Прегледни рад *UDC: 004.738.5:658.8(497.11), JEL: Z00*

ПОЛИТИКА ПОВЕЋАЊА БЕЗБЕДНОСТИ ПРЕДУЗЕЋА НА ИНТЕРНЕТУ

POLICY INCREASING SECURITY COMPANIES ON THE INTERNET

Славиша Трајковић
Универзитет у Приштини, Економски факултет, К. Митровица
Бојана Милосављевић
Висока техничка школа струковних студија Звечан
Срђан Милосављевић
Универзитет у Приштини, Економски факултет, К. Митровица

Абстракт: *Безбедност предузећа на Интернету је од круцијалне важности за пословање, без обзира на то што су трошкови израде решења неопходних за правилну заштиту веома често доста велики. Сва предузећа која користе Интернет на удару су великих напада и претњи које знају да буду свакодневне. Да би се компаније заштитиле од ризика које са собом носи пословање на Интернету морају се применити одговарајуће мере безбедности. Мере безбедности представљају скуп правила која су укључена у све активности организације у вези са безбедношћу. Због тога свака компанија треба да има адекватну политику безбедности и да се њом континуирано бави.*
У овом раду аутори се баве политиком повећања безбедности на Интернету, безбедношћу мреже и контролом приступа.
Кључне речи: *Предузеће, Политика безбедности, Интернет, Безбедност мреже, контрола приступа*

Absrtact: *Enterprise Security on the Internet is of crucial importance for the business, irrespective of the fact that the cost of developing the solutions necessary for proper protection are often quite large. All companies that use the Internet are being hit high-profile attacks and threats that tend to be everyday. In order to protect the company from risks arising from a business on the Internet must implement appropriate security measures. Security measures are a set of rules that are included in all activities related to safety. That's why every company should have adequate security policy and that it continually engaged.*
In this paper, the authors deal with the policy of increasing Internet security, network security and access control.
Key words: *The company, Security Policy, Internet, Network security, access control*

1. ПОЛИТИКА БЕЗБЕДНОСТИ: ОСНОВА ЗАШТИТЕ НА ИНТЕРНЕТУ

Иако могућност конекције на Интернет нуди огромне предности због могућности већег приступа информацијама, она је опасна због сајтова са ниским нивоом безбедности. Интернет „пати“ од очигледних проблема везаних за безбедност који, уколико се игноришу, могу да имају погубне последице за неприпремљене

сајтове[1]. Предузећа су, с правом, забринута у погледу безбедности коришћења Интернета и постављају следећа питања: 1/ Хоће ли хакери пореметити интерне системе?; 2/ Хоће ли важни подаци предузећа бити угрожени (промењени или прочитани) приликом преноса?; и 3/ Хоће ли предузеће бити доведено у непријатну ситуацију? Све претходно речено представља ваљан разлог за бригу. Појављују се многа техничка решења која се односе на основне проблеме везане за безбедност Интернета. Међутим, њихова је цена веома висока. Многа решења ограничавају функционалност да би повећала безбедност. Остала захтевају значајне уступке на рачун једноставне употребе. Код осталих, особље које ради на традиционалним ресурсима троши време на њихову имплементацију и рад, а захтева се и трошење новца за куповину и одржавање опреме и софтвера.

Политика безбедности на Интернету има за циљ доношење одлуке о томе како ће се предузеће заштитити. Углавном је потребно поделити ову политику на два дела: генералну политику и посебна правила (која су еквивалентна посебној политици система)[2]. Да би политика која се одности на Интернет деловала, творац политике мора да разуме уступке који се чине, политика безбедности се мора синхронизовати са другим одговарајућим питањима политике предузећа.

Интернет је извор од виталне важности који мења начин на који комуницирају и послују многа предузећа и појединци. Интернет, међутим, пати од знатних широко-распрострањених проблема везаних за безбедност. Многе организације и предузећа претрпела су напад уљеза или покушај упада који је за последицу имао губитке у продуктивности или репутацији. У неким случајевима, предузећа су морала привремено да се дисконектују са Интернета и инвестирају знатна средства у исправљање проблема са конфигурацијом система и мреже. Сајтови који нису свесни ових проблема, или им они нису познати, суочавају се са ризиком да их нападну уљези у мрежу. Чак се и сајтови који поштују праксу добре

[1] Behrouz Forouzan, *TCP/IP Protocol Suite (Mcgraw-Hill Forouzan Networking),* New York,2009, Проблеми који су саставни део услуга *TCP/IP*, сложеност конфигурације хоста, рањивости које су унете током процеса развоја софтвера и разни други фактори заједно, допринели су томе да неприпремљени сајтови постану отворени за активности уљеза и проблеме које оне доносе.

[2] Behrouz Forouzan, *TCP/IP Protocol Suite (Mcgraw-Hill Forouzan Networking),* New York,2009.Генерална политика одређује укупан приступ питању безбедности на Интернету. Ова правила дефинишу оно што је дозвољено и оно што није дозвољено. Правила се могу допунити процедурама и осталим смерницама,

безбедности суочавају са новом рањивошћу софтвера и упорношћу уљеза.

Основни проблем је тај што Интернет није пројектован тако да буде веома безбедан. Неки од проблема везаних за Интернет са садашњом верзијом *TCP/IP* су:

- Могућност једноставног прислушкивања и копирања[3]
- Рањивост услуга TCP/IP[4],
- Недостатак политике[5], и
- Сложеност конфигурације.[6]

1.1. НАЈВАЖНИЈИ ТИПОВИ ПОЛИТИКЕ БЕЗБЕДНОСТИ

Политика безбедности рачунара сваком човеку значи нешто друго. Она може значити директиву вишег руководства за израду програма безбедности рачунара, одређивање његових циљева и утврђивање одговорности, може се односити на одлуке руководства средњег нивоа по питањима као што су приватност е-мејлова или безбедност факсова. Или, она може значити правила за техничку безбедност одређеног система[7].

У овом поглављу се термин политика безбедности рачунара дефинише као документација о одлукама везаним за безбедност рачунара – која обухвата све претходно описане типове политике. Приликом доношења одлука руководиоