Предлог за заштита на податоци, безбедност на информации и права на пристап

(Името на овој документ е: „Предлог за заштита на податоци, безбедност на информации и права на пристап_Конечна_2020“, користениот фонт на текст е Arial 11, единечен проред, 6 pt пред и потоа)

Миодраг Перишиќ, МСЕЕ, ИКТ експерт, проект „Поддршка на реформите во правосудниот сектор“

Скопје, јуни 2020 г.

Финансирано од Европската Унија

Владимир Полежиновски, 22/12, Скопје,
Република Северна Македонија
Тим лидер д-рДевил: +389 (0) 70 224044
Е-пошта: deville@planet.gr

Проектот го реализира NIRAS и партнерот во конзорциумот Planet

Table of Contents

Кратенки:....3
Извршно резиме....4
1. Дефиниција и вовед....4
Резултати од испитувањето на мислењата на обуката за ИКТ „Отворен простор“....4
2.Елементи на политиката за безбедност на информациите....5
2.1 Цел....5
2.2 Опсег....5
2.3 Цели на безбедноста на информациите....5
2.4 Политика за контрола на овластувања и пристап....6
2.5 Класификација на податоци....8
2.6 Поддршка и работење со податоци....9
....11
2.7 Обуки за подигнување на свесноста за безбедноста....11
2.8 Обврски, права и должности на персоналот....11
2.9 Упатување на релевантното законодавство во Северна Македонија....12
2.10 Други точки што би можеле да бидат опфатени со ПБИ:....12
3. Заклучок (важноста на ПБИ)....13
4. Општи предлози за правосудните институции во Северна Македонија....13
5. Кибер-безбедност....13
6. Права на пристап....14
Судови:....14
Обвинителство: 15
7. Акциски план....15
Список со референци....17

Кратенки:

ИКТ	Информатичко-комуникациска технологија
ЈО	Јавно обвинителство
ITIL	поранешен акроним за Библиотека на информатичко-технолошката инфраструктура, претставува збир од детални практики за управување со ИКТ услугите (ITSM) чиј фокус е усогласување на ИКТ услугите со потребите на деловното работење.
АКМИС	Автоматизиран Систем за управување со судски предмети, кој се спроведува во сите судови во Северна Македонија
HW	Хардвер на компјутерски системи, опрема што се користи за вршење ИТ активности
SW	Софтвер на компјутерски системи, програми, апликации и разни програмски алатки, кои работат на хардвер
Служба за корисничка поддршка	систем што им помага на корисниците на компјутерските системи и на ИКТ персоналот
ДИТ	Директор за информатички технологии, висока раководна позиција во една организација, одговорна за сите информатички услуги, складирање и безбедност
Сервер	хардверски уред, со процесор, меморија и складиште, кој се користи за разни функции за компјутерска обработка, а се чува на полици со многу поврзани сервери во нив

Извршно резиме

Овој документ, откако ќе се изготви, треба да стане дел од збирот различни документи, предлози и рамки, изготвени како резултати на спецификацијата на бараните услуги во рамките на проектната задача (ToR), за компонентата 3 (ИКТ) од проектот „Поддршка на реформите во правосудниот сектор“

Документот првично беше изготвен од страна на проектниот консултант, ИКТ експертот, по што беше споделен со голем број лица од ИКТ секторот низ целата земја, истакнати членови на ИКТ заедницата и во судовите и во обвинителствата, кои дадоа дополнителни, конкретни коментари и детали, со цел да биде целосно применлив и во согласност со моменталната состојба во овие организации и нивните идни потреби и можните насоки поврзани со ИКТ.

Покрај ова, во документот беа земени предвид и претходно изразените мислења и предлози, документирани во извештајот за обуката „Отворен простор“, која се одржа во Скопје, кон крајот на јануари 2020 година, а вклучуваше над 20 избрани ИКТ-професионалци од различни судови и обвинителства во Северна Македонија (повеќе детали во продолжение).

Овој документ претставува заеднички пристап кон примената на Политиката за безбедност на информациите, прилагодена на специфичната состојба во правосудните институции во Северна Македонија, како што се судовите и обвинителствата.Онаму каде што е можно или применливо, се вметнуваат кратки белешки, со конкретни коментари за состојбата во овие институции.

На крајот, ќе биде предложен конкретен пакет мерки што треба да се преземат во правосудните организации во Северна Македонија, а кои се засноваат врз инпутите обезбедени од страна на Советот за ИКТ и поширокаата ИКТ заедница во овие организации.

1. Дефиниција и вовед

Политиката за безбедност на информациите (ПБИ) претставува збир на правила донесени од страна на една организација за да се осигури дека сите корисници или мрежи на ИКТ структурата во рамките на доменот на организацијата се придржуваат кон прописите во врска со безбедноста на податоците што дигитално се чуваат во рамките на овластувањата на организацијата.

ПБИ управува со заштитата на информациите, која претставува една од многуте вредности што треба една корпорација да ги заштитува.Во овој текст ќе се разгледаат некои од најважните аспекти што треба да се земат предвид кога се размислува за развој на ПБИ.Рационално земено, може да се каже дека политиката може да биде опсежна колку што креаторите сакаат ИКТ да биде опсежна:во основа, сè од А до Ш во однос на безбедноста на ИКТ, па и повеќе од тоа.Од таа причина, акцентот овде е ставен на неколку клучни елементи, но не заборавајте ја и слободата што ја имаат организциите кога ги изготвуваат своите упатства.

Резултати од испитувањето на мислењата на обуката за ИКТ „Отворен простор“

На обуката „Отворен простор“, што нашиот проект ја организираше кон крајот на јануари 2020 година, за членовите на Советот за ИКТ и други вработени во ИКТ секторот во разни судски институции во Северна Македонија, од присутните беше побарано да дадат свои мислења за неопходните приоритетни активности и иницијативи на неколку теми.Во однос на темата „Организација на ИКТ“, овие беа нивните ставови:

1. Електронска размена на информации помеѓу различните институции во рамките на системот (тековни проблеми, активности и сл.); во моментот, ова се прави само на состаноците на Работната група за ИКТ, на секои 2-3 месеци;
2. Систематизација и документирање на сите ИКТ активности;

3. Создавање систем за корисничка поддршка за сите вработени во ИКТ, како лесен, достапен метод за размена на искуства и решавање на заедничките проблеми (сега, единствената локална алатка е ИТ Форумот (Битола));
4. Дефинирање и воспоставување јасна хиерархија за ИКТ во рамките на судството, одговорност и поле на надлежности на секое ниво, создавање ефикасни процеси на комуникација (нова организација);
5. Централизирано, долгорочно планирање на сите потреби за ИКТ;
6. Обезбедување задолжителна (сертифицирана) обука за ИКТ за целиот ИКТ персонал, најмалку еднаш годишно;
7. Структура на организацијата на ИКТ за правосудството – да биде јасно воспоставена, според принципот на најголема ефикасност.

Сметаме дека е важно да се земат предвид овие предлози кога се препорачуваат решенија за „Заштита на податоци, безбедност на информации и права на пристап“, и да се применат со цел постигнување најдобри можни ефекти.

2.Елементи на политиката за безбедност на информациите

2.1 Цел

Институциите креираат политики за безбедност на информациите заради:

- Воспоставување општ пристап кон безбедноста на информациите
- Откривање и спречување компромитирање на безбедноста на информациите, како што се злоупотреба на податоци, мрежи, компјутерски системи и апликации.
- Заштитување на угледот на организацијата во однос на нејзините етички и правни обврски; кога се работи за правосудниот сектор, а особено судовите, ова е од најголемо значење.
- Почитување на правата на клиентите во правосудниот систем, државјаните, недржавјаните и деловните субјекти; еден од начините за постигнување на оваа цел е обезбедување ефективни механизми за одговор на жалбите и прашањата во врска со реални или перципирани неусогласености со политиката.

2.2 Опсег

ПБИ треба да се однесува на сите податоци, програми, системи, објекти, друга техничка инфраструктура, корисници на технологија и трети страни во дадена организација, без исклучок.

2.3 Цели на безбедноста на информациите

Организацијата што се стреми да изготви функционална ПБИ треба да има добро дефинирани цели во врска со безбедноста и стратегијата за кои раководството има постигнато договор.Сите тековни несогласувања во овој контекст може да го направат нефункционален проектот за политика за безбедност на информациите.Најважното нешто што експертот за безбедност треба да го запомни е дека неговото познавање на практиките за управување со безбедноста ќе му овозможи да ги вклучитие практики во документите штое задолжен да ги изготви, а тоа е гаранција за потполност, квалитет и искористливост.

Поедноставувањето на јазикот на политиката е нешто што може да ги отстрани разликите и да обезбеди консензус кај раководството.Оттаму, треба да се избегнуваат нејасни изрази.Внимавајте и на правилното значење на поимите или обичните зборови.Најдобро е политиката да биде кратко и концизно формулирана.

Во неа треба да се избегнат и одвишни формулации (на пр., беспредметно повторување во пишувањето) со оглед на тоа што темата на ИКТ ги прави документите гломазни и неусогласени, со неразбирливост што го отежнуваразвојот.Конечно, мноштвото детали можат да го попречат целосното усогласување на ниво на политиките.

