DOI: 10.5937/vojdelo1906059T

ОБЛИЦИ И СУБЈЕКТИ УГРОЖАВАЊА ПОСЛОВНИХ ИНФОРМАЦИЈА У САЈБЕР ПРОСТОРУ

Дејан Н. Тепавац
Министарство одбране Републике Србије

Поуздане информације представљају основ смисленог људског деловања, успостављања међуљудских, међународних и пословних односа. Информације посебно добијају на значају са напретком информационо-комуникационих технологија и настајањем глобалних пословних мрежа, односно умрежавањем институција и присутношћу неког од видова информационо-комуникационих технологија у животу највећег дела људске популације.

Посебно место и улогу у свету информација имају пословне информације јер од њих зависи ефикасност функционисања информационо-комуникационог система (ИКС) националних држава, као и привредних субјеката. Појава великог броја пословних информација намеће следећа питања: како из мноштва информација извући потребне и корисне; како расположиве информације употребити тако да се постигне најбољи пословни резултат; како онемогућити злоупотребу информација и ИКС-а; и како заштитити информације и обезбедити сигуран и несметан рад ИКС-а.

Заштита пословних информација је активност која се реализује у циљу обезбеђивања несметаног и континуираног рада ИКС–а, сводећи ризике и претње на минимум. Заштита пословних информација представља заједнички задатак пословних субјеката и државних институција. Квалитетна заштита пословних информација, између осталог, подразумева стандардизацију информационе безбедности, а савремени стандарди који се данас употребљавају односе се на генерисање, пријем и чување података унутар ИКС-а.

Кључне речи: *пословне информације, информациона безбедност, информационо-комуникациони систем, заштита*

Увод

Заступљеност ИКТ-а у свакодневном животу савременог човека је досегла такав ниво да је готово незамисливо функционисање друштва без примене напредних технологија овог типа. Пракса је показала да напредне ИКТ-е поједностављују приватне и пословне обавезе човека, омогућавају бржу и лакшу комуникацију и податке чине доступним корисницима. Приступ таквим подацима је тиме омогућен и појединим лицима која немају поштене намере када је у питању експлоатација осетљивих информација.

Такве информације погодују неким криминалним, екстремистичким и терористичким организацијама у повоју, које још увек немају развијене механизме за обуку лица и довољно сазнања о тим областима. Данас постоји низ националних и међународних институција које се баве спречавањем и истрагама ове врсте криминала, који се најчешће назива високотехнолошким криминалом.

Да би се лакше схватио појам угрожавања пословних информација, неопходно је поћи од појма претње коју Путник дефинише на следећи начин: „Претња је, по природи, апстрактан концепт – она је нешто што има потенцијал да стави једну организацију, особу или друштво у ризичну ситуацију. Претња је могућност да се оствари нежељени догађај. Када се ова могућност актуализује, она престаје да буде претња и постаје догађај попут других. У тренутку када је претњу уочио надлежни ауторитет или менаџмент она постаје део ризика, те као таква предмет расподеле њиховог времена и расположивих ресурса (људских, техничких, финансијских итд.) ради супротстављања“.[1]

ИКС су данас основа за пословање великих пословних система, у којима менаџмент захваљујући квалитетним корисничким програмима, анализама, пресецима и проценама, долази до употребљивих информација на основу којих доноси стратешке одлуке. О значају информационих технологија сведоче активности надлежних државних органа који се односе на увођење е-управе, што представља једну од ставки Стратегије развоја информационог друштва у Републици Србији до 2020. године.[2]

Данас је грађанима омогућено школовање употребом ИКТ, подизање докумената, заказивање прегледа у здравственим установама, комуникација са јавним службама и установама. С друге стране, захваљујући техничким достигнућима, лицима са штетним намерама, омогућено је лакше фалсификовање службених докумената и исправа, као и друге врсте манипулација када је у питању електронско пословање. Војни ИКС, системи државне управе, системи за контролу ваздушног и железничког саобраћаја, снабдевање гасом, водом, електроенергијом, врло су атрактивни уносни циљеви. Како се заштитити од тешко предвидљивих извршилаца напада као што су: незадовољни грађани, разочаран персонал, терористи, непријатељске државе или, пак, верски фанатици? Ако имамо на уму да им на располагању стоје сателитски линкови, савремени компјутери и велики избор разноврсних мета (компјутерски системи: аеродрома, болница, саобраћајне сигнализације, банака, нуклеарних погона и оружја) схватићемо колико решавање овог проблема представља велики изазов.[3]

Често се под информационим системима подразумевају само техничка средства (рачунари и системи преноса информација на даљину и сл.), међутим, потребно је уврстити и људе који их користе и опслужују, као и физички простор у којем се информације размењују и касније анализирају.

Недовољно дефинисана законска регулатива која се односи на заштиту информационих система је погодно тле за противзаконито деловање злонамерних организација и појединаца који својим деловањем угрожавају поједине сегменте националне безбедности, али исто тако и личну безбедност грађана.

---

[1] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 62.

[2] Видети више на: (http://www.gs.gov.rs/lat/strategije-vs.html, 2015, 12. април)

[3] Ђорђевић, И. (2007). *Безбедносна архитектура у условима* глобализације. Београд: Службени гласник РС, Факултет безбедности.

Одређење појма „cyber криминал“

Једна од најизраженијих и најчешћих злонамерних активности јесте коришћење интернета за спровођење криминалних радњи као што су трговина људима, продаја дроге, вршење превара, обављање финансијских превара крађом идентитета и слично. Овај облик криминала се у литератури назива високотехнолошки или сајбер (енгл. cyber) криминал.

Један од међународних докумената који дефинише категорије сајбер криминала је Европска конвенција о сајбер криминалу.[4] Карактеристична дела која могу да се доведу у контекст рада су:

– Дела против поверљивости, интегритета и доступности компјутерских података и система (незаконити приступ, пресретање, уплитање у податке или системе, коришћење уређаја, програма, лозинки);

– Дела везана за компјутере код којих су фалсификовање и крађе најтипичнији облици напада;

– Дела везана за кршење ауторских и сродних права обухватају репродуковање и дистрибуцију неауторизованих примерака дела компјутерским системима.

UNDOC-ова обимна студија о компјутерском криминалу (енгл. Comperhensive Study on Cybercrime) из 2013. године, четрнаест дела групише у три категорије:[5]

– Дела против поверљивости, интегритета и доступности компјутерских података или система код којих је најзаступљенији незаконити приступ компјутерском систему; незаконити приступ, пресретање или стицање компјутерских података; незаконито ометање компјутерског система или компјутерских података; производња, дистрибуција или поседовање алата за злоупотребе рачунара и кршење приватности или мера за заштиту података;

– Дела везана за компјутере ради личне или финансијске користи или штете какви су превара или фалсификат; дела везана за идентитет; кршење ауторских права или права на жиг; слање или контролисање слања ”spam“ порука.

– Дела везана за компјутерске садржаје, а односе се на говор мржње, дистрибуцију или поседовање дечје порнографије или за подршку тероризму.

Класификација cyber криминала домаћих аутора Дракулића указује на следеће категорије:[6]

– Политички: cyber шпијунажа, хакинг, cyber саботажа, cyber тероризам, cyber ратовање;

– Економски: cyber преваре, хакинг, крађа интернет услуга и времена, пиратство софтвера, микрочипова и база података, cyber индустријска шпијунажа, преварне интернет акције (неиспоручивање производа, лажна презентација производа, лажна процена, надграђивање цене производа, удруживање ради постизања веће цене, трговина робом са црног тржишта, вишеструке личности);

[4] http://www.coe.int/sr_RS/web/conventions/, 2016, 3. јул

[5] https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, 2016, 3. јул)

[6] Дракулић, М. и Дракулић, Р. (2014). Cyber криминал. *Везе Cyber криминала са иррегуларном миграцијом и трговином људима*, *XII*, 365–386.

– Производња и дистрибуција недозвољених и штетних садржаја: дечја порнографија, педофилија, ширење ставова верских секти, ширење расистичких, нацистичких и сличних идеја и ставова, злоупотреба жена;

– Манипулација (трговина, дистрибуција и слично) забрањеним производима, супстанцама и робама: дрогом, људима и децом, људским органима, оружјем;

– Повреда cyber приватности: надгледање е–поште, spam, phishing, крађа идентитета, прислушкивање, снимање chat rooms,[7] праћење е–конференција, приказивање и анализа cookies.[8]

Облици и извори угрожавања пословних информација

Корисници пословних информација улажу планске и организоване напоре с циљем да их оптимално и ефикасно заштите од лица (појединаца) и колективитета који настоје и покушавају да их сазнају. Реч је о непрекидном, двостраном процесу који треба да резултује регистровањем чињеница, односно да да одговор на питања ко, како и зашто може да угрози пословне информације. Сазнате чињенице се користе за планирање и реализовање њихове заштите. Расположива сазнања указују на следеће карактеристичне облике и изворе угрожавања пословних информација у сајбер простору:

– Сајбер напади техничког типа

– Сајбер напади уз коришћење обмане

– Злоупотреба сајбер простора као средства масовне комуникације

– Субјекти претњи у сајбер простору

Повезивање рачунара са серверима (рачунарима великог капацитета) на којима се чувају резервне копије података представља један од облика ризика у сајбер простору. У случају губитка података информације се могу реконструисати са резервних медијума чиме се обезбеђује ефикасност, економичност и поузданост рада пословног субјекта. Да би се повећала ефикасност запослених, врши се повезивање рачунара на интернет чиме се омогућује међусобна комуникација запослених са удаљених локација, комуникација са другим компанијама и омогућује се пренос важних података и пословних информација. Међутим, потребно је имати у виду да овај процес може бити угрожен на различите начине. У том смислу пословни субјект предузима све мере како би открио, контролисао и, у што већој мери, ублажио утицај могућих ризика. Интернет пружа брз и прилично јефтин начин за обављање послова и пренос информација. Ипак, тај процес може бити поремећен на различите начине, тако што ће подаци бити украдени, измењени, уништени. У циљу анализе постављене теме са аспекта могућности отицања заштићених информација, по-

[7] *Соба за чет* (енгл. chat – онлине интерактивна комуникација између сурфера) – Помоћу чета је могућа комуникација са људима који се налазе у истом chat room–у, с тим што је много уобичајенија комуникација дописивањем, тј. куцањем преко тастатуре, него директна комуникација говором, помоћу микрофона и слушалица. (http://bezbednostdecenanetu.weebly.com/105610771095108510801082-104810851077108810851077109010871086111210841086107410 72.html, 2016, 3. јул).

