Доц. др Видоје Спасић
Правни факултет Универзитета у Нишу

UDK: 004.738.5:347.78

ОНЛАЈН БЕЗБЕДНОСТ

Апстракт: *Развој информатичке технологије, а нарочито интернета донео је човеку многе погодности. Међутим, дигитална технологија и мрежно окружење носе и бројне ризике. Ово због тога, јер је интернет отворена мрежа без централизованог система управљања, па је њена рањивост евидентна. Бројни су начини на које различити субјекти, споља или изнутра, могу угрозити безбедност на интернету. Пре свега, на удару су приватни подаци, интелектуална својина и други ресурси, па, чак и само функционисање мрежног система. Због тога је обезбеђивање онлајн сигурности озбиљан задатак читавог друштва, дакле не само лица која непосредно раде на мрежи, већ и свих других субјеката који на било који начин имају везе са онлајн активностима.*

Кључне речи: *интернет, информатичка безбедност, мере заштите.*

1. УВОД

Интернет је изузетан медијум за рад, комуникацију, информисање, истраживање, учење и забаву. Омогућава нам да будемо у редовном контакту са постојећим и да упознајемо нове пријатеље, да истражујемо идеје и погледе на свет о којима до сада нисмо могли ни да сањамо. На жалост, као што има креатора свега лепог и корисног, на интернету има и нечег због чега он има и своју тамну страну. Постоје милиони сајтова са негативним, често и агресивним, криминалним садржајем. Креатори тамне стране толико су бројни и активни да се сваке секунде појави један такав сајт. Томе треба додати - крађу бројева кредитних картица (самим тим и новца и индентитета), стварање и преношење вируса, постојање шпијунских програма, нежељене поште (спамова) и мноштво других злоупотреба.

Стални технички и комерцијални развој онлајн услуга, такође угрожава приватност, а усмереност ка профиту ствара веома снажан притисак за масовним надзором становништва. Ипак, није све тако црно, јер нове технологије пружају и могућност заштите личних информација. Комуникације нпр., могу бити шифроване како би се заштитила поверљивост, а такође и анонимност учесника комуникације. Електронска плаћања могу бити структуирана тако да анонимност минимизира или елиминише прикупљање података о личности, јер је најефикаснији начин контроле сопствених података о личности спречавање да ти подаци дођу у неку базу података.

Забринутост великог броја корисника интернета изазива чињеница да се информације које се тичу њих самих аутоматски генеришу, прикупљају, складиште, међусобно повезују и користе у различите сврхе, укључујући комерцијалне, па и незаконите. Даваоци пословних и интернет услуга имају приступ великој количини података о личности својих потрошача. Они прикупљају, контролишу, користе и уступају (продају) ове податке трећој страни без сагласности лица на која се они односе.

Праћењем понашања корисника на интернету могуће је формирати комплетан профил корисникових навика, имати податке о његовим интересовањима (које сајтове посећује, који садржаји га интересују,

колико се задржава на појединим страницама), податке о томе шта купује онлајн итд.

Флуидна структура не штити интернет од прислушкивања и контроле од власти. Пошто је медијум нов, недостаје му заштита коју имају традиционални телефонски системи. Државне и националне обавештајне службе веома брзо су прилагодиле своје капацитете за пресретање електронске поште и контролисање интернет саобраћаја.

Техничка структура интернета, као и рањивост мреже, такође, веома озбиљно доводи у питање и безбедност ауторскоправно заштићеног садржаја, било које врсте. Због тога се дигитална технологија појављује као реална претња постојању интелектуалне својине у најширем смислу.

Због свега изнетог, у крилу информатичке технологије морају се перманентно стварати и развијати системи заштите безбедности од свих врста напада и угрожавања интегритета целокупног садржаја који фигурира на мрежи. Досадашњи приступ борбе против појединачних последица, на жалост, ефикасан је само у појединачним случајевима, док генерална претња онлајн безбедности још увек остаје.

2. БЕЗБЕДНОСТ

Безбедност на мрежи, односно онлајн безбедност је актуелна тема која изазива пажњу многих субјеката, а нарочито је значајна за кориснике и провајдере информационе технологије (IT).[1] Масовна употреба PC, PDA и бежичних уређаја на интернету довела је до смањења безбедности корисника. Генерално, безбедност се односи на заштиту IT добара, али и личних добара и, начелно се дели на следећих пет главних области:

а. Безбедност локације (“сајта”) - Компјутерски центри и просторије у којима се одвијају IT активности везане за обраду података, односно у којима су смештени и ускладиштени информатички ресурси;

1 Стриктно посматрано, информатичка безбедност је шири појам од онлајн безбедности, јер укључује не само мрежну (онлајн) безбедност већ и офлајн безбедност. Код онлајн активности приступ мрежи је перманентан, док се код офлајн радњи приступ мрежи врши ad hoc, дакле само по потреби (нпр. убацивањем картице у аутомат приликом подизања новца или плаћања).

б. Безбедност ресурса - Опрема и постројења, софтверски програми и системи, као и базе података привредног субјекта;

в. **Безбедност комуникацијске мреже -** Локалне (LAN) мреже, WAN мреже, интранет и екстранет мреже;

г. Безбедност сервиса - Сигурност информатичких функција, највиша расположивост према корисницима;

д. Безбедност приватности - личних података.

Безбедносни програм прописује заштитне процедуре и одговорност лица задужених за очување безбедности. Под нарушавањем безбедности подразумева се свака радња која може изазвати било који облик оштећења система или неког његовог елемента или ресурса. Безбедносни програм обухвата **с**куп политика и заштитних мера које ће бити примењиване за одговорност појединаца задужених за очување безбедности.

2.1. Типови нарушавања безбедности

Угрожавање података (безбедности) у рачунарским мрежама може бити разноврсно, као нпр. прислушкивање, анализа, мењање или задржавање информација, лажно представљање итд. Зависно од утицаја потенцијалних нападача на ток информација, начелно постоје две врсте напада на рачунарске мреже, односно два облика нарушавања безбедности:

- **Пасивни напади** (енгл. passive atacks) и
- **Активни напади** (енгл. active atacks).