Оттаму, начинот на кој раководството ја гледа безбедноста на ИКТ се чини дека е еден од првите чекори кога некој има намера да воведе нови правила во оваа област.Исто така, експертот за безбедност треба да се осигури дека ПБИ има еднаква институционална тежина како и другите политики донесени во рамките на корпорацијата.Во случаи кога организацијата има поголема структура, политиките можат да се разликуваат и поради тоа да се издвојат со цел да се дефинираат процесите во конкретниотдел од таа организација.

Безбедноста на информациите се смета дека заштитува три главни цели:

- Доверливост – податоците и информациите мора да бидат ограничени на лица што имаат овластување за пристап и да не се откриваат на други;
- Интегритет – да се чуваат податоците непроменети, целосни и точни, а ИКТ системитефункционални;
- Достапност – цел што укажува на тоа дека информациите или системот им се на располагање на овластените корисници кога е потребно.

2.4 Политика за контрола на овластувања и пристап

Обично, безбедносната политика има хиерархиска поставеност.ИКТ подразбира дека вработените на пониско ниво обично се должни да не ги споделуваат тие малку информации што ги имаат, освен ако не се изрично овластени.Спротивно на тоа, вработените на повисоко хиерархиско ниво во организацијата може да имаат доволно овластувања да одлучат какви податоци можат да се споделат и со кого, што значи дека тие не се врзани со истите услови за безбедност на информациите.Значи, логиката е дека ПБИ треба да ја земе предвид секоја основна позиција во организацијата со спецификации што ќе го разјаснат статусот на нивните овластувања.

Усовршувањето на политиката се одвива истовремено со дефинирањето на административната контрола, или со други зборови, овластувањата што ги имаат лицата во организацијата.Во суштина, во ИКТ, овластувањата се доделуваат врз основа на хиерархија, каде што некој може да има овластување за сопствената работа, раководителот на одредена институција (на пр., претседател на судот или раководител на судот, доколку постои) има овластување за досиејата што им припаѓаат на кругот на луѓе за кои е назначен, а системскиот администратор има овластување само за системските датотеки.Се разбира, корисникот може да има овлатување за пристап до одредени класифицирани информации кога тоа е неопходно.Затоа, податоците мора да имаат доволно карактеристики на грануларностсо цел да се овозможи соодветен овластен пристап.Тука лежи тенката линија на изнаоѓањето фина рамнотежа помеѓу тоа да се дозволи пристап на оние што треба да ги користат податоците како дел од својата работа и да не се дозволи пристап на неовластени лица.

Пристапот до мрежата и серверите на компанијата, без оглед дали е во физичка смисла на зборот, треба да биде преку поединечни најавувања за кои е потребна автентикација во форма на лозинки, биометрика, картички за идентификација, токени итн.Мора да се врши следење на сите системи за да се евидентираат обидите за најавување (успешни и неуспешни) и точниот датум и време на најавување и одјавување.

Евиденција на пристапот до ресурси

Вработените во ИКТ се одговорни за одржување на следниве датотеки за евиденција најмалку 60 дена за секој сервер што го поддржуваат:

1. Датотеки за евиденција на пристапот до ресурси:треба да ги содржи успешните и неуспешните обиди за најавување;
2. Датотеки за евиденција на активности:активности што ги вршат системските администратори.АКМИС води своја евиденција на активности, но станува сè понејасен; датотеките за евиденција на АКМИС не го регистрираат пристапот за читање, а не даваат ниту конкретни информации за промената на податоците.

Проблем 1: *Дали секој суд ги чува овие датотеки за евиденција активни и дали повремено се проверуваат заради повреда на безбедноста?*

Процена на локалната ситуација 1:

Судови:

Иако секој серверски оперативен систем е поставен за да се чуваат датотеките за евиденција на пристапот до системот, понекогаш нивната големина го ограничува времето на нивно чување во системот, особено во големите судови, и кога има голем број настани што треба да се евидентираат. Според законот, секој суд мора да има службеник за безбедност, кој е надлежен за периодично прегледување на сите датотеки за евиденција.

Се покажа дека датотеките за евиденција на активности значително го забавуваат работењето на системот во судовите, па затоа не се користат, со оглед дека АКМИС води своја евиденција на активности, а и претставува основен систем во судовите (еден исклучок е тоа што АКМИС не го регистрира пристапот за читање)

Постои нов закон за заштита на личните податоци, усогласен со регулативите на ЕУ (БДПР), кој дополнително регулира некои аспекти од оваа област.

Јавни обвинителства:

Ситуацијата е слична како во судовите, со таа разлика што нивниот систем за управување со предмети (СУП) е помодерен, централизиран систем, без локални инсталации (сите корисници пристапуваат до системот преку интернет). СУП, за разлика од АКМИС, ги регистрира сите видови пристап, вклучувајќи и пристап до режимот само за читање.

Потребна активност 1:

Со новите, помоќни сервери инсталирани во сите судови, би требало да се чуваат сите датотеки за евиденција.

Пријавување повреди на пристапот

1. ИКТ персоналот води процес на доставување извештаи за неважечките обиди за најавување, по барање; не постои конкретен систем за следење на најавувањата во судовите, така што нивното следење е речиси невозможно.
2. ИКТ персоналот води процес на откривање и реагирање на систематските напади на серверските системи што ги поддржуваат.

Проблем 2: *Дали секој суд го одржува овој процес на доставување извештаи за неважечки најавувања и дали има периодични барања за доставување ваков извештај?*

Процена на локалната ситуација 2:
Судови:
*Според сегашните регулативи, службеникот за безбедност во секој суд мора најмалку двапати годишно да го проверува почитувањето на безбедносните правила, вклучително и најавувањата т.е. извештаите за нивната примена.Дирекцијата за безбедност на податоците е овластена да спроведува периодична ревизија на безбедносните правила на секој суд, по случаен избор.*Во овој момент нема алатки за следење на најавувањата или софтвер за управување со најавувањата, така што неважечките обиди за најавување треба да се најдат рачно, што е тешко да се изврши и може да доведе до нецелосни извештаи.*По ревизијата од страна на Дирекцијата за безбедност на податоците во некои судови, тоа беше една од забелешките што произлегоа од оваа ревизија. Затоа, Судскиот совет во неколку наврати побара средства за набавка на ваков вид софтвер, но досега не се обезбедени средства. За овој процес да се направи поефикасен и посеопфатен и да се спроведат периодични проверки и извештаи, софтверот за следење на најавувањата е од суштинско значење. Треба да се земе предвид и фактот дека службениците за безбедност во судовите се лица што се занимаваат со правни работи.*

Јавни обвинителства:
Ситуацијата е слична на судовите.

Потребна активност 2:

- *Погрижете се службениците за безбедност во секој суд/ЈО редовно да ги проверуваат сите најавувања, во согласност со прописите, користејќи нови алатки за следење на најавувањата*

Да се навратиме на развојот од претходната точка – како што ќе се развива програмата за безбедност на ИКТ, можеби ќе биде потребно ажурирање на политиката.Иако таквото нешто не мора да значи дека ќе биде и подобрување на безбедноста, ИКТ во секој случај е разумна препорака.

2.5 Класификација на податоци

Податоците можат да имаат различна вредност.Поради градациите на вредносниот индекс, може да биде неопходноодвојување и посебни режими/процедури за постапување за секој вид.Затоа, системот за класификација на информациите може да успее да се погрижи за заштитата на податоците што се од големо значење за организацијата, а да ги изостави незначајните информации што инаку би ги преоптоварile ресурсите на организацијата.Политиката за класификација на податоците може да го организира целиот пакет на информации на следните начини:

1. Класа со висок ризик – податоци заштитени со формално, официјално државно законодавство, тука се вклучени и финансиските податоци, податоците за платниот список и персоналот (барања за приватност). („Мерки за висока заштита“)
2. Доверлива класа – податоците во оваа класа не ја уживаат привилегијата да бидат под закрила на законот, туку сопственикот на податоците оценува дека ИКТ треба да биде заштитена од неовластено обелоденување. („Мерки за средна заштита“).Со оглед на природата на работата на ИТ кадрите, тие треба да поседуваат и

безбедносен сертификат; сега само мал процент од ИТ персоналот има таков сертификат (речиси воопшто немаат).

3. Јавна класа – овие информации можат слободно да се дистрибуираат.(„Мерки за основна заштита“)

***Проблем 3**: Дали оваа класификација на податоците е слична на дефинициите во релевантниот локален документ:*

„Технички и организациски мерки“, како што е дефинирано во член 5 од „Правилникот за изменување и дополнување на правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци“, издаден од Дирекцијата за заштита на личните податоци, во март 2009 година.

Процена на локалната ситуација 3:

Судови:
Во Северна Македонија, постои институцијата Дирекција за безбедност на класифицирани информации ДБКИ, која издава безбедносни сертификати на сите лица на кои им е потребен пристап до заштитени информации, во согласност со трите нивоа на безбедносни сертификати , како што е прикажано во 2.5. Се чини дека релативно мал број од клучните кадри во судовите (судиите) го имаат највисокото ниво на сертификација („Класа со висок ризик“).
Во Врховниот суд, сè уште нема посебна просторија за чување на тајните документи, кои бараат високо ниво на безбедност, иако прописите предвидуваат таа да постои.
АКМИС нема опција за работа со предмети што бараат високо ниво на безбедност, така што тие не можат да се обработуваат со оваа апликација!