[8] *Колачић* (енгл. Cookie) – метод који у софтверу служи за прикупљање информација о лицима која посећују неку Web локацију да не би посетилац морао да се региструје сваки пут приликом посете. (Тасић В. и Бауер, И. (2004). *Речник компјутерских термина*. Београд: Микро књига)

требно је извршити анализу ИКС у којима се рачунари повезују са серверима.[9] Конфигурисањем приступа интернету, омогућује се комуникација са другим рачунарима и пренос података у оба смера, што представља посебну претњу за сервере, посебно уколико нису заштићени одговарајућим рачунарским програмима. Узимајући у обзир да је интернет мрежа која наводно „нема власника", иако је познато да су поједине државе и институције власници делова комуникационих канала, проблем отицања заштићених информација додатно долази до изражаја.[10]

Да би се лакше разумело које су то најосетљивије тачке криминалног понашања корисника ИКС-а, потребно је нагласити да постоје следећи нивои рачунарских примена: прикупљање и пренос података, складиштење података, аутоматска обрада података, дијагностика стања и доношење одлука, управљање и контрола, истраживање и развој.

Информациони криминал представља противзаконито понашање група и појединаца чији су основни циљеви деловања везани за недозвољени приступ информацијама о појединцу, организацијама или институцијама. Потребно је нагласити да се понекад изједначавају појмови *информациони* и *компјутерски криминал*. Информациони криминал представља шири појам од компјутерског криминала. Компјутерски криминал подразумева да је компјутер средство којим је извршена противзаконита делатност прикупљања информација, што у случају информационог криминала не мора да буде случај. С обзиром на то да се у Републици Србији ова врста криминала у званичним институцијама дефинише као високотехнолошки, јасно је да су и извршиоци такве врсте криминалних активности образована и едукована лица из области ИКТ-а, па је самим тим доказивање и сузбијање ове врсте делатности сложен поступак. Код појединих аутора појављује се и термин *cyber криминал*.[11]

Да би се смањио ризик потребно је идентификовати потенцијалне претње и рањиве тачке у ИКС-у. Претња по безбедност информација је свака активност која представља опасност за поверљивост, интегритет, или расположивост података. Слаба тачка је пропуст у заштити информација. Терминолошки, безбедност информација подразумева: поверљивост (обезбеђује да само овлашћено особље има приступ информацијама), интегритет (обезбеђује да само овлашћено особље модификује податке), расположивост (обезбеђује овлашћеном особљу приступ информацијама и системима кад год је то потребно).

Контрола ризика при употреби ИКТ-а постиже се утврђивањем и вредновањем ризика, откривањем извора претњи и рањивих тачака и предузимањем мера да се ризици потпуно отклоне или сведу на минимум. Ризик је изложеност губитку или могућем оштећењу. Када говоримо о безбедности информација, под ризиком подразумевамо могућност да спољни фактори угрозе податке, што би проузроковало губитак времена, новца и репутације. Претња се дефинише као свака активност која представља могућу опасност по информације. Слаба тачка одређена је као пропуст у заштити информација односно безбедности система, мреже, процесима и процедурама.[12]

---

[9] У области информационих технологија сервер је рачунарски систем који пружа услуге другим рачунарским системима – клијентима. Комуникација између сервера и клијента одвија се преко рачунарске мреже.

[10] Џигурски, О. (2002). Информатика. Београд: Факултет цивилне одбране, стр. 117.

[11] Дракулић, М. и Дракулић, Р. (2010). Европска перспектива регулисања интернет услуга: изазов традиционалном европском праву. *Телекомуникације*, *6*, 49–63.

[12] Кукрика, М. (2002). *Мала енциклопедија квалитета – Управљање сигурношћу информација*. Београд: Текон системи, стр. 81-82.