Пасивни су сви облици утицаја (нпр. прислушкивање, надгледање и сл.) на ток информација без активних измена у самом току.[2] Пасивне методе је, зависно од конфигурације тешко, али не и немогуће приметити и онемогућити, а као најчешћи механизми заштите примењује се шифровање информационог тока, односно садржаја.

Активни напади подразумевају промену садржаја информација или њиховог тока, као и модификацију мрежних пакета, производњу

2 Тако, нпр. прислушкивање коаксијалних каблова је релативно лако извести уз помоћ електромагнетских сензора, док се прислушкивање оптичких каблова не може извести без интервенције на каблу, што слаби сигнал и што се може детектовати и спречити.

новлашћених мрежних пакета или прекид информационог тока. Ови напади су опаснији и разноврснији.

Уз помоћ безбедносних програма субјекти - предузећа (власници добара и права) штите се од два различита облика нарушавања безбедности:

- **Заштита против упада** - усмерена је на одвраћање напада који долазе било споља или изнутра, укључујући и злоупотребу IT добара од стране запослених у том предузећу. Упад представља насилан и неовлашћени приступ неком систему. Заштита обухвата и поступке за откривање упада након што се они већ догоде, као и поступке анализе и процене њиховог негативног утицаја на интегритет података, односно ресурса или софтвера.

- **Заштита од пресретања** (interception) - усмерена је ка превенцији од преузимања података за време њиховог преношења преко комуникацијских линкова. Пресретање је неовлашћено преузимање података и информација за време њиховог преношења преко мреже или других комуникацијских линкова.

2.2. Последице нарушавања безбедности

У случају да дође до нарушавања или повреде безбедности могу настати бројне штетне консеквенце. Све оне се генерално могу поделити на следећих шест категорија:

а. **Уништење ресурса -** Оштећење опреме и постројења, односно брисање података и софтверских програма.

б. Неисправност података и апликација - Модификација софтвера и апликација, тако да приликом њихове употребе долази до потпуно погрешних резултата, односно оштећења података како би се они учинили неупотребљивим или непоузданим.

в. Одбијање пружања сервиса (denial-of-services) - Онемогућавање корисника у употреби различитих сервиса: електронске поште, веб сајта и сл. који су му, под нормалним околностима, доступни.

г. Крађа сервиса – Неовлашћено коришћење услуга провајдера у обради података, без плаћања новчане накнаде за то коришћење (нпр. крађа времена на интернету).

д. Крађа ресурса - Нелегално копирање или преузимање података, софтвера, музике, филмова и других дигиталних садржаја (повреде ауторскоправно заштићеног садржаја).

ђ. **Повреда или нарушавање приватности** – Неовлашћен приступ личним подацима, односно повреда личних добара.

2.3. Извори нарушавања безбедности

За нарушавање онлајн безбедности могу послужити четири основна извора: запослени у предузећу, хакери, терористи и компјутерски вируси.

2.3.1. Запослено особље

Пре свега, нарушавање безбедности могуће је од стране инсајдера. Бивши или тренутно запослени радници у неком предузећу представљају уобичајен, примарни извор нарушавања безбедности. Појединци, који су на било који незадовољни статусом у предузећу - компанији, често сами узимају правду у своје руке тако што нападају IT имовину свог послодавца. То може бити нека врста саботаже на хардверу или уметање деструктивних или малициозних наредби у компјутерске апликације. Исто тако, запослени могу искористити своју позицију у предузећу и добро познавање неке апликације како би извршили пресретање информација и њихово неовлашћено коришћење. То може бити крађа идентитета, која се методама пресретања користи за продају персоналних идентификационих података.

2.3.2. Хакери

Хакери су особе које неовлашћено приступају неком компјутерском систему, обично путем мреже (а понекад и физички приступе неком компјутеру или мрежном постројењу) мотивисани стицањем профита или обичним изазовом. Појам хакер се не односи на изузетне вештине у компјутерском програмирању и употреби компјутера на инвентиван, продуктиван и коректан начин. Број хакера широм света је током протекле деценије значајно нарастао, првенствено због све веће расположивости компјутера у школи, на радном месту и код куће.

Хакери, по правилу, нису терористи, пошто они то што чине раде из хобија, забаве или жеље за доказивањем.[3]

2.3.3. Сајбер терористи

То су лица која са предумишљајем изводе политички мотивисане нападе против информација, компјутерских система, компјутерских програма података, који за последицу имају насиље над неборбеним циљевима од стране поднационалних група или тајних агената. Терористи, могу предузимати нападе са циљем уништења информационе технологије, чисто ради изазивања страха међу запосленима, потрошачима, добављачима и другим учесницима на тржишту, нарочито уколико ти напади могу проузроковати неизвесност даљих догађања. Стога, онлајн шпијунажа и тероризам на нету представљају претњу глобалној безбедности.

Сајбер-тероризам је усмерен ка постројењима на која се ослањају IT. У потенцијалне мете терориста спадају: електричне централе, постројења за пречишћавање воде и контролни сиситеми у ваздухопловству. Финансијски мотивисани терористички напади усмерени су углавном према банкама и берзама.

2.3.4. Компјутерски вируси, спајвери и други малициозни програми

Осим наведеног постоје и други извори нарушавања IT безбедности. **У**пади у компјутерске системе могу се остварити и путем софтвера. **Компјутерски *вирус*** је скривени програм који без знања корисника врши одређене измене у начину функционисања компјутера или модификује податке и програме који су на њему.[4] У техничком

3 Хакери су у Америци већ ушли у компјутерски систем Пентагона; У Индији у министарске фајлове; У Немачкој у компјутер државног канцелара; Кинески хакери су ушли у јужнокорејски систем безбедности. Напади могу да буду испланирани тако да угрозе безбедносни систем, кључну инфраструктуру једне земље, да оптерете комуникациони систем или евентуално изазову пљачку банке.