Јавни обвинителства:
Многу мал број на јавни обвинителства на ниво на основни јавни обвинителства имаат сертификати за безбедност, освен одделението за организиран криминал; ова станува проблематично кога се појавува потенцијален предмет со класифицирани докази.
Апликацијата на СУП нема опција за работа со предмети што бараат високо ниво на безбедност, така што тие не можат да се обработуваат со оваа апликација!

Потребна активност 3:

- Погрижете се доволен број судии и јавни обвинители да имаат безбедносни сертификати, вклучувајќи ги и оние за високо ниво на безбедност, во согласност со прописите
- Побарајте двете клучни апликации во судовите и во јавните обвинителства (АКМИС и СУП) да вклучуваат обработка на предмети со сертификати за високо ниво на безбедност

Сопствениците на податоците треба да ја одредат класификацијата на податоците и точните мерки што треба да ги преземе лицето задолжено за заштита на податоците за да го зачува интегритетот во согласност со тоа ниво.

2.6 Поддршка и работење со податоци

Во овој дел можеме да најдеме членови што го предвидуваат:

- Регулирањето на општите системски механизми одговорни за заштита на податоците

- Системите што содржат лични информации и/или информации за деловни субјекти, како што се оние во правосудниот сектор, мора да бидат заштитени во согласност со постојните национални или организациски или секторски стандарди и најдобрите секторски практики (доколку има).Во таквите системи мора да функционира:
    - Најнова заштита против малициозен софтвер
    - Мрежна бариера
    - Шифрирање
    - Да бидат извршени адекватни исправки, кога ќе се појави потреба

Проблем 4*: дали се преземени сите овие мерки за заштита, во сите правосудни институции, особено во судовите?*

Процена на локалната ситуација 4:
Судови:
Сите горенаведени мерки се преземени во сите судови на РСМ
Јавни обвинителства:
Сите горенаведени мерки се преземени во СУП

Потребна активност 4:
Не се потребни активности.

- Резервни копии од податоците:Резеврвните копии треба да бидат шифрирани, во согласност со најдобрите практики во индустријата и хостирани во област на физичка безбедност.Резервните медиуми мора секогаш да се чуваат на некое од следниве:
    - Компјутерски центар
    - Ормар за податоци
    - Одредена канцеларија, заклучена и достапна само за избран персонал
    - Од исклучителна важност е да има одобрен објект за складирање медиуми надвор од локацијата; повеќето судови зачувуваат резервни копии од податоците без да ја проверат функционалноста и конзистентноста на податоците.Прво, затоа што не постои унифицирана постапка за проверка на вратените податоци и второ, затоа што нема реални технички ресурси за тоа да се реализира.

- Пренесување на податоците:
    - Трансфер на податоци може да се врши само со безбедни механизми за трансфер
    - Секоја информација на преносен уред (лаптоп, USB, диск итн.) што треба да се пренесе надвор од организацијата или во рамките на јавна мрежа, мора да биде шифрирана во согласност со општоприфатените стандарди во индустријата и важечките закони и регулативи (доколку има)

***Проблем 6**: Дали овие правила за пренесување на податоците се почитуваат во сите институции?*

Процена на локалната ситуација 6:
Судови:
Не постои строга контрола на надворешните уреди што се користат за копирање податоци, како USB, на оддалечени локации (локални судови со АКМИС), иако постојат правила за ова прашање!
Постои политика за ограничување на USB и други безбедносни политики, која се применува во согласност со законот за заштита на податоците.Исто така, (во некои судови) постојат ИСО процедури за:Управување со резервни копии, правила за пристап до просторијата на серверите, класифицирани информации итн.
Јавни обвинителства:
Бидејќи јавните обвинителства користат СУП како централно-базиран систем, само централната локација ги има податоците, така што полесно е да се контролира нивното пренесување; сепак, ова не е строго контролирано.

Потребна активност 6:

- И судовите и јавните обвинителства треба построго да ја регулираат и спроведуваат политиката за пренесување податоци на мобилни уреди, вклучително и шифрирање.