Унутрашње тачке упада представљају најчешће системи који нису у обезбеђеној просторији и којима није конфигурисана локална заштита. Спољашње тачке приступа представљају компоненте које повезују пословне субјекте са интернетом, апликације које се користе за комуникацију преко интернета и комуникациони протоколи. Мрежну структуру чине каблови, мрежни уређаји и мрежни сервиси који омогућавају повезивање рачунара. Ова структура омогућава и повезивање са интернетом и прикључивање удаљених рачунара изван компаније. Тачке упада су места преко којих је могуће прикључење и продор у мрежну инфраструктуру и приступ информацијама. Спољашњи упад је могућ кроз везу са интернетом извођењем *DoS* напада или испробавањем корисниковог имена и лозинке који би омогућио пролаз кроз проверу аутентичности. Унутрашњи напад могао би потећи од неког запосленог који може да се повеже преко отвореног мрежног прикључка и покуша да приступи заједничким ресурсима који не захтевају лозинку.[13] Апликације које се користе за приступ интернету, такође могу представљати тачку упада. Спољашњи напад може се реализовати убацивањем вируса или паразитских програма преко *e*-поште. Отварањем ове поште, вирус може да зарази систем или да омогући нападачу контролу система. Напад изнутра могућ је преко помоћних програма оперативног система, који служе за повезивања са другим системима на интерној компанијској мрежи и који за приступ не захтевају корисничко име и лозинку. Могућа је и злоупотреба апликација као што је *web* претраживач за приступ поверљивим информацијама са ограниченом безбедношћу приступа.[14]

Интернет и друштвене мреже који су рањиви и несигурни због огромног броја корисника, отворености и нерегуларности, идеално су скровиште криминалцима различитог типа, којима је потребно друштво, као што им је неопходна и „публика“. Лакоћа „вршљања“ сајбер простором даје им осећај моћи и неухватљивости.[15]

Путник прави следећу класификацију претњи у сајбер простору:

– Сајбер напади

– Сајбер напади уз коришћење обмане (социјални инжењеринг и сајбер напади техничког типа и фишинг)

– Сајбер напади техничког типа (напади помоћу малициозних програма – malwer, напади усмерени на опструкцију услуга – Denial of Service или Distributed Denial of Service)

– Злоупотреба сајбер простора као средства масовне комуникације

– Информационо ратовање

– Пропаганда

– Психолошки рат

– Обавештајна делатност.[16]

[13] Ruth, A. & Hudson, K. (2004). *Сертификат Security+, Microsoft* Corporation. Чачак: Светлост, стр. 13.

[14] Ruth, A. & Hudson, K. (2004). *Сертификат Security+, Microsoft* Corporation. Чачак: Светлост, стр. 21.

[15] Урошевић, В. (2014). *Везе cyber криминала са иregуларном миграцијом и трговином људима*. Београд: МУП Републике Србије, стр. 175.

[16] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 73.

Сајбер напади техничког типа

Врсте угрожавања у сајбер простору би се могле поделити у две категорије. Прву категорију представљају случајне или ненамерне грешке настале креирањем неког програмског пакета, које употребом од стране корисника обезбеђују неовлашћеним лицима приступ заштићеним информацијама. Други, чешћи облик угрожавања представља смишљено састављени програми за наношење штете у ИКС као што су malweri[17] (вируси, црви (енгл. worms), тројански коњи, споредна врата), рекламирање без сагласности корисника (енгл. adwer), ботови, отмичари, шпијуни (енгл. spyware) и слично. Најчешће се пажња усмерава ка претњама које долазе из окружења и сматрају се могућим, док оне које се јављају унутар система врло често бивају занемарене.

Вирус (енгл. virus) је било који програм који зарази извршне датотеке и при њиховом покретању преноси се на друге извршне датотеке и извршава неке штетне акције. Термин ***вирус*** у информатичком смислу је први употребио Фред Коен (Fred Cohen) у чланку објављеном 1984. године под насловом „Експерименти у рачунарским вирусима".

Неки вируси, поред сопствене репродукције, садрже још две компоненте:

– Функцију активације која садржи основне критеријуме на основу којих вирус „одлучује" да ли да изврши напад;

– Једну или више додатних функција које се састоје од редоследа инструкција за наношење штете систему у виду брисања датотека или диска, приказивања нежељених порука на екрану итд.[18]

Тројански коњ (енгл. trojan horse) представља злонамерни програм који се маскира као користан, а онда се прикачи на неки други користан програм и на тај начин нападачу шаље информације о корисничким лозинкама, банковним рачунима и другим подацима до којих нападач настоји да дође. У неким земљама, као што је САД и Аустралија, тројански коњи се користе и за потребе полиције, наравно уз одобрење суда, те се на тај начин прикупљају информације о потенцијалним извршиоцима кривичних дела из области високо-технолошког криминала. Ова врста програма се шири и ажурира инсталацијом комерцијалних оперативних система или преко даваоца интернет услуга. Даваоци интернет услуга су у обавези да на захтев надлежних државних служби безбедности, а уз сагласност суда, обезбеде надлежним органима приступ и инсталацију таквих врста података.

Црви (енгл. worms) су програми или кодови који користе сигурносне пропусте у програмима или у оперативном систему да би се ширили и извршавали путем мреже. Црв је самокопирајући рачунарски програм који користи мрежу за слање сопствених копија на остале рачунаре унутар неке мреже, без интервенције корисника. Чини штету на мрежи тако што је успорава. За дистрибуцију ове врсте програма најчешће се користи електронска пошта.

[17] Назив је добијен од речи *malicious* и *software.*

[18] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 75 -76.

