сектора.

Политика одговора на безбједносне инциденте

Сваки запосленик дужан је пријавити безбједносне инциденте попут успореног рада сервиса, немогућности приступа, губитка или неовлашћене измјене података, појаве вируса и сл.

Администратори смију пратити корисничке процесе. Ако постоји сумња да се рачунар користи на недозвољен начин може се излистати садржај корисничког директорија, али не смије се провјеравати садржај корисничких докумената, e-mailova и сл.

Безбједоносна политика мобилних уређаја

Свака особа, апликација и уређај који се повезује на пословну мрежу мора се аутентификовати као корисник чији је приступ одобрен од стране одговорних у ИТ сектору.

Корисници мобилних уређаја не могу приступити повјерљивим и осјетљивим подацима.

Одговорни из ИТ сектора имају овлаштење да погледају, модификују, направе резервне копије и по потреби обришу пословне податке са мобилних уређаја.

Одговарајући антивирусни софтвер мора бити инсталиран на свим мобилним уређајима који приступају пословној мрежи.

Како би се смањила могућност да се угрозе приватни подаци корисника мобилних уређаја потребно строго одвојити приватне од пословних података.