2.7 Обуки за подигнување на свесноста за безбедноста

Споделувањето на безбедносните политики за ИКТ со персоналот претставува клучен чекор.Ако ги натерате да го прочитаат и да го потпишат документот како потврда не мора да значи дека тие се запознаени и ги разбираат новите политики.Обуката ќе ги ангажира вработените со цел да изградат позитивен став кон безбедноста на информациите, што ќе обезбеди тие да добијат претстава за воспоставените процедури и механизми за заштита на податоците, на пример, за прашањата во врска со нивоата на доверливост и чувствителноста на податоците.Обуката за подигнување на свесноста треба да се осврне на широк спектар на теми од суштинско значење: како да се собираат/користат/бришат податоци, да се одржи квалитетот на податоците, управување со евиденција, доверливост, приватност, соодветно користење ИКТ системи, правилно користење на социјалните мрежи и др.Веројатно е добра идеја на крајот да има и мал тест.Клучни поенти за обуката за подигнување на свесноста за безбедноста на информациите:

- Оваа обука ќе биде вклучена во процесот на воведување на новиот персонал
- Тековна програма за подигнување на свесноста, која ќе ја креира и одржува соодветна организациска единица со цел свесноста за безбедноста на персоналот да се обновува и ажурира кога е потребно

2.8 Обврски, права и должности на персоналот

Општите согледувања во оваа насока генерално се однесуваат на одговорноста на лицата назначени за извршување на спроведувањето, едукацијата, одговорот на инциденти, прегледите на пристапот на корисниците и периодичните ажурирања на ПБИ.

1. Сите вработени ќе се придржуваат кон процедурите за безбедност на информациите, вклучително и за одржување на доверливоста на податоците и интегритетот на податоците.Во спротивно, може да дојде до дисциплински постапки.
2. Секој вработен е одговорен за оперативната безбедност на информатичките системи што ги користи.

3. Секој корисник на системот ќе ги почитува безбедносните барања што се во моментот во сила, а исто така ќе обезбеди највисоко ниво на доверливост, интегритет и достапност на информациите што ги користи.
4. Горенаведените правила ќе се применуваат во секое време, под услов инволвираниот персонал да биде соодветно и навремено едуциран за важечките правила на ПБИ.

2.9 Упатување на релевантното законодавство во Северна Македонија

(Тука ќе бидат наведени сите релевантни национални законски регулативи во Северна Македонија што се однесуваат на безбедноста на информациите, како и линкови до сите меѓународни стандарди, на Европската Унија и други, кои се референтни за националните регулативи, како на пример, БДПР)

1. „Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци“, издаден од Дирекцијата за заштита на личните податоци, во март 2009 година
2. „Правилник за изменување и дополнување на правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци“, издаден од Дирекцијата за заштита на личните податоци, во март 2010 година
3. „Правилник за стандардите и правилата за безбедност на информациските системи кои што се користат во органите за комуникација по електронски пат”, издаден од Министерството за информатичко општество, јуни 2010 година
4. „Судски деловник“, издаден од Министерството за правда, јуни 2013 година, членови 12, 88
5. „Деловник за изменување и дополнување на судскиот деловник”, јули 2014 година

2.10 Други точки што би можеле да бидат опфатени со ПБИ:

Постапка за заштита од вируси, постапка за откривање упади, постапка за далечинско работење, технички упатства, ревизија, барања за вработените, последици од неусогласеност, дисциплински постапки, вработени со прекинат работен однос, физичка безбедност на ИТ, упатувања на придружни документи и сл.

Проблем 9: *Дали некои од овие дополнителни активности се дефинирани и применети во судските системи на Северна Македонија?*

Процена на локалната ситуација 9:
Судови:
ИКТ персоналот на Врховниот суд, Судскиот совет и 4 апелациони судови се сертифицирани за ИСО, со околу 10 клучни процедури дефинирани со ИСО.
Јавни обвинителства:
Јавните обвинителства не се сертифицирани за ИСО; не се дефинирани дополнителни процедури!

Потребна активност 9:

- Судовите треба да се погрижат редовно да се почитуваат овие постапки засновани на ИСО и персоналот да биде информиран за нив; ИСО сертификација треба да се спроведе и во основните судови.Јавните обвинителства треба да се обидат да добијат ИСО сертификат, исто како и судовите!

3. Заклучок (важноста на ПБИ)

Претежно од невнимание, многу организации, без многу да размислат, одлучуваат да преземат готов примерок на политика за ИКТ од веб-страница и да го копираат/залепат овој готов материјал во обид некако да ги прилагодат своите цели и целите на политиката да одговараат на калапот што обично е необработен и чијазаштитае со премногу широк спектар.Правилен метод е, дури и кога се копираат некои готови правила на ПБИ, тие задолжително да бидат прилагодени на конкретните потреби и правила на организацијата, во случајов други правни правила и прописи што се однесуваат на правосудниот сектор во Северна Македонија, било да е тоа ИКТ само за системот на судови, или за други сегменти на правосудниот сектор.