Споредна врата (енгл. backdoor) је програм који се најчешће у рачунару шири комбинацијом са тројанским коњем или црвом. Један од примера споредних врата представља *споредна рупа* који активира улаз у систем у који се инсталира, дајући могућност контроле система познаваоцу IP адресе. Споредна врата је дакле програм који омогућава комплетно заобилажење сигурносне процедуре у одређеном систему.

Следећи програми се употребљавају у активностима *неауторизованог праћења активности корисника*:

Adware је програм који без дозволе корисника приказује рекламе на његовом рачунару доносећи аутору приходе од сваке рекламе. Могу бити инсталирани на разне начине, а најчешће као тројанци или црви.

Spyware је злонамерни програм који скупља информације о кориснику и начину како користи рачунар. Дистрибуирају се као тројанци или црви. *Spyware* може да прати које „*web* сајтове" корисник посећује, електронску пошту коју шаље, или да бележи откуцане карактере на тастатури откривајући тако шифре или личне податке корисника. Сакупљени подаци се могу пренети до централног рачунара и злоупотребити. Врло често се налазе у саставу бесплатних програма, а најчешће бесплатних игара које се инсталацијом уносе у рачунар, и при том шаљу информације о коришћењу интернета неког корисника и слично.

Spam је нежељена пошта. Најчешће су у питању *spam* рекламне поруке чијим слањем спамери зарађују. Негативни ефекат је губитак радног времена на читање и брисање ових порука из inbox–а. Spam поруке су везане и за крађу идентитета јер се шаљу у име недужне особе или компаније.

Лишавање услуге (DoS) и *дистрибуирано лишавање услуге* (DDOS) су напади који имају циљ да онемогуће клијенте да користе рачунарске услуге, рачунарске мреже[19] и информационе ресурсе. Опструкција се реализује нападом на системе који омогућавају наведену услуге (нпр. сервер електронске поште). Напади се односе на део о доступности информација, а не на њихову поверљивост или садржај. Сајбер напади су усмерени на деструкцију, то јест лишавање услуга корисника тако што нападе извршавају на делове система који те услуге обезбеђују, као што су сервери. Такви напади могу да проузрокују озбиљне штете и последице по функционисање државног система, на последице које се односе на нарушавање имиџа националне државе, као и ширење страха међу њеним грађанима. Слична је ситуација и са појединим пословним субјектима, који трпе огромне економске губитке блокадом сајтова и сервера чији је задатак несметано обезбеђивање функционалности пословања. Сам начин напада изводи се тако што нападач успоставља у првој

[19] Рачунарска мрежа је скуп рачунара повезаних одговарајућом комуникационом опремом. Она омогућава да рачунари у мрежи међусобно комуницирају, односно да размењују податке. На тај начин се омогућава да се одређени рачунарски ресурси (подаци, програми, рачунарско време, периферијски уређаји итд.), лоцирани на рачунарима повезаним у мрежу, ставе на располагање свим корисницима мреже. Главне компоненте рачунарске мреже су комуникациони медијум, комуникациони уређаји, комуникациони протоколи и командни софтвер. То се постиже нападом на системе који омогућују ову врсту услуга (сервер са ускладиштеним *web*-сајтовима или сервер електронске поште). Нападом је угрожена доступност информација, а не њихова поверљивост. Један од начина извођења напада је генерисање великог броја захтева у краткој јединици времена. Потенцијална последица је губитак времена потребног за оспособљавање система, што посредно може узроковати и економске последице.

фази контролу над првим рачунаром који постаје „мастер“ напада. Преко овог рачунара инфицирају се други рачунари који се називају „зомбији“. Ефекат се постиже оног момента када зомби рачунар извршава сваку радњу коју нападач задаје неком врстом malwera, најчешће црвом, преко мастера, а да при том корисник није ни свестан шта се дешава. „Зомби рачунар се може испрограмирати тако да омогући отварање споредних врата унутар локалне мреже пословног субјекта, односно организације којој рачунар припада и на тај начин, депласира све примењене безбедносне мере организације.“[20]

Компаније у свету издвајају десетине милијарди долара за заштиту од програма као што су malweri који корисницима одузимају радно време и на тај начин смањују продуктивност рада тих компанија. Према речима Џона Стјуарта (John Stuart), шефа одељења за безбедност података у компанији *Cisco*, безбедност информација није више само борба против вируса и *spam*-а. Данас, покушај да се обезбеде послови, лични идентитет, па и саме државе, захтева већи ниво координације између страна које у прошлости нису заједно сарађивале онолико колико је било потребно. Да ли ће национална, лична безбедност, као и безбедност компанија бити на високом нивоу, зависиће само од сарадње и комуникације између ових страна.[21]

Сајбер напади уз коришћење обмане

Неки од најизраженијих облика *сајбер напада уз коришћење обмане* су:

