ТЕХНИЧКИ И МЕТОДОЛОШКИ АСПЕКТИ ЗАШТИТЕ ЕЛЕКТРОНСКИХ КОМУНИКАЦИЈА И ИНФОРМАЦИЈА

Потпуковник Милорад С. Маркагић*

Потреба да се информације заштите стара је колико и људско друштво. У савременом свету, развојем средстава телекомуникација и информатике, обрада, пренос и складиштење информација доживели су метаморфозу из конвенционалних у методе дигитализације, а самим тим и поступак њиховим руковањем захтева нове методе приступа.

Интерес да се са једне стране дође до информација, а са друге стране да оне буду заштићене представља вечиту борбу оних у чијим су рукама информације од непознатих или неовлашћених лица.

Проблематици заштите информација мора се приступити са посебном пажњом, узимајући у обзир све релевантне чиниоце који утичу на безбедност, али се заштита никако не сме препустити само појединцима или уском кругу стручних лица, већ је то задатак целе организације и система одбране. У том сегменту познавање метода и поступака, као и обука кадра играју велику и значајну улогу. Рад је плод вишегодишњег рада и искуства аутора у овој области.

*Аутор ради у Војној академији

Паралелно са технологијом, развија се и расте употреба релативно једноставног приступа средствима комуникација и информационој технологији, што за последицу има убрзани проток и повећану количину информација, које се преносе у свакодневној комуникацији између појединаца, али и у предузећима и државним институцијама. Брз развој интернета и глобализација мреже нису само олакшали пренос информација, образовања и забаве, него су допринели и променама у безбедности у виду повећања и лакоће

добијања података и информација, како оних у изворном облику тако и оних у дигиталном формату, који се преносе телекомуникационим средствима.

Проток информација је веома тешко контролисати, посебно оних који се преносе бежичним или јавним мрежама. Због тога, класични поглед заштите података полако губи примат и преноси се у електронски свет, односно свет информационо-комуникационих технологија (ИКТ). Решавање питања безбедности информација превазилази појам производње, прераде и преноса са папирних медија и улази у зону виртуелног света.

Снимио: Јово Мамула

Поред традиционалних војних претњи по безбедност државе, претња у области ИКТ, у смислу изазова, ризика и претњи, у последње време постаје додатни фактор на који се треба усредсредити. То је довело до редефинисања концепта националне безбедности у свим земљама света, који је био, поред стандардних војних, обавештајних, терористичких претњи, проширен и унапређен да обухвати и сајбер претње.

Сведоци смо брзе промене, модификације безбедносних претњи с једне стране и недостатак сигурносне културе, с друге стране, било из разлога неспособности и незнања или и као намерних дела лица који се баве информацијама.

Последњих неколико година „процуреле" су обавештајне, дипломатске као и информације највиших државних органа појединих земаља, које су бивши радници тих истих обавештајно-безбедносних структура стављали на располагање јавности.

ИНФОРМАЦИОНА БЕЗБЕДНОСТ

Стање безбедности, на најширем нивоу у организацији/инфраструктури протока информација, стекло је потпуно другачију димензију. Од локалног до међународног нивоа све већи значај даје се заштити информација и њиховог пута од извора до крајњег одредишта. Један од најважнијих сегмената и приоритета у вођењу националне безбедности је заштита инфраструктуре и људских ресурса, у којој сајбер безбедност има важни улогу.

Идентификација, детекција, благовремено деловање и отклањање безбедносних претњи које укључују рат, тероризам, економске и еколошке претње, организовани криминал и друге претње, захтева укључивање свих чинилаца друштва, а често и међународну сарадњу.

У разматрању развоја технологије, слободно можемо користити термин информатичка револуција, јер је пораст обраде, преноса и складиштења информација у електронском облику у огромној мери преузео примат од конвенционалних метода.

Ради ефикасне и потпуне заштите информација потребно је, пре свега, идентификовати спољне претње безбедности, а затим анализирати рањивости сопственог система, узимајући у обзир међузависност свих фактора у руковању информацијама.

Систем одбране продуктиван је само у оној мери колико је процес доношења одлука, преношење и руковање у рукама оних који спроводе ове радње и поступке.

Знајући да квалитет и брзина преноса информација зависи од људских и техничких фактора, норме и стандарди морају бити постављени тако да обезбеде прецизне смернице које треба следити током редовних и уобичајних токова коришћења информација.

