Заштита на лични податоци од малку поинаков аспект
Проблеми во ИТ поради недостаток на законска регулатива
одразени во секојдневното работење

Нота : Студијата е направена врз база на презентацијата одржана на 07 април во рамките на работилницата " Новата рамка за заштита на лични податоци"

Краток вовед: Живееме во време на висока технологија каде што секоја информација и пристапот до неа се од најголемо значење. Заради тоа сигурноста мора да е максимално контролирана поради заштита од злоупотреба во најразлични цели а поддржана со законски регулативи и стандарди. Во продолжение ќе го изложам мојот став базиран врз 15 годишно искуство во работа со податоци, бројни семинари и стручна литература, како и голем број статии презентирани на интернет.

Податоците во 21 век се најскапиот производ што се нуди на пазарот. Со вистински податок во вистинко време е можо се да се оствари. Заради тоа, податоците како такви се подложни на најразлични злоупотреби како заради лична корист така и намерно нанесена штета, профит, борба со конкуренција, нови достигнувања па дури и заради задоволство и забава. Во едно вакво време и опкружување најважно е тие информации да се заштитат и санкционира секакво неовластено и незаконско користење на истите. Ако ни провалат во домот или ни украдат кола, не ограбат на улица, секогаш можеме да пријавиме во полиција или надлежни институции, но ако ни ги украдат информациите и ги злоупотребат ние немаме каде да се обратиме за помош и легални права, како и надомест за претрпената штета која може да биде многу пати поголема од крадењето на колата. Затоа е многу важно да подотацоте како такви се заштитени со добри и цврсти закони и да се спроведуваат мерки на предострожност за навремено спречување на секакви манипулации со нив. Меѓутоа мора да се води сметка за еднаква заштита и процедура за податоците запишани во електронски облик и доставени на хартија, бидејќи резултатите се потполно идентични. Јас ќе се задржам на проблемите и процедурите околу чување и обработка на податоци во електронска форма.

Податокот во една база може да биде нападнат од три стрни, од внатрешни субјекти (вработени во организацијата), надворешни субјекти (било кој човек на земјината топка) и во периодот на трансфер низ телекомуникациските водови од една во друга филијала во склоп на една организација или различни компании при размена на податоци.

Најчести и најопасни упади се од внатрешните субјекти. Некои истражувања и анкети покажуваат дека дури 90% на неовластени користења се од вработените или пак со нивна помош. Поставувањето на работни процедури и нивоа на пристап и заштита се една од најбитните мерки на предострожност и заштита во ваквите случаи. Тука е потребна заштита на физичко и логичко ниво. Физичкото уништување на податоците може да настане од неправилно ракување со техничката опрема, оштетување или расипување на компјутерите или евентуални елементарни катасрофи. Во ваквите случаи најдобра заштита се редовните бекапирања на системите и базите, а во поосетливите системи и далечински водени сервери на различни локации. Многу е важно да контролата на бекапот (резервна копија на сите податоци содржани во еден компјутер) биде направена од стручно лице, бидејќи доста се чести случаите кога бекапите не само што не се верни на оригиналот, туку се сосема нешто друго и непотребно а понекогаш и празни медиуми. Како физичка заштита се подразбира и сигурноста на локацијата каде е сместен компјутерот, бидејќи сите сигурносни ситеми во мрежата се небитни, ако некој успе да влезе во просторијата и физички го украде целиот компјутер заедно со комплетната содржина во него. И само да напомнам уште еден пример за лошо организиран бекап, кога медиумите се чуваат на видни и достапни места, и често до самите машини, па во случај на пожар или елементарна непогода, ќе се уништат заедно со машината. Заради тоа тие треба да се чуваат на посебно одредени и заштитени локации. Со еден збор, потребна е строго дефинирана процедура во пишана форма за целокупната активност околу физичката заштита на податоците, за која што секој вработен ќе сноси одговорност доколку не се придржува до строго дефинираните правила.

Кога станува збор за логичката заштита на податоците, се мисли пред се на нивната веродостојност. Што може да се случи? Заради нестручно работење или недоволно познавање на апликациите може некој податок да се внесе погрешно. Како банален пример може да се земе полот на вработениот, па некој господин да добие ружи за 8 март бидејќи е внесен како женско, меѓутоа што е уште многу пострашно некој човечки живот може да биде загрозен заради добивање на крв од погрешна крвна група која по грешка е промашена при внесот за "само" една буква. Поради тоа најважен фактор е добрата обученост на вработените и нивно максимално познавање на апликацијата на која работат. Исто така, строга дефинираност на нивото на пристап, односно на кого му е дозволено да внесува податоци, кој ќе ги верифицира и потврдува, кој има право на измени, бришења или само читање на внесените податоци а на крајот и нивно процесирање, односно обработка за понатамошни потреби. Целата оваа структура мора да е специфицирана во процедури и овластувања, подкрепени со законски норми и регулаиви. И секако најважно, поделба на податоците по ниво на критичност и воведување на системот на 4 или 6 очи. Тоа значи дека таквите податоци треба да се проверат најмалку 2 до 3 пати пред да тие бидат запишани во базата. Ако на некој субјект во досието му се згреши бојата на очите нема да му се нанесе иста штета како кога би му го згрешиле матичниот број (тогаш тој ќе биде некој друг а не самиот).