Мрежна крађа идентитета – Фишинг (енгл. Phishing) користи се за описивање илегалног прикупљања осетљивих информација обманом (бројеви кредитних картица, корисничка имена, лозинке, PIN кодови и слично), при којој се нападач представља као неко вредан поверења и као неко ко има право и потребу за таквом врстом података (нпр. лажне поруке наводно послате из банке или друге финансијске организације).[22] *Фишинг* поруке могуће је препознавати по томе што се у поруци траже лични подаци, инсистира се на хитности, линкови су лажирани, тело (body) електронске поруке је најчешће слика, пружају се нереална обећања и сл. Спровођење *Фишинг* напада врши се коришћењем различитих техника, маскирање URL адреса, пресретање комуникације, пропусти у *web*-апликацијама, лажиране HTML email поруке. Заштита од *phishing* напада подразумева едукацију корисника, снажну аутентификацију корисника, обраћање пажње на сигурност при развоју web-апликација, сигурност email корисника, дигитални потпис порука електронске поште.[23]

Термин *социјални* (*друштвени*) *инжењеринг* се употребљава у случају поступка заобилажења разних врста заштита, одавањем лозинки или других поверљивих информација које њихови власници свесно или несвесно одају нападачу. *Социјални инжењеринг* означава врсту напада при којој се нападач не служи информатичким тех-

[20] Петковић, Т. (2009). *Пословна шпијунажа и економско ратовање*. Нови Сад: Protexi Group System, стр. 293- 295.

[21] Петковић, Т. (2009). *Пословна шпијунажа и економско ратовање*. Нови Сад: Protexi Group System.

[22] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 89

[23] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 85 - 86.

никама, већ путем комуникација наводи жртву да учини безбедносне пропусте и прекрши норме и процедуре, а да не примети да је изманипулисана. Нападачи користе разне технике које у великом броју случајева постају изузетно ефикасне. До изражаја долази вештина нападача да, у наизглед необавезном разговору, дођу до таквих информација које им обезбеђују пробијање постављених механизама заштите.

Социјални инжењеринг припада скупу напада на рачунарске системе, али и на системе у ширем смислу речи. Он се најједноставније може дефинисати као умеће навођења других особа да поступају према жељама нападача. Ради се о начину стицања информација и података до којих нападач легитимним путем не би могао доћи. Односи се и на прибављање бројева кредитних картица и PIN бројева у сврху *on-line* плаћања туђим картицама. При томе се не искоришћавају слабости и недостаци техничких система, већ се напад усмерава на најслабију карику целокупног ланца у систему безбедности – на људски фактор. У суштини, ради се о психолошкој игри, у којој нападач покушава да злоупотреби неко од шест основних правила људског понашања: ауторитет, склоност, узвраћање, доследност, друштвена неоспорност, реткост.[24] Најчешће методе преваре које се користе у социјалном инжењерингу су уверавање (које се сматра најважнијим предусловом), лажно представљање, стварање одговарајуће ситуације, искоришћавање моралне одговорности, жеља за помагањем и коришћење старих веза из пословних контаката.

Злоупотреба сајбер простора као средства масовне комуникације

Један од најчешћих облика злоупотребе сајбер простора представља информационо ратовање. У циљу бољег разумевања овог појма, потребно је дефинисати и направити разлику између појмова као што је информационо ратовање, информатички рат, сајбер рат и мрежни рат. Информационо ратовање обухвата правне и дипломатске мере, пропаганду, психолошке кампање, политичке и културне субверзије, уплитање у локалне медије, активности на промоцији дисидентских и/или опозиционих покрета преко ИС.

„Информатички рат је само једна компонента информационог ратовања која се своди само на његов технички аспект, коришћење технике ради реализације циљева унутар информатичке структуре непријатеља. Разлика између информатичког и информационог ратовања је онај квалитет који се може обухватити појмом социјални инжењеринг, односно употреба информационе структуре за промену свести припадника нападнутог ентитета.“[25] Информатичко ратовање може да се дефинише као „акције које се предузимају у циљу постизања информационе предности као подршке војној стратегији, деловањем на непријатељске информације и информационе системе, при томе штитећи своје информације и информационе системе.“[26]

Сајбер рат подразумева прикупљање информација о информационом систему непријатеља како би се његови ИС–и делимично или у потпуности елиминисали.

[24] Cialdini, R. B. (2009). *Influence: Science and practice (Vol. 4)*. Boston: Pearson Education.

[25] Ђорђевић, И. (2007). *Безбедносна архитектура у условима* глобализације. Београд: Службени гласник РС, Факултет безбедности, стр. 83.

[26] Џигурски, О. (2002). Информатика. Београд: Факултет цивилне одбране, стр. 143.

Мрежни рат представља сукобе ниског интензитета који значе намеру да се онемогући, оштети или промени оно што циљна популација зна о себи или мисли да зна о себи и свету у коме живи.