Релативно независни атрибути објективно оријентисаног приступа информацијама засновани су на неколико захтева, као што су:

- поверљивост,
- интегритет,
- доступност,
- неопозивост,

- функционална безбедност,
- поузданост ТКИ система,
- поузданост имплементираног система заштите,
- квалитет хардверских компоненти у најширем смислу,
- повезаност компоненти у један систем,
- примена мера и поступака регулисаних законима, смерницама и прописима ...

У научним круговима, али и у најширем смислу, у свакодневној комуникацији, у употреби су многе дефиниције безбедности информација, у зависности од нивоа и сврхе њиховог коришћења.

На националном нивоу општа дефиниција била би заштита виталних националних и државних интереса, у економији то би биле пословне информације о технолошком развоју, у области заштите података о личности информације не би требало да буду доступне трећим странама итд.

У пракси, сигурност информација нераскидиво је повезана са концептом заштите. То су активности и процедуре које се предузимају ради спречавања или минимизирања штете на имовини или особама, без обзира на то да ли они представљају претње од природних фактора, случајне грешке или фактор људске руке. [2]

Поуздане, тачне, висококвалитетне, интегрисане и брзо преносиве информације неопходне су за правовремено доношење одлука и реализацију планираних радњи и активности. Тиме оне постају најугроженији и најкритичнији ресурс државе и система одбране.

Ако се вредност информације посматра кроз функцију времена, онда је ово најутицајнији фактор у заштити информације. У зависности од врсте и степена тајности, примењују се одговарајуће методе заштите, узимајући у обзир реалне процене ризика, расте значај заштите и компаративне вредности и инвестиција.

Безбедоносне информације реализује се кроз систем заштите, са посебним освртом на процену ризика и претњи, и на тај начин контролишу и штите информације, тако да се сигурносни ризик у потпуности елиминише или смањи на прихватљив ниво.

Сигурност података и систем заштите спроводе се ради:

- спречавања опасности по државу,
- заштите личних података,
- спречавања терористичких активности,
- спречавања крађе и преваре,
- спречавања крађе интелектуалне својине,

- спречавања неовлашћених и незаконитих радњи,
- превенције повреде приватности,
- превенције цурења корпоративних информација и података,
- превенције промене података током преноса ...

Овакве и сличне активности захтевају налажење и имплементацију оптималног система заштите, који је економски оправдан и служи својој основној сврси, а то је ефикасна и економична заштита информација током припреме, уноса, обраде, преноса, дистрибуције и складиштења.

САЈБЕР БЕЗБЕДНОСТ

Савремени оружани сукоби и ратови незамисливи су без сфере информационог деловања, па се све чешће користи појам информациони или информатички рат. Иако слични по називу оба сегмента имају своје место и улогу, па су скоро све армије у свету увеле или уводе у употребу офанзивне или дефанзивне методе за сајбер ратовање. Наравно не треба испустити из разматрања и класичне методе ратовања, а нарочито методе нападе на информације, који су још актуелни и спроводе се перманентно.

Преузето са web cajra euro legal

Још један незаобилазни фактор који утиче на комплексност заштите информација јесте и брзи развој мобилних телефона, који су за кратко време од основне намене еволуирали у мини рачунаре. Имајући у виду да велики број корисника осим приватних, овим путем размењује и огроман број службених и поверљивих информација, а да је садржај потпуно незаштићен и да су путеви преноса јавно доступни, овом сегменту треба посветити знатну пажња.

ПРЕТЊЕ И НАПАДИ

Све информације, а нарочито оне у електронском облику, подложне су разним облицима унутрашњих и спољашњих претњи.

Како је овај вид обраде, преноса, заштите и чувања података знатно олакшан, учињен ефикаснијим, ефективнијим, флексибилнијим и знатно је допринео продуктивности у раду, смањењу трошкова и мањем ангажовању ресурса, појавили су се и пратећи начини деловања многобројних фактора на електронске информације.

Осим раније поменуте поделе на намерне и изазване нападе и претње, овде ћемо се осврнути на неке најкарактеристичније и најзаступљеније облике претњи и напада.

Унутрашњи (интерни) напади и претње

Било да је реч о намерним или ненамерним активностима, ове претње и нападе изводе лица из организацијске целине с циљем стицања неке добити, жеље за самодоказивањем или зарад шпијунаже.

Пошто систем одбране није у потпуности аутохтон и велики број спољних сарадника или компанија су ангажовани у процесу, за реализацију појединих активности којима се делом баве спољни сарадници или компанија, ова категорија представља кориснике са нижи нивоом поверења, често укључених у активности у којима постоје информације које су под одређеног степеном тајности и доступне су им у неком облику.

Крађа, или чак намера да се открију или оштете и поремете информације, често остаје непримећена и неоткривена у унутрашњој средини или постају очигледне релативно касно.

Иако поједине елементе ових напада можемо наћи у и спољашњим претњама, сврха иза потенцијалних напада унутар организације је да се умањи утицај информација и да је учине недоступне корисницима, трајно или за одређени период.

Спољашњи (екстерни) напади и претње

Систем одбране, као један од кључних фактора безбедности државе, подложан је непрекидном праћењу, анализи и покушајима деструкције на свим пољима, те се тако у општем појму безбедности и заштите неминовно долази до закључка да су подаци и информације константно на удару противничке стране.

Напади се изводе путем прислушкивања, блокирања, контроле протока информација, пресретањем, довођењем у заблуду, лажне идентификације, модификације информација, као и физичким уништењем фактора и елемената са којима или којима се информацијом рукује.

Шпијунажа, крађа, убацивање злонамерних програма у систем електронске обраде података информација су све чешће појаве напада на ТКИ система.

Искуства показују да огроман број напада долазе унутар система, пре него да су дела екстерних фактора.

Додатни облици угрожавања безбедности информација

Неки од фактора који могу утицати на безбедност информација у најширем смислу, а не могу се подвести под раније наведене врсте напада и претњи, јесу појаве и активности на које се неретко не може утицати, иако су предузете све мере. Ти облици угрожавања били би:

- честа немогућност одређивања посебних зграда, објеката или делова инфраструктуре за поступање са информацијама,
- кварови и ненамерна оштећења уређаја и средстава,
- напонске варијације,
- катастрофичне природне појаве и непогоде,
- недостаци у конфигурацији техничких уређаја и средстава (хардверска решења),
- непотпуна или непостојећа програмска (софтверска) решења,
- утицај различитих фактора на спојне путеве и
- недовољна попуњеност кадром и техничким средствима.

СИСТЕМ ЗАШТИТЕ

Основни циљ заштите информација јесте да се у потпуности рационализује управљање ризиком, од процене до елиминисања или редукције на прихватљиви ниво.

Систем заштите спроводи се у неколико корака, који не морају нужно да буду, а обично јесу, везани за сваки сегмент, међусобно су зависни и немају стриктне границе. Корелација односа евидентна је од почетка процеса па све до коначног краја активности који се односе на заштиту информација:

- дефинисање пројекта,
- процена ризика и претњи,
- имплементација заштите,
- контрола ефикасност,
- надоградња у оквиру постојећих система заштите,
- упоредни развој нових система,
- замена постојећих решења и
- евиденција.

За имплементацију и реализацију ових активности неопходно је испунити основне претпоставке и услове који су се у пракси показали као веома успешни и представљају скуп персонала, организационих, оперативних и тактичких мера:

- јасно дефинисана политика заштите,
- тренирано особље за успешну примену мера заштите,
- обезбеђена средства за спровођење заштите,
- спровођење интерне и екстерне контроле мера заштите,
- унапређење система заштите и
- санкције за кршења регулације.

Принципи реализације

Нормативни оквир је тај који обезбеђује потпуно функционисање система заштите. Стратегија заштите представљала би документат који обезбеђује технологију, методологију и одговорност учесника у систему заштите.

За реализацију, коришћење, надзор и контролу, планирање функција, реализацију циљева и побољшање метода заштите неопходно је израдити сва нормативна документа на највишем нивоу, полазећи

од основних постулата датих у системским документима (закони, стратегије, доктрине...), а који се огледају кроз израду упутстава, правилника и доношење наредбодавних аката.

Да би се осигурала безбедност информација у сопственом систему, али и код других власника/носиоца ТКИ, или у оквиру јавне мреже, треба следити принципе који су широко прихваћени у светској теорији и пракси.