4 Kevin D. Mitnick, 35-годишњи компјутерски криминалац, међу првима је осуђен за злочине у области IT-а. Он је провалио у систем компјутерског физичара из Сан Диега у Калифорнији, Kutoma Šimomure и украо више страница поверљивог извештаја о истраживањима у области безбедности мобилне телефоније. Хакер је откривен и ухапшен првенствено захваљујући самом Šimomuri. Након одслужења затворске казне и условне казне током које му је била забрањена употреба компјутера, Mitnick је написао књигу под насловом „Уметност преваре“.

смислу, вируси су мали компјутерски програми који инфицирају рачунаре и лако се преносе са једног рачунара на други. Вируси се креирају са намером да узрокују оштећења или направе хаос у неком систему. Најчешће се шире као атачменти у имејлу – инфицирани рачунар може без знања корисника разаслати на десетине хиљада имејл порука које као атачмент садрже вирус, користиће углавном корисников имејл адресар да би пронашао нове жртве. Други начини на који се може доћи „у посед" вируса је даунлоудовање („скидање") са неког интернет сајта приликом преузимања неког садржаја – музике, фотографије или једноставног програма. Понекад је довољна и само посета таквог сајта да би се „закачио" вирус.

Карактеристика вируса је способност саморепродукције - прелажења са компјутера на компјутер приликом размене података. Сваки вирус се одликује специфичним карактеристикама. Неки неповратно бришу податке, тако што по зараженом диску пишу бесмислице. Други преузимају контролу над оперативним системом и узрокују потпуни престанак функционисања компјутера. Трећи врше уметање разноразних инструкција у оперативни систем. Најгори облици вируса су знатно суптилинији, јер приликом кретања кроз компјутер врше измене ситних детаља у одабраним фајловима на тако неприметан начин да их је изузетно тешко детектовати. Најосетљивији у погледу безбедности су PC рачунари.

Спајвери су програми који се од вируса разликују по томе што се не реплицирају и не шире самостално већ „чекају" да грешком буду даунлоудовани, што се често догађа када се користе P2P (пир ту пир) програми (нпр. за размену музике). Могу биди веома опасни – посебно ако спадају у ону врсту која када је корисник на интернету даунлоудује вирусе.[5]

Преваре и крађе личних података приликом куповине, такође су могуће. Онлајн куповина веома је популарна у свету а постепено се развија и код нас. Веома комфорно, седећи пред својим рачунаром,

5 Вируса и њихових врста има много, као и начина на који могу деловати на нечији рачунар. Ипак, не мора неко бити експерт и знати све о њима да би се могао заштити. Најбољи начин заштите од вируса је употреба антивирус програм (он се мора редовно апдејтовати пошто у супротном веома брзо постаје бескористан због брзине којом настају нови вируси), фајервол – заштитни зид (firewall) и здрав разум, односно велики опрез приликом сваке онлајн активности.

могуће је куповати разне производе и плаћати их кредитном картицом. Међутим, овакве могућности су велики изазов за сајбер криминалце.

Сајбердејтинг се појављује као латентан извор опасности. Имајући у виду чињеницу да се на мрежи може реализовати уговарање састанака, то омогућава појаву интернет педофилије, односно интернет предатора. Облици овакве злоупотребе деце и тинејџера могу да варирају од егзибиционизма и продуковања порнографских садржаја, дакле без непосредног физичког контакта, па све до фактичког физичког злостављања које укључује и само сексуално насиље.

Будући да може да омогући брзо и релативно лако дистрибуирање, односно прибављање и чување порнографских садржаја, али и ступање у контакт са потенцијалном жртвом, интернет може да представља погодан медијум за педофилију. Приступ детету или тинејџеру може се остварити преко различитих чет сервиса и сервиса за брзу размену порука.[6] Анонимност комуникације, која је на овај начин омогућена, додатно може погодовати потенцијалним злоупотребама. Оно што интернет омогућује педофилима такође је и стварање мрежа – виртуелних заједница у којима владају често веома „колегијални" односи, и путем којих се размењују материјали и различите информације.

2.4. Неки посебни облици претње на интернету

Спам – нежељена пошта. Према неким подацима, од укупног броја и-мејлова који се дневно пошаљу на свету (више милијарди), спам чини највећи део порука.

Phishing - коришћење лажних е-мејл адреса и легитимних веб сајтова. Phishing дословно значи пецање туђих личних података. Оно што овим тзв. пецарошима треба јесу туђи бројеви рачуна, лозинке, и други лични подаци, које ће касније употребити у противзаконите сврхе.

Botnet - софтверска мрежа за распростирање вируса, постала је средиште преварантских активности на интернету.

Reputation hijacking - све више криминалаца на интернету користи праве е-мејл адресе са великим, легитимним интернет

6 У последње време комуникација се нарочито остварује преко друштвених мрежа facebook или myspace, или преко све популарнијег skype.

провајдерима за слање нежељених порука (спам). Ова крађа (отмица) помоћу туђих адреса се једноставније спроводи, јер је тада спам теже препознати и блокирати.

3. МЕРЕ БЕЗБЕДНОСТИ

У рачунарским мрежама се у циљу спречавања евентуалних напада и могућих оштећења података примењују одређени сигурносни сервиси, од којих су најзначајнији:

а. Аутентификација (енгл. authentication);
б. Тајност података (енгл. data confidiality);
в. Непорицање порука (енгл. nonrepudation);
г. Интегритет података (енгл. data integrity);
д. Контрола приступа (енгл. access control) и
ђ. Расположивост ресурса (енгл.resource availability)

Ради повећања IT безбедности предузећа, односно компанија обично се примењује шест категорија безбедносних мера. Избор мера зависиће од потребног нивоа безбедности. Ту спадају: (1) опште безбедносне политике и процедуре, (2) софтвер за заштиту од вируса, (3) дигитални потписи, (4) шифровање, (5) заштитнии (противпожарни) зидови и (6) прокси сервери.