О важности информационог простора сведоче актуелне војне доктрине које информациони простор третирају као пети борбени амбијент, паралелно са копном, водом, ваздухом и космосом.[27] Потребно је нагласити да информатички рат и информационо ратовање не подразумевају искључиво уништавање информационих система непријатеља него и заштиту сопствених информационих система, што укупној војној стратегији даје предност у решавању сукоба. Дакле информационо ратовање представља сегменат подршке свеукупној војној стратегији тако што спровођењем информационих активности слабе непријатеља, а сопственим снагама дају предност у домену спровођења војних активности, како у рату, тако и у миру. Инфомрациони рат се примењује и у сферама економије, политике и културе, чему је погодовао развој интернета. Као и физички, сајбер простор такође припада ономе ко га се први домогне. Како би стратегије успостављања контроле над интернетом биле успешне потребно је да се усвоје следеће максиме:

– загосподарити каналима за проток информација,

– емитовати у највећој могућој мери властите погледе и ставове са циљем њиховог наметања,

– непрекидно усавршавати методе и средства за обраду информација.[28]

Следећу врсту злоупотребе сајбер простора представља *сајбер тероризам* и он се односи на пропаганду и психолошки рат. За сајбер тероризам погодно је деловање у областима као што су хемијска, прехрамбена, фармацеутска индустрија, водоснабдевање, нуклеарни програми, енергетска делатност.[29] Циљеви сајбер терориста усмерени су на нарушавање безбедности живота и имовине грађана као и основних субјеката који обезбеђују нормално функционисање друштва. Ефекти који се постижу спровођењем сајбер тероризма су ширење страха, панике и насиља. Предност у односу на класични тероризам је географска покривеност и могућност брзог деловања готово у свим деловима света.

Путем сајбер простора терористи теже да допру до три аудиторијума:

– постојећих и потенцијалних бораца и подржавалаца,

– међународног јавног мњења које није директно укључено у конфликт, али је заинтересовано за његове кључне елементе,

– непријатељске или противничке јавности.[30]

Терористичке организације деловањем у различитим друштвеним делатностима могу да проузрокују штете великих размера, што може да угрози животе више стотина и хиљада људи. Хемијски акциденти, намерно изазвани, могу да проузрокују загађења у животној средини и да негативно утичу на безбедност грађана који насељавају таква подручја будући да изазивају штетне утицаје по здравље становништва и негативне импликација на квалитет и исправност пољопривредних произ-

[27] Џигурски, О. (2002). Информатика. Београд: Факултет цивилне одбране, стр. 141.

[28] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 97.

[29] Ђорђевић, И. (2007). *Безбедносна архитектура у условима* глобализације. Београд: Службени гласник РС, Факултет безбедности, стр. 82-84.

[30] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 105.

вода који се користе у исхрани. Постигнути ефекти могу да буду краткорочни и дугорочни. Циљеви које терористичке организације настоје да постигну су брзи, краткорочни и ефикасни и иду ка томе да степен страха и незадовољства достигну максимум, како би утицај на опстанак владајуће структуре био што ефикаснији. Пласирање разних врста дезинформација о деловању терористичких група на територији неке државе, затим блокада и „рушење" сајтова важнијих државних органа и управа, представља такође једну врсту cyber тероризма која у одређеној мери постиже ефекат страха и несигурности код грађана те националне државе или бар неког њеног дела. Трећи аспект cyber терористичког деловања у сајбер простору представља прикупљање и пласирање информација путем интернета о изради смртоносног оружја које ће у каснијој фази бити примењено у терористичке сврхе. На разним интернет порталима постоје читава упутства о начину израде експлозивних направа којима је могуће угрозити животе и безбедност грађана циљане државе у већим размерама.[31] Овде се у суштини ради о потребној логистичкој подршци сајбер тероризму коју терористи спроводе путем интернета, како би се створили услови за извођење терористичког акта. Као и у претходним ситуацијама које се односе на шпијунажу или криминално деловање корисника информационих система, у спровођењу ове врсте недозвољене активности, терористима посао олакшавају лица која се налазе унутар система, а спремни су да, услед неких разлога (нпр. верски фундаментализам) или уцена на сарадњу, помажу таквим организацијама.

Терористичке организације користе сајбер простор такође за регрутовање и обуку потенцијалних терориста путем интернета. Поједини web-сајтови и форуми приказују елементе обуке, снимке из актуелних сукоба, борилачке вештине и слично. Поред наведене намене, интернет се често користи за прикупљање новчаних фондова потребних за финансирање активности терористичких организација. Размена информација међу терористичким организацијама и појединцима је такође развојем интернета једноставнија, теже се открива, а применом одговарајућих заштитних мера гарантује готово потпуну конспиративност. [32]

Субјекти претњи у сајбер простору

Хакерски напади представљају продор у ИС корисника са намером манипулисања и прибављања заштићених података и информација, пословних тајни и других поверљивих података.

„*Хакер* је особа која ствара изван стандардних техничких лимита, користећи сопствене вештине, са циљем да надмудри и креативно превазиђе ограничења која му се намећу, не само у пољима његових интересовања (која се могу сврстати под информационе технологије) већ и у свим осталим аспектима живота."[33] Хакери који искључи-

[31] У Ослу (Норвешка), 2011. године извршен је напад на зграду Владе у којем је погинуло седморо људи, бомбом направљеном од вештачког ђубрива. Сличан напад се догодио 1995. године у Оклахоми у којем је страдало 168 жртава. (http://www.politika.rs/vesti/najnovije-vesti/Bomba-u-Oslu-napravljena-od-vestackog-djubriva-i-dizela.lt.html, 2016, 4. март)

[32] Пласирање скривених порука, мигрирање сајтова, паразитски сајтови.