Основни принципи, без улажења у дубље објашњење термина, који су очигледни из њихових имена, били би:

1. принцип управљања,
2. принцип „Никад сам",
3. принцип ротације радних места,
4. принцип раздвајања дужности
5. принцип минималне привилегије и
6. принцип „потребе да се знају основе".

Политика заштите

Да би се успешно реализовали принципи и спровео програм заштите информација надлежни органи документују, реализују и предузимају све мере на примени, одржавању, унапређењу и контроли реализације мера заштите. Овим се превасходно баве стручни органи и службе, али је подршка командовања неопходна у свим фазама и деловима реализације политике заштите.

У складу са формирањем и организационом структуром, дефинисаним задацима, потребама, величином и опремљеном јединицом – институцијом, развијени су нормативни акти, обавља се контрола и систем заштите је унапређен.

Нормативна регулатива треба да садржи следеће елементе:

- израду/опис особља и елемената материјала/ресурса укључених у систем заштите,
- обуку, додатно образовање, подстицање свести о потреби и неопходности заштите,
- процену ризика и њено руковођење,
- процену отпорности и издржљивости система у ванредним ситуацијама,
- регулисање начина заштите података и информација,

- политику сагласности, хоризонтално и вертикално у организацији,
- нормативно регулисање нивоа поверљивости,
- руковање поверљивих података и информација које је застарео,
- архивирање и складиштење,
- право на приступ првобитним информацијама,
- право дистрибуције, енкрипције, преноса и копирања информација,
- безбедносне елементи ТКИ система,
- заштиту особља,
- мере физичке и техничке заштите објеката, средстава и информација,
- превентивне и корективне мере,
- контролу спровођења мера заштите и
- санкције.

Имплементацијом ових и других регулаторних стандарда у систему управљања постигнуто је неколико циљева, а најважнији примарни циљ јесте да се у потпуности сачувају и одрже поверљивости информација или коришћења информација на прихватљивом нивоу ризика.

Мере

На бази анализе ризика, претњи и напада, а у складу са проклamованом политиком и принципима заштите, спроводе се и мере заштите ТКИ система и информација за чије је руковање и креиран наведени систем.

Мере заштите представљају скуп поступака и активности које предузимају појединци, организационе целине и топ менаџмент система одбране, а базиране су на методолошкој основи, искуствима из свакодневних активности, праћењу трендова у окружењу и широј заједници, ако и на глобалном плану.

Сажетак подела мера безбедности, које се не могу посматрати као одвојени, независни субјекти, биле би организационе, оперативно-тактичке и техничке мере заштите.

Комбинујући све ове облике доћи ће до потпуне имплементације мера које могу би бити угрожене од појединца или институције.

Физичка и техничка заштита – обухвата заштиту зграда, просторија и простора, бирајући најпогодније место за рад, инсталирање мера против упада, заштиту од пожара, видео-надзор и мере физичког обезбеђења. Значај ових мера је утолико већи ако се узме у обзир чињеница да су спроведене на информацијама у писаној форми – материјалном облику, као и у електронској форми.

Преузето са сајта еКапија

Заштита од угрожавајућег електромагнетног зрачења – примарни циљ је да се елиминишу сви паразитски сигнали и зрачења или да се смање на границу са контролом нивоа буке.

Криптозаштита – применом математичко-логичке трансформације спроведене код алгоритама и одговарајуће енкрипције и дешифровања штити се информације и преносе од читљивих до несхватљивих форми, што га чини доступним заинтересованим и само овлашћеним лицима. Овај облик заштите предмет је посебне научне дисциплине – криптологије.

Специјално обучено особље бави се праћењем развоја алгоритама широм света и уједно ствара своје криптографске методе и системе. Већина државних институција, као и приватни сектор, имају специјализоване тимове који се баве овом методом заштите.

Обезбеђивање компјутера, мобилних уређаја и рачунарских мрежа – предузимање свих радњи које штите поједине елементе и интерне или јавне мреже из свих угрожава фактора. Употреба лиценцираних софтвера, контрола приступа, заштита од вируса и вишеслојни систем архитектуре заштите мреже потребни су да би се избегао или смањио утицај фактора ризика. Ова ставка додатно је допуњена елементима као што су управљање корисничким налозима, откри-

вање илегалних активности, ротација запослених, смањење или укидање права приступа, заштита особља и континуирано ажурирање програма.