3.1. Опште безбедносне политике и поступци

Превенција различитих облика нарушавања безбедности, укључујући неовлашћени приступ компјутерским системима, захтева пре свега одлично физичко обезбеђење, као и квалитетне безбедносне политике и процедуре.

Очигледно је да се прва мера састоји у ангажовању часних и поузданих људи од интегритета. Постоји још 10-ак додатних техника које могу бити од драгоцене помоћи у одвраћању упада и пресретања. Ту спадају следеће технике:

а. Честа промена приступних лозинки - Од корисника би требало захтевати да приликом сваког покушаја приступа систему у њега уносе своје личне идентификационе кодове. Лозинке-пасворди су најстроже поверљиве информације.

б. Ограничавање употребе система - Корисницима треба омогућити приступ само неопходно потребним функцијама система, а никако им не дозволити пун приступ систему.

в. Ограничавање приступа подацима - Корисницима треба дозволити приступ само оним подацима који су им неопходни за извршавање послова из њихове надлежности.

г. Успостављање контроле физичког приступа - Приступне картице и такозвани биометријски уређаји - који препознају глас, отиске прстију или дланова, ретину ока или потписе - представљају неке од најефикснијих система за физичко обезбеђење.

д. Подела одговорности – Суштински важне функције, које подразумевају високи ризик или огромну вредност података који се обрађују, треба на одговарајући начин раздвојити како би у обраду података било укључено више особа. Мрежним и администраторима базе података треба доделити одвојене одговорности по питању контроле приступа систему.

ђ. Шифровање (енкрипција) података - Променом изгледа података, путем њиховог скремблovања и кодирања, биће знатно отежана њихова неовлашћена употреба, чак и уколико хакер успе да им приступи.

е. Успостављање процедуралне контроле - Уколико се корисници и запослени у IT одељењу стриктно придржавају јасно дефинисаних процедура, опасност од нарушавања безбедности биће знатно умањена.

ж. Провођење едукативних програма - У едукативним програмима из области безбедности треба истаћи опасност од упада, објаснити методе које користе хакери, и пружити упутства о томе како треба реаговати приликом откривања упада.

з. Инспекција активности унутар система - Током вршења инспекције (аудит), независни стручњаци детаљно прегледају трансакције и активности везане за компјутерску обраду података како би анализирали њихово порекло и утицај на систем и потврдили да су све ове активности претходно одобрене и да су извршене од стране овлашћених лица.

и. Бележење свих трансакција и активности корисника - Неопходно је стално пратити и бележити све активности унутар система, као и идентитет особа које су те активности извршавале.

Као додатак овим техникама, неке компаније примењују метод такозваног повратног позива (call-back).[7]

3.2. Софтвер за заштиту од вируса

Да би своје системе заштитиле од вируса, многе компаније су принуђене на куповину софтвера за детекцију вируса, специјалних програма који врше скенирање компјутерских дискова у потрази за вирусима. Постоје два основна метода за детекцију вируса: скенирање и пресретање.

Програми за скенирање претражују меморију рачунара ради проналажења вируса. Већина програма ове врсте одговарајућом поруком упозоравају корисника да је вирус откривен. Након тога, корисник може програму наложити да уништи вирус и, уколико је могуће, изврши поправку оштећених података. Програми за детекцију вируса раде у позадини, пратећи активности на обради података и сигнализирају кориснику откривње вируса. Рано откривање и блокирање вируса од кључне је важности за очување интегритета података.[8]

---

7 Овај метод функционише на следећи начин. Када позивач окрене одговарајући број за приступ систему, он доставља број телефона са којег врши позивање. (Већина савремених система може овај број аутоматски детектовати). Позивач затим прекида везу да би систем, након што провери да ли је тај телефонски број валидан и овлашћен, упутио повратни позив тој особи. Метод повратног позива у комбинацији са другим техникама пружа драгоцену додатну заштиту безбедности.

8 Компанија Novell, произвођач софтвера и највећи снабдевач канцеларијских мрежа за PC на територији САД, до овог закључка је дошла на тежи начин. Наиме, пре неколико година она је била приморана да својим потрошачима, њима око 4.000, пошаље писмо у којем их упозорава да им је грешком испоручила заражене копије дискова за ажурирање њиховог мрежног софтвера. У питању је био вирус који је касније постао познат по имену *Stoned III.* Менаџери Novella су успели да извор овог дебакла лоцирају у производном процесу. Касније је откривено да је вирус пореклом из Европе и да је настао свега три месеца пре но што је компанија произвела дискове. Ради спречавања појаве оваквих и сличних проблема компанија Novell је набавила специјалан софтвер за дигитално потписивање.

3.3. Дигитални потписи

Релативно нова технологија шифровања дигиталног потписа (digital signature encryption) ослања се на математички метод кодирања, која је дизајнирана у циљу спречавања вируса у покушају напада на податке и програме. Лако преносиви дигитални потписи могу се користити за проверу идентитета пошиљаоца поруке или потписника неког документа. На тај начин се доприноси онлајн безбедности.

Законски акт о електронским потписима у глобалној и националној трговини САД (краће: Закон о е-потписима), који је ступио на снагу 2000. године, дефинише да су дигитални потписи, у формалноправном смислу, исто тако валидни као и класични својеручни потписи сачињени мастилом на папиру.[9] Очекује се да ће овај закон, који се односи искључиво на електронске трансакције на територији САД, охрабрити пословне компаније да дефинишу сопствене процедуре за употребу е-потписа. То ће за последицу имати знатно брже обављање рутинских пословних активности и елиминисање трошкова везаних за штампање и слање трговинских уговора и других и правних докумената у папирној форми.