[33] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности, стр. 121.

во за себе желе да остваре себичне интересе и на тај начин да дођу до новца и других врста користи, називају се *крекери*. Они нелегално користе информационе системе и наносе штету рачунарском систему жртве. У ову категорију се могу сврстати сви они чија се активност описује као декадентна, усмерена на ширење болесних идеја и погледа (националне, расне, верске и друге нетрпељивости и мржње), уцењивање, преваре, лажна обећања, трафикинг, дроге и на рушење друштвеног система и општеприхваћених вредности. *Хактивисти* се користе истим методама и техникама као и хакери, међутим циљеви које они спроводе односе се на привлачење пажње јавности на неки политички, социјални и проблем друге врсте. Нападом на „web сајт", хактивисти мењају његов садржај, најчешће насловну страну, као доказ да су били присутни, а често га и блокирају. *Инсајдери*, у најширем смислу представљају злонамерне актере који дејствују прикривено унутар и против организације чији су део. Мотиви за спровођење злонамерне активности могу да буду: различит систем вредности у односу на радну организацију у којој су запослени, радозналост, освета, изнуда, уцена.

Сајбер простор и ИКТ су постали окосница диверзификације криминалних дела и инструменти који криминалним организацијама омогућавају бољу оперативну ефикасност. Тежња за илегалним стицањем профита представља суштински мотив за профил сајбер криминалца у односу на профил хакера, који је мотивисан најчешће славом, забавом или злобом.

Закључак

Нагли развој ИКТ-а довео је до нових видова комуникације и размене података који се суштински разликују у односу на до тада разрађен традиционални систем. У циљу регулисања међусобних права и обавеза дошло је до усклађивања докумената, процедура, правила између учесника комуникационог процеса, што је захтевало професионалан кадар, квалитетну организацију пословних процеса и примену савремених технологија. ИКТ-е у савременом свету врло брзо постају незаобилазна компонента у савременим друштвеним токовима у готово свим областима људског живота. Паралелно са развојем ИКТ-а развијају се и злонамерне активности лица и организација које настоје да их угрозе. У циљу супротстављања таквим намерама, пословни субјекти примењују све расположиве мере заштите информација које се спроводе у циљу превентивног деловања и спречавања случајног или намерног негативног утицаја на рад ИКС-а и злоупотребе информација. Дефинисањем облика угрожавања пословних информација које се налазе у оквиру ИКС-а и формулисањем конкретних мера које ће се предузимати у циљу спречавања неовлашћених лица да дођу до заштићених информација, наведена активност се конкретизује и унапређује. Проблем посебно долази до изражаја у случају нарушавања ИКС-а значајних за свеопште функционисање друштва, које може да доведе до катастрофалних последица по целу друштвену заједницу, а у неким случајевима и по међународно окружење. У циљу безбедносне заштите ИКС-а, потребно је константно деловати у правцу супротстављања свим облицима угрожавања, чиме се заштита ИКС-а доводи на прихватљив ниво. Неопходно је истаћи да се заштита задржава на прихватљивом нивоу, а не апсолутном, пошто апсолутна заштита, узимајући у обзир претходна искуства о облицима угрожавања ИКС-а, не постоји.

Литература

[1] Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности.

[2] Ђорђевић, И. (2007). *Безбедносна архитектура у условима* глобализације. Београд: Службени гласник РС, Факултет безбедности.

[3] Дракулић, М. и Дракулић, Р. (2014). Cyber криминал. *Везе Cyber криминала са иregуларном миграцијом и трговином људима*, *XII*.

[4] Џигурски, О. (2002). Информатика. Београд: Факултет цивилне одбране.

[5] Дракулић, М. и Дракулић, Р. (2010). Европска перспектива регулисања интернет услуга: изазов традиционалном европском праву. *Телекомуникације*, *6*.

[6] Кукрика, М. (2002). *Мала енциклопедија квалитета – Управљање сигурношћу информација*. Београд: Текон системи.

[7] Ruth, A. & Hudson, K. (2004). *Сертификат Security+, Microsoft* Corporation. Чачак: Светлост.

[8] Урошевић, В. (2014). *Везе cyber криминала са иregуларном миграцијом и трговином људима*. Београд: МУП Републике Србије.

[9] Петковић, Т. (2009). *Пословна шпијунажа и економско ратовање*. Нови Сад: Protexi Group System.

[10] Cialdini, R. B. (2009). *Influence: Science and practice (Vol. 4)*. Boston: Pearson Education.

[11] Тепавац, Д. (2018). *Заштита пословних информација у функцији националне безбедности,* Докторска дисертација.

Интернет извори:

[12] http://www.gs.gov.rs/lat/strategije-vs.html

[13] [1] http://www20.coe.int/sr_RS/web/conventions/

[14] https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf,

[15] http://bezbednostdecenanetu.weebly.com/105610771095108510801082-104810851077108810851077109 0-108710861112108410861074 1072.html