Заштита папирних носилаца и електронског (оптичког) складиштење података – иако се ова врста заштите може квалификовати као средство физичке заштите, због свог значаја, а истовремено имајући у виду чињеницу да количина информација у оптицају расте великом брзином, овом елементу треба посветити посебну пажњу, повезујући нове са класичним подношењем средстава складиштења.

Уништавање папира, хард-дискова и оптичких дискова – производи попут белешки, слика, видео-записа и других радних материјала, као и држање актуелних информација на различитим медијима, уништавају се након истека одређеног рока или нечије потребе за њима, у посебно одређеним локацијама, од физичког уништења, дробљења, уситњавања, паљења на високим температурама, претварањем у прах, тако да сваки траг информација која је постојала на медијима могу бити трајно уклоњени и уништени.

Спровођење мера заштите је право, дужност и одговорност управљања свих корисника који долазе у контакт са информацијама и било би прикладно да се на свим нивоима управљања формирају тимови ради заштите података и одржавања сајбер безбедност.

ОБРАЗОВАЊЕ И ОБУКА

Знајући да је сегмент заштите комплексан појам и нераскидиво везан за свакодневно функционисање, рад, рекреацију и заштиту виталних интереса државе, образовању и обуци – додатном оспособљавању у заштити информација се кроз перманентан процес приступа са више аспеката и на више начина и простора деловања.

Обука појединаца и тимова и неговање њихових вештина почело је у исто време када је порастао значај али и коришћење обраде, комуникације и преноса информација, чиме су приступ информацијама које су од значаја за одбрану и безбедност постале приступачне.

Први корак било би информисање о свим важећим прописима којима се регулишу питања и предмет поверљивости и заштите података и информација.

Ово је праћено процесом савладавања перцепције, психомоторних и друштвених вештина и навика, са фокусом на практичне мере у спровођењу заштите.

Поред едукације у институцијама система, неопходан је континуиран приступ на свим нивоима обуке и додатно образовање у реализацији постојећих решења и за стицање нових знања и вештина, који су доведени у вези са модернизацијом средстава манипулације информације.

Закључак

Ако је данас основно питање ко влада информација, а не ко влада капиталом, нужно се намеће потреба постојања адекватног и пуног предузимања мера њихове заштите.

Доступност хардвера и софтвера, ниска цена и релативно једноставно руковање омогућили су да је проток информација доживео геометријско прогресивни раст у последње време.

Поверљивост, интегритет и непорецивост података, нарочито кроз мрежни пренос од великог су значаја за појединца и државу у целини. Савремени ток обраде, преноса и складиштења података незамислив је без употребе информационих технологија, али то неминовно води ка проблему заштите података и информација.

У зависности од јачине одбрамбених и заштитних механизама, имплементиране мере спроводе се за заштиту информација и података на свим нивоима и у свим структурама.

Изазови и претње су свеприсутни и пролазе кроз промене, доживљавају метаморфозу, а чешће су испред развоја, свести и механизама за праћење технолошке заштите.

Људски фактор, као саставни део безбедности, заједно са техничким, обухвата компактну и чврсту јединицу.

Правни оквири, благовремено предузимање мера за заштиту, контролу, надзор и ревизију, као и обука особља непрекидан су задатак стручњака и менаџмента, као и сваког појединца.

Литература

1. S. Manzuik, K. Pfeil, Network Security Assessment – from Vunerability to Patch, Syngress, 2007
2. A. Partia, D. Andina, IT Security Management: IT Securiteers – Setting up an IT Security Function Springer Science + Business Media, 7818, 2010.

3. T. Grance, K. Kent, B. Kim, Computer Security Incident Handling Guide, NIST SP 800-61, January 2004
4. B. Rodić, G. Đorđević, Are you sure that you are safe? Produktivnost AD, Belgrade 2004
5. R. Ross, M. Swanson et al, Guide for the Security Certifiti on and on Accreditation of Federal Information Systems, NIST SP 800-37, publications, 2004
6. ИСО/ИЕЦ 27001:2005
7. ИСО/ИЕЦ 27032
8. М. Станковић, Н. Петровић, Н. Димитријевић, *Информациона безбедност и заштита тајних података у информационо-телекомуникационим системима*, „Нови гласник" 1/2016