3.4. Шифровање

Када говоримо о заштити против пресретања података (приликом њиховог преношења преко комуникацијских линкова), једна од најефикаснијих мера безбедности састоји се у шифровању (енкрипцији) података. Енкрипција се састоји у употреби одговарајућег математичког алгоритма ради конверзије података у шифровани облик, који се још назива цифарским текстом. Овај алгоритам користи такозвани кључ, односно неку промењљиву вредност, како би дату поруку превео у „прерушени облик“ цифарског текста. Сложеност тог кључа представља детерминишући фактор степена безбедности који ће бити уграђен у тај цифарски облик.[10]

---

9 Видети шире у: В.Спасић, Дигитални потпис у светлу Директиве ЕУ, Симпозијум о рачунарским наукама и информационим технологијама, Зборник радова YUINFO Ниш, 2004, CD-ROM, електронска публикација.

10 Видети шире у: В.Спасић, Улога криптографије у трансферу и приступу информацијама на интернету – правни аспекти, Симпозијум о рачунарским наукама

Технологија заснована на математичкој шеми кодирања, дизајнирана је у циљу спречавања вируса у њиховом покушају напада на податке. Данас су у најширој употреби следећа три метода енкрипције: инфраструктура јавног кључа, прилично добра приватност и виртуална приватна мрежа.

У области пружања финансијских услуга недавно је развијен метод безбедне електронске трансакције (secure electronic transaction - SET), који представља својеврсну адаптацију метода шифровања помоћу јавног кључа и методе дигиталног сертификата (који се назива електронским новчаником), а служи за безбедно обављање финансијских трансакција преко интернета.[11]

3.5. Прилично добра приватност (*Pretty good privacy* - PGP)

Прилично добра приватност је назив популарног програма који служи за шифровање и дешифровање имејл порука и шифровање дигиталних потписа, како би прималац поруке могао да буде сигуран да њен садржај није током преноса претрпео никакве измене. Уколико се жели користити PGP ради заштите електронске поште, потребно је купити релативно јефтину "full" верзију овог програма и инсталирати је на свом компјутеру. [12]

3.6. Виртуелна приватна мрежа

Виртуална приватна мрежа (VPN) представља један од начина за коришћење јавне телекомуникацијске инфраструктуре, као што је интернет, ради остварења безбедне комуникације између клијент-компјутера на удаљеним локацијама и неке предузетничке

и информационим технологијама , Зборник радова YUINFO Ниш, 2001, CD-ROM, електронска публикација.

11 Међу најактивнијим учесницима у развоју СЕТ пројекта биле су и веома познате компаније као што су: MasterCard, Visa, Microsoft i Netscape. Сваком кориснику СЕТ програма додељује се електронски новчаник (т.ј. дигитални сертификат), након чега се новчане трансакције обављају и верификују уз помоћ комбинације дигиталних сертификата и дигиталних потписа.

12 Програм садржи кориснички интерфејс који је компатибилан са већином популарних имејл апликација. Јавни кључ, који представља саставни део PGP програма, мора бити регистрован на PGP серверу како би и други корисници са којима ће бити размењиване поруке могли на њему да пронађу корисников јавни кључ.

мреже. VPN мрежа функционише тако што користи заједничку, јавну инфраструктуру, уз истовремено очување приватности преко одговарајућих безбедносних процедура и такозваних тунелских протокола. Шифровањем података на полазној тачки и њиховим дешифровањем у тачки пријема и слањем података тунелским протоколима ствара се систем у који не могу продрети подаци који нису на одговарајући начин шифровани.

3.7. Заштитни (противпожарни) зидови

Заштитни или противпожарни (firewall) зидови сматрају се суштински важним механизмом заштите од неовлашћеног приступа преко комуникацијских канала (жичаних или бежичних). Под појмом заштитни зид (firewall) означава се софтверски програми специјалне намене, смештен на серверском рачунару који играју улогу мрежног пролаза (gateway). Овај софтвер је дизајниран ради заштите корисника неке приватне мреже, путем блокирања свих оних порука које долазе од корисника са других мрежа, а за које се установи да у себи садрже потенцијално штетне програме или податке.

У комбинацији са неким усмеравајућим (рутерским) програмом, firewall софтвер врши анализу свих пакета који пристижу на дату мрежу. Он притом анализира порекло тог пакета, његово одредиште, намену, садржај и евентуалне прилоге (attachments), како би установио да ли се тај пакет може безбедно проследити ка жељеном одредишту.[13] Firewall пружа веома добру заштиту, како од упада споља тако и од тзв. "инсајдера" који покушавају да неовлашћено приступе систему преко мреже.

Данас се ови програми све чешће уграђују у оперативне системе као и комуникацијске уређаје.

3.8. Прокси сервери

Прокси сервер (Proxy server) се често користи ради очувања безбедности интернет апликација и система. Проксији су мала стоваришта са подацим. Серверски рачунар игра улогу посредника

13 Веома често ће извршни (executable) програми, или приложени фајлови већих димензија, бити задржани на филтеру заштитног зида, јер је firewall софтвер оценио да њихов садржај може штетно деловати на систем који тај firewall штити.

између неког PC рачунара и интернета, физички раздвајајући пословну мрежу од неке спољне мреже. Овај сервер најчешће функционише у комбинацији са неким заштитним зидом (firewall) и у себи обично садржи кеш меморију, у којој чува недавно посећене веб странице како би им следећи пут корисник имао бржи приступ.

Када прокси сервер од неког корисника прими захтев за приступ интернету (захтев за преглед неке веб странице), он најпре проверава да ли је тај захтев валидан по питању корисника који га је поставио, да би затим претражио сопствени кеш и проверио да ли у њему већ постоји претходно преузета копија тражене веб странице. Уколико тражену страницу пронађе у кешу, он је одмах шаље кориснику, елиминишући тако потребу за прослеђивањем његовог захтева ка интернету. Ако, пак, тражене веб странице нема у кешу, прокси сервер испоставља захтев за преузимањем те странице са интернета да би је, одмах по њеном пристизању, проследио кориснику.