Во делот за заштита на податоците од надворешни субјекти, станува збор за неовластен пристап кон базите од лица кои воопшто несмеат да дојдат во допир со нив. Тоа се таканаречени хакери, или натрапници. Нивните цели се најчесто од лична корист, а не така ретко и докажување на нините можности за упад во

недозволени системи. Може да бидат со страшни последици, доколку ги уништат сите податоци (само да предизвикаат штета), или пак провокативни, кога само им стават до знаење на вработените дека биле тука и можат да прават што сакаат. Доста често се случуваат финансиски кражби, понекогаш злобни упади на конкуренцијата за да докаже надмоќ, или промена на содржината на податоците заради избегнување на санкции или пак добивање на награди и пофалби. Од која и да е причина упадот, секако прави штета од многу големи размери затоа што најчесто треба многу време да се примети дека некој тоа неовластено го сменил, а доста често останува и неприметена целата активност. Овие дејствија би ги споредила со неовластено влегување во нечив дом или фирма и разгледување и менвање на личните предмети на некој субјект, што е кривично дело а во компјутерското опкружување сеуште останува неказнето. И што е уште полошо нема кај да се пријави и не постои некој што би ги гонел. Заради тоа во делот на заштита на информационите системи нетреба да се штедат средства и ресурси за максимален мониторинг, затоа што само еден упад може да биде кобен засекогаш.

Преносот на податоци низ јавните телекомуникации е секојдневна и неизбежна активност. Во сегментот од една до друга машина тој е во облакот од информации и надвор од нашата контрола, и како таков лесен за манипулација. Заради тоа, при трансферот на податоци потребно е да се користат сите модели и достигнувања во теоријата на шифрирање, кодрање и сигурносни механизми. Лесно може податоците да се пресретнат на патот и да стигнат во рацете на неовластени лица кои може понатаму да ги злоупотребат. Во вакви случаи најдобро е да се направт стрикни договори, во кој дел од патот на податокот е одговорен испраќачот, примачот или компанијата што врши пренос.

Сите наведени проблеми, процедури и заштити треба да се спроведат и имплементираат под стручен надзор на вработените во ИТ секторот но под строга контрола и дефинирани правила од менаџментот на организацијата. Секој раководител треба за својот сектор да достави писмена студија за сите активности и права на вработените околу работењето со податоците во нивниот дел на обработка. Колку повеќе се поделени и специфицирани обврските, толку е подобар системот на контрола и заштита. И на крај, како врв на целата пирамида се наоѓаат системските администратори и лицата од ИТ, кои располагаат со сите лозинки и имаат пристап до системот во целост. Заради тоа мора да се направи детална структура на нивниот пристап и секако да се изврши ревизија од вработени надвор од секторот. Најдобар начин е да лозинките бидат поделени на два дела (или се постават повеќе лозинки доколку тоа е потребно) и за секоја промена во системската администрација бидат присутни најмалку двајца вработени. Најопасно е кога некој систем администратор располага со сите лозинки и ги има сите пристапи, па е во можност да направи секакви манипулации со податоците и никој неможе да го контролира.

За избегнување на злоупотреби и максимална контола е потребно да секој корисник потпише согласност со процедурите и сигурносните политики на организацијата, со што лично ја превзема одговорноста за секоја неправилност и во потполност е известен до каде е неговота одговорност. А понатаму самата организација експлицитно наведе кога е виновен вработениот, кога неговиот раководител (зарадо лошо поставена процедура) или пак целата организација доколку се нанесе штета на некој субјект заради погрешна обработка на податоците.

Најдобар начин на проверка е секојдневно следење на лог фајловите (записи во системот каде што е наведена целата негова активност) во тек на 24 часа. Овие логови треба понатаму да се ревидираат и од лица надвор од ИТ секторот. Да се определи времето на достапност до системите и податоците, и секоја активност надвор од пропишаното време да е дозволена само со согласност и надзор на одговорно лице. Системите се најчесто напаѓани вон работното време, попладневни и ноќни часови како и викенди и празници, заради намален мониториг и отсатност на системските администратори. Мора да се блокира пристапот на секое корисничко име, доколку вработениот во одреден период не доаѓа на работа (зарди годишни одмори, боледувања и сл.).

Уште една препорака, која е многу важна а доста често запоставена, е сигурноста на софтверите и апликациите. Сите софтвери кои не се лиценцирани и не стандардизирани може во себе да содржат голем број грешки, а некои дури и поставени "дупки" или таканаречени "backdoor" кои што програмерите може намерно да ги вградат и после од таму да влегуваат неприметно и неовластено ги користат податоците. Потребно е да софтверот се набавува од сертифицирани компании со ИСО стандарди кои гарантираат за сигурноста и точноста на податоците и нивната обработка, а сето тоа вградено во меѓусебни договори со ниво на права и одговорности. На вработените треба да им се забрани внесување на секаков вид софтвери од надвор и нивна инсталација на било која машина од мрежата без претходна консултација и одобрување од овластените во ИТ секторот.

Како заклучок би навела : што подобра обученост на корисниците, редовно школување на вработените во ИТ околу сите нови технологии и достигнувања, користење на сите расположиви средства за набавка на добри и сигурни софтвери и дефинитивно никако штедење или импровизации околу информатичката технологија во една организација.