Висококвалитетната ПБИ може да ја направи разликата помеѓу компаниите во развој и успешните компании.Зголемената ефикасност, зголемената продуктивност, јасноста на целите што секој субјект ги има, разбирањето кои ИКТ и податоци треба да се обезбедат и зошто, идентификувањето на видот и нивоата на безбедност што се бараат и дефинирањето на најдобрите применливи практики за безбедност на информациите се доволни причини за да се поткрепи оваа изјава.

4. Општи предлози за правосудните институции во Северна Македонија

Иако постојат неколку национални документи што се однесуваат на општите правила за безбедност на информациите за судовите наведени овде во точка 2.9, постои загриженост дали сите овие правила и прописи се спроведуваат на систематски начин, во сите институции во рамките на правосудството.Оттука, се наметнува потребата за дополнително внимателно, редовно испитување и процена на мерките пропишани тука, проширувајќи ги низ целокупниот правосуден систем.

5. Кибер-безбедност

Кибер-безбедноста се однесува на безбедносните проблеми, процедури и методи што се релевантни за заштитата на ИКТ системите и податоците што ги содржат од упади преку Интернет.Табелата подолу, од НИСТ (Националниот институт за стандарди и технологија, најпознатата организација во оваа област), го прикажува прифатениот стандарден процес на справување со заканите за кибер-безбедноста.

Овој циклус на активности покажува дека процесот започнува со идентификување на заканите за кибер-безбедноста, вклучително и процена на ризиците, потоа продолжува со воспоставување соодветна заштита за утврдените закани, потоа со воведување методи и алатки за откривање на таквите закани, проследено со претходно утврден одговор на овие закани.По соодветниот, претходно утврден одговор, мора да следи процес на обновување, каде што треба да се санираат сите оштетувања на системите и податоците.Овој циклус постојано се практикува бидејќи заканите и ризиците што се создаваат со текот на времето се менуваат.Прашањето за кибер-безбедност ќе биде посебно разгледано подоцна.

6. Права на пристап

Судови:

Доделувањето на правата на пристап се регулира на годишно ниво, со употреба на ажурираниот документ „Распоред за работа на судиите и судска администрација на судовите“.Персоналот од овој документ потоа се поврзува со улогите доделени од АКМИС системот.

Во овој случај, „улогите“ се поврзани со различниот збир права на пристап, дефинирани за секој конкретен вид работна позиција во судот, на пр., улогата на службеникот задолжен за архивата е различна од улогата на судскиот помошник, со тоа што на секоја од овие улоги ѝ е доделена различна слобода за пристап до разни компоненти на системот, а во рамките на нив, различен избор помеѓу правата за читање, пишување и менување.

Системот за доделување улоги во рамките на АКМИС се чини дека обезбедува доволен избор на разни комбинации на права на пристап со цел да се изберат конкретните работни задачи за секој вид вработен во судот, па дури и за конкретно лице.

За натамошен развој на пристапот поврзан со правата на пристап може да бидат потребни, колку што тоа го овозможуваат технологијата и финансирањето, пософистицирани алатки за спроведување и обезбедување строго почитување на доделените права на пристап.Ова може да се направи преку примена на разни биометриски алатки, како скенирање на мрежницата, отпечатоците од прсти и слично.

Обвинителство:

Персоналот во обвинителската организација подлежи на истите ограничувања и примена на правила, во согласност со својот Систем за управување со предмети (СУП), кој е централно инсталиран систем, наспроти АКМИС, кој е дистрибуиран систем (еден примерок од истиот софтвер во секој суд).

7. Акциски план

Ова е пакетот препораки, претставени во документот, со предложени дополнителни активности:

Совет за ИКТ:

Овој документ, кој веќе е проширен со коментарите и предлозите собрани од повеќе вработени во ИКТ низ целата земја, ќе биде испратен од нашиот проект до Советот за ИКТ, за натамошни нивни активности.Очекуваме Советот за ИКТ да продолжи со следниве активности:

a. Прегледување на документот, при што ќе се разгледаат натамошни проширувања или подобрувања, на својот следен месечен состанок;
b. Назначување на еден од членовите како известувач за управување со процесот на пополнување на овој документ;
c. Советот за ИКТ треба, при прегледот на овој документ, да ги разгледа потребните активности, дефинирани во документот, и нивните последици врз идните планови за стратегијата за ИКТ, како и потребните измени на стратегијата за ИКТ, временскиот распоред и финансиските потреби;
d. Откако ова ќе се изврши, Советот треба да го вметне овој документ како дел од стратегијата за ИКТ и да го испрати комплетираниот документ, заедно со предложените активности, временскиот распоред и финансиските очекувања, за натамошно разгледување до Министерството за правда и другите релевантни тела/институции;

Потребна активност 1-10:

- *Со новите, помоќни сервери инсталирани во сите судови, би требало да се чуваат сите датотеки за евиденција.*
- *Погрижете се службениците за безбедност во секој суд/јавно обвинителстворедовно да ги проверуваат сите датотеки за евиденција, во согласност со прописите, користејќи нови алатки за следење на датотеките за евиденција.*
- Погрижете се доволен број судии и јавни обвинителида имаат безбедносни сертификати, вклучувајќи ги и оние на високо ниво, во согласност со прописите;
- Побарајте клучните апликации во судовите и во јавните обвинителства (АКМИС и СУП) да вклучуваат процесирање на предмети со сертификати за висока безбедност;

- И судовите и јавните обвинителстватреба да обезбедат редовно зачувување резервни копии на податоците на сите локации, според прописите, да се пренесат на ленти и да се чуваат на безбедни, одделни локации, подалеку од просторијата на серверите;
- И судовите и јавните обвинителства треба построго да ја регулираат и спроведуваат политиката за трансфер на податоци на мобилни уреди, вклучително и шифрирање;
- И судовите и јавните обвинителства треба да обезбедат редовно информирање и обука за свесноста за безбедноста, во што ќе биде вклучен новиот персонал; Наставна програма на Академијата за судии и јавни обвинители на оваа тема;
- И судовите и јавните обвинителства треба да дефинираат методи за ширење информации до целиот свој персонал;
- Судовите треба да се погрижатредовно да се почитуваат овие постапки засновани на ИСО стандардите и персоналот да биде информиран за нив; ИСО сертификација треба да се спроведе и во основните судови. Јавните обвинителства треба да се обидат да добијат ИСО сертификат, исто како и судовите;
- Судовите и јавните обвинителства треба да размислат за проширување на своите методи поврзани со правата на пристап со употреба на биометрика и прецизирање на тековните методи за правата на пристап.

Резултати поврзани со финансиите и временскиот распоред:

- Промени во клучните апликации во судовите и во јавните обвинителства (АКМИС и СУП) за да вклучат процесирање на предмети со сертификати за висока безбедност: приближно 50.000 ЕУР, во период од 6 месеци.
- Избор, набавка, обука и примена на новата алатка за следење на датотеките за евиденција: приближно 50.000 ЕУР, во период од 3 месеци.
- Спроведување ИСО сертификација и во основните судови: приближно 20.000 ЕУР, во период од 4 месеци.
- Набавка и примена на дополнителни биометриски алатки: приближно 50.000 ЕУР, во период од 6 месеци.

Список со референци

Bayuk J. (2009). *How to Write an Information Security Policy*. Преземено на 04/06/2014 одhttp://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html?Page=2

Entrepreneur. *Information Technology Security Policy*. Преземено на 04/06/2014 одhttp://www.entrepreneur.com/formnet/form/731

IG Toolkit (2007). *NHS CFH_Corporate infosec Policy Template 2007*. Преземено на 04/06/2014 одhttps://www.google.bg/?Gfe_rd=cr&ei=knylu52dlopb8gf93og4cq#q=NHS+CFH_Corporate+infosec+Policy+Template+2007

Olson, I & Abrams, M. *Information Security Policy*. Преземено на 04/06/2014 одhttp://www.acsac.org/secshelf/book001/07.pdf

Perkins, J. (2013). *Information Security Policy*. Преземено на 04/06/2014 одhttp://www.lse.ac.uk/intranet/lseservices/policies/pdfs/school/infsecstait.pdf

Scott, A. (2013). *How to create a good information security policy*. Преземено на 04/06/2014 одhttp://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy

Sophos Ltd. *Sophoslabs Information Security Policy*. Преземено на 04/06/2014 одhttp://www.sophos.com/en-us/legal/sophoslabs-information-security-policy.aspx

Techopedia. *Information Security Policy*. Преземено на 04/06/2014 одhttp://www.techopedia.com/definition/24838/information-security-policy

Timms, N. (2014). *Secure Networks: How to Develop an Information Security Policy*. Преземено на 04/06/2014 одhttp://www.networkcomputing.com/secure-networks-how-to-develop-an-information-security-policy/a/d-id/1234642?

The University of Illinois (2014). Information Security Policy – The University of Illinois. Преземено на 04/06/2014 одhttp://www.obfs.uillinois.edu/cms/one.aspx?Portalid=909965&pageid=914038

University of Oxford (2012). *Information Security Policy*. Преземено на 04/06/2014 одhttp://www.it.ox.ac.uk/media/global/wwwitservicesoxacuk/sectionimages/security/Information_Security_Policy_2012_07.pdf