Прокси сервер је потпуно невидљив са становишта корисника и не мења значајно брзину преузимања веб страница. Функције проксија, firewall и кеширања веб страница могу бити поверене засебним прогамима или бити обједињене у једном програму.

3.9. Поузданост IT сервиса

Како пословне компаније постају све више зависне од IT-а, тако расте потреба за непрекидном доступношћу својих компјутера и комуникацијских система. Са овом зависношћу неминовно долази и потреба за поузданошћу система. Поузданост (*reliability*) представља управо гаранцију да ће систем радити оно за шта је пројектован.[14] Поузданост IT сервиса се може разматрати на следећа четири нивоа: (1) компјутери са толеранцијом грешке, (2) системи за непрекидно напајање, (3) планови за опоравак од хаварије и (4) удаљена резервна постројења.

14 Као пример поузданости система наводи се Nasdaq мрежа, код које је улагање у поузданост система допринело да ова берза настави са радом и у условима терористичког напада на зграде Светског трговинског центра.

3.10. Приватност

Појам приватности можемо посматрати у класичном (традиционалном) и у савременом (информатичком смислу). Информатичка приватност обухвата скуп података (информација) о личности, насталих употребом дигиталне технологије, које дају печат његовој индивидуалности, а које су правно заштићене од неовлашћеног приступа и повреде од стране свих других лица. У ужем (техничком) смислу, под појмом приватности (privacy) обично подразумевамо начин прикупљања, употребе и заштите личних информација на мрежи. Проблем приватности није настао тек са појавом компјутера.[15] Међутим, огромне могућности IT-а са аспекта складиштења и преузимања података вишеструко су појачале потребу за ефикасном заштитом приватности. Има мишљења, чак, да ће, у годинама које су пред нама, заштита приватности представљати главни проблем и баласт у међусобним односима пословних компанија и потрошача.[16]

3.10.1. Начини угрожавања приватности на интернету

Када корисници посете неки сајт углавном мисле да нико нема увид у то што они раде. Међутим, ствари не стоје тако. Уз помоћ савремених технологија могуће је "вирити преко туђег рамена", бележити шта гледа или „скида", које сајтове посећује и колико дуго остаје на појединим страницама. Савремено доба донело је технологију која иде испред етике. Уз помоћ данашњих PC-а практично свако може да "завири" у интиму свакога. Постоји више начина за угржавање нечије онлајн приватности.[17]

Колачићи (cookies) су текстуалне датотеке које је написао читач клијента и садрже информације које је послао сервер, а које се налазе на рачунару корисника. Они чувају информације о кориснику и употребљава их конкретан сервер (или сервер у оквиру истог поддомена) којег је корисник раније посетио ради персонализације веб

15 И у прошлости је било жучних расправа око тога да ли, на пример, фотографисање других људи без њиховог пристанка представља атак на њихову личну приватност или не.

16 Видети шире у: В.Спасић, Приватност у дигиталном свету, Правни живот бр.11/2004, стр.867-886.

17 Видети шире у: В.Спасић, Неки аспекти приватности у сајберспејсу, Зборник радова Правног факултета у Нишу, бр.46, 2005, стр. 207-226.

страница, за саопштавање ажурираних података у вези са релевантним информацијама. Колачићи такође представљају начин за посматрање понашања корисника на мрежи без њиховог знања о томе.

Приватност интернет корисника угрожавају и спајвери, тзв. шпијунски програми (**Spyware)**. Већина ових програма је, у суштини, више непријатна него што је штетна. Користе их специјализоване компаније за прикупљање и обраду релевантних података са рачунара на којима су овакви програми инсталирани, а затим те податке достављају својим клијентима, односно субјектима којима су статистички подаци од великог значаја за агресивнији и ефикаснији наступ на тржишту. На рачунар долазе, најчешће, инсталацијом неких од бесплатних више или мање практичних и атрактивних „програмчића" (најчешће као њихов скривени део), а могу бити инсталирани и као вирус. Корисник најчешће не може приметити да је овакав програм инсталиран на његовом рачунару. Једном учитани на рачунар, ови програми прикупљају податке и шаљу их на одређену адресу.

Корисници, углавном, не схватају постојање проблема везаног за постојање Spyware програма на њиховим рачунарима – најчешће нису ни свесни њиховог постојања и начина њиховог деловања. Када је у питању легалност оваквог софтвера најчешће га инсталирају сами корисници прихватајући све услове коришћења програма (најчешће и не читајући услове везане за коришћење).

Spyware програми функционишу на више начина, почев од праћења активности, одашиљања података компанијама које то користе у маркетиншке сврхе, па све до програма за снимање и праћење комуникација са рачунара.

Све врсте софтвера које се користе на интернету су дизајниране тако да корисник оставља трагове свих врста трансакција. Снимање трагова се одвија на свим нивоима: кеш меморији корисничког PC-а, прокси серверима провајдера који омогућавају приступ интернету или интранет сервера компаније и сервера провајдера садржаја.

Неке од најжешћих дебата које се у последње време воде у вези са приватношћу инициране су првенствено најновијим техничким достигнућима на плану телекомуникација. Једно од кључних и најдискутабилнијим је питање: Да ли чињеница да мобилни оператер у сваком тренутку зна тачну локацију особе која користи мобилни телефон представља повреду њене приватности?

3.10.2. Спам и приватност

Термином спам означава се свако неовлашћено слање нежељених (unsolicited) имејл порука. Овакве поруке се обично шаљу групно (као такозвани bulk mail) ка великом броју прималаца, чије се адресе извлаче из мејлинг листа на интернету.

Са становишта примаоца, на ове поруке се најчешће гледа као на „смеће“ (junk mail) или, у најбољем случају, као на гомилу бесмислица. Правила имејл бонтона налажу да по сваку цену траба избегавати спамовање. Спам на интернету је, генерално еквивалентан нежељеним аутоматским рекламним позивима преко телефона.

Поједине врсте имејл порука, за које би се на први поглед могло рећи да представљају спам, заправо су поруке за чије је слање корисник, свесно или несвесно, дао одобрење приликом регистрације на неком веб сајту. Наиме, уколико посетилац веб сајта неке компаније означи поље за потврду поред питања типа “да ли желите да примате обавештења о производима наше компаније?”, он тиме фактички даје сагласност за пријем оваквих рекламних порука.[18]

Треба истаћи и значајно повећање трошкова на интернету, узроковано повећањем обима мрежног саобраћаја услед слања спам порука, чиме се уједно продужава и време реакције на друге врсте мрежних захтева. Поред тога, нтернет провајдери и сродни субјекти морају инвестирати у куповину додатних сервера и комуникацијских линкова како би успели да одрже очекивани ниво квалитета својих услуга.

3.11. Етички моменат и IT технологија

Под онлајн моралом (ethics) подразумевамо скуп неписаних правила понашања корисника које треба поштовати приликом употребе информационе технологије. Пословни морал односи на њихове активности у сфери бизниса, укључујући и начин њиховог опхођења према конкуренцији, потрошачима и свим другим субјектима са којима њихова фирма послује.

Важно је, међутим, разликовати морално понашање од легалног понашања. Морално понашање се односи на извршавање очекиваних

18 Оне се у интернет жаргону обично означавају као opt-in e-mail или permission-based e-mail.

активности, док се под легалним понашањем обично подразумева извршавање захтеваних активности.

Нека активност, дакле, може бити легална иако неморална, док друга може бити морална, али у исто време и противзаконита, односно нелегална.

У неке од најактуелнијх моралних проблема са којима се савремене компаније морају суочити спадају:

а) Приватност електронске поште;
б) Софтверске лиценце;
в) Ауторска права над софтвером;
г) Приступ хардверу;
д) Власништво над интелектуалном својином;
ђ) Приступ фајловима;
е) Власништво над подацима.

3.12. Дигитална пиратерија

Етички проблеми се у подједнакој мери односе и на употребу дигиталних садржаја и софтвера, као и на њихове карактеристике. Попут података и информација, софтвер такође представља драгоцену компоненту сваког пословног система: он је тај који надгледа обраду и трансформацију података у неки користан и употребљив облик. С обзиром на то да је комерцијални софтвер прилично скуп, он је често на мети пирата. Исто важи и за дигиталне садржаје.

У најширем смислу, под пиратеријом (piracy) се подразумева израда нелегалних копија информација заштићених ауторским правом. Дигитална пиратерија састоји се у нелегалном копирању дигиталних производа и информација. Поред музичке и филмске, данас највећи проблем представља софтверска пиратерија.[19]

3.12.1. Заштита од софтверске пиратерије

Поред музичке и филмске пиратерије, у дигиталном окружењу изузетан проблем представља софтверска пиратерија. Она се састоји у изради нелегалних копија софтвера. Овај облик криминала представља

19 В.Спасић, Савремени облици пиратерије, Правни живот, бр. 13/2007, стр. 297 и даље.

један од најозбиљнијих проблема у савременој информационој технологији, јер због своје масовности ствара огромне губитке компанијама које се баве производњом софтвера.[20]

Мада ниједан од постојећих метода софтверске заштите не гарантује потпуну безбедност, у савременој IT индустрији се најчешће примењују следећа три метода борбе против пиратерије: (1) заштита ауторских права, (2) заштита од копирања и (3) лиценцирање по месту употребе.

3.12.2. Ауторско право

Ауторско право (copyright) штити оригинална ауторска дела од неовлашћене употребе.

Године 1998. ступио је на снагу Миленијумски Закон о зашити ауторских права над дигиталним садржајима (Digital Millennium Copyright Act). Овај закон представља практичну имплементацију уговора потписаних у децембру 1996. године на женевској конференцији Светске организације за интелектуалну својину (World Intellectual Property Organization - WIPO).

Између осталог, њиме су обухваћена и нека друга питања у вези са заштитом ауторских права. Овим законом дефинишу се и казнене мере против субјеката који угрожавају одредбе других важећих закона о ауторским правима. Њиме се, такође, јасно дефинишу права и одговорности у области спровођења заштите ауторских права, посебно субјеката који предузимају активности на мрежи (нарочито интернет сервис провајдера).

3.12.3. Заштита софтвера од копирања

Произвођачи и продавци софтвера осмислили су многе технике којима би копирање софтвера било у потпуности онемогућено. Технике заштите од копирања (copy protection) састоје се у примени хардверских или софтверских карактеристика које спречавају покушаје копирања неког програма или копирани софтвер чине непоузданим. Међутим, ниједна од до сада разијених техника заштите од копирања није се показала потпуно поузданом. Што је још горе, примена ових техника

20 Произвођачи софтвера процењују да на сваку легално продату копију софтвера долази чак седам пиратских копија.

онемогућава копирање софтвера од стране појединаца који су потпуно легално купили неки програм и желе да направе његову резервну копију за случај да доде до било каквог оштећења на оригиналној копији. Могућност креирања резервне копије предвиђена је у већини уговора о софтверској лиценци. Да би изашли у сусрет корисницима који су софтвер легално купили, већина произвођача је потпуно одустала од покушаја заштите свог софтвера од копирања. Ипак, они и даље предузимају све законом предвиђене мере у борби против софтверске пиратерије.

3.12.3.1. Лиценцирање софтвера по месту употребе

Ради помоћи фирмама са великим бројем корисника и, истовремено, сузбијања софтверске пиратерије, многи произвођачи софтвера нуде могућност такозваног лиценцирања по месту употребе (site licensing). На основу једног оваквог уговора о лиценци, купац се обавезује да произвођачу плати одређену новчану накнаду на име креирања договореног броја копија неког конкретног програма. Надаље, купац је дужан да строго води рачуна и бележи имена корисника којима је додељена копија програма, као и број и називе компјутера или компјутерских мрежа на којима су те копије инсталиране.

Од оваквог начина лиценцирања обе стране имају користи. Купци добијају могућност креирања потребног броја легалних копија софтвера и то по цени која је значајно нижа (обично око 50%) од његове малопродајне цене. Са друге стране, произвођач на овај начин проширује своју корисничку базу и истовремено обесхрабује и дестимулише пиратске покушаје.

3.12.3.2. Софтвер јавног домена

Постоје неки софтвери који нису заштићени ауторским правима. Незаштићени софтвер (онај који се може без ограничења јавно користити), назива се још и софтвером јавног домена (*public domain sofmware*). Субјекти који су креирали овакав софтвер и имају право својине над њим, својевољно су одлучили да га учине доступним свакоме ко жели да га користи.

Такозвано *shareware licenciranje* представља комбинацију најбољих карактеристика заштићеног софтвера и софтвера јавног

домена. Слично као код софтвера јавног домена, shareware софтвер се даје на употребу и бесплатно дистрибуира. Међутим, овде креатор софтвера задржава право својине над њим и захтева од корисника да се региструју и плате неку номиналну новчану накнаду за коришћење. Регистрација омогућава корисницима да редовно ажурирају купљени софтвер, док номинална накнада обезбеђује креатору неопходна новчана средства за наставак рада на развоју тог софтвера.[21]

4. УМЕСТО ЗАКЉУЧКА – КАКО СЕ ЗАШТИТИТИ?

На основу свега изнетог у раду јасно произилази неколико закључака. Упркос постојању различитих могућности за заштиту (технолошких, правних, етичких), безбедност на мрежи је врло осетљива категорија. Изложени су ризику како лични-поверљиви подаци физичких и правних лица, тако и други важни ресурси и садржаји (новчана средства, интелектуална својина, али и само функционисање информатичког система). Због свега тога, многи субјекти су још увек резервисани према масовнијој употреби онлајн система за обављање свакодневних делатности (посебно приликом куповина и плаћања). Проблем онлајн безбедности је вишезначан и никада апсолутно решив. Као што се криминал никада не може искоренити до краја, тако и онлајн безбедност никада неће бити апсолутна. Коначан и максималан циљ је подићи безбедност на што виши а ризике свести на што нижи ниво. За остварење тог циља потребно је ангажовање многих субјеката, а највећи опрез је на крајњим корисницима онлајн услуга. Јер, колико год други бринули о њихово онлајн безбедности, највише морају бринути они сами. Стога, да би безбедност била што већа треба се придржавати неких основних правила и упутстава:

● Никада не треба давати своје личне податке у одговору на непроверене захтеве. Уколико сам корисник није иницирао комуникацију, никада не треба достављати осетљиве личне податке;

● Никада не треба саопштавати лозинке преко телефона или мреже на основу захтева који су непроверени;

21 Понекад се дешава да компанија или појединац понуди свој софтвер по изузетно ниској цени. На овај начин се корисници подстичу на практично бесплатну употребу софтвера, док аутор истовремено јавно прокламује своје право власништва над њим.

● Не отварати пошту чији је пошиљалац тотално непознат;

● Не отварати пошту која садржи послат фајл - привезак (attachment), нарочито не дирати привезак, осим у случају познатог пошиљаоца;

● Не скидати "бесплатне" игре, програме и смајлије тј. емотиконе, пре провере поузданости код веродостојних извора;

● Не инсталирати програме и игре са "бесплатних" и пиратских CD-а и DVD-а. Треба знати да, кад се покрене програм за "крековање" (crack) тј. разбијање шифре за програм који је инсталиран, у већини случајева истог тренутка тај "крек" покушава да се преко интернета, са корисниковог рачунара, јави серверу свог творца. У том тренутку постоји велики ризик по корисников рачунар;

● Инсталирати квалитетан анти вирус програм који обједињује и функције: anti-rootkit, anti-spyware, још боље ако има web-scanner i link-scanner (као рецимо AVG анти вирус) и свакодневно га ажурирати;

● Инсталирати поуздан firewall (заштитини зид) упркос постојању Windows-овог. Његова предност у односу на Windows-ов је, између осталих и та што обавештава кад год се појави неовлашћен или до тада непознат саобраћај на мрежним интерфејсима корисниковог рачунара;

● Стално имати на уму да, колико год изгледало феноменално лако и пријатно делити податке о себи на Фејсбуку, Мајспејсу, Твитеру итд., сваки од њих редовно бива подвргнут прикупљању података о свим корисницима, а сви прикупљени подаци вероватно ће завршити у базама појединих националних служби безбедности (FBI-у и других).

Vidoje Spasić LLD,
Assistant Professor at Faculty law in Niš

ONLINE SECURITY

Summary

Development of information technology, especially mhe internet has led to significant changes in many segments of society. However, the effects of such technological advances are twofold. On the one hand, significantly facilitated and improved opportunities for communication, access to mhe variety of material (content), business activities and transactions, as well as opportunities for various forms of entertainment. However, digital technology and network environment carries certain risks, including adverse effects of different nature. Given that the internet is an open network without a centralized management and control system, one of mhe characteristics of the internet is its vulnerability. In other words, safety on the internet is a very sensitive categories.

There are many ways, forms and subjects that might in any way compromise the security of mhe internet. Malpractice and illegal activities can be compromised private data, intellectual property and other resources and facilities, and, even only functioning network system. Therefore, the provision of online security is a great mission and purpose of the whole society, not only IT specialists that work directly on the network, but also all other entities in any way have a connection to the internet. Of course, we think of all users of internet services, because the destruction and disintegration of mhe internet network system would affect them the most.

Key words: *internet, online security, measure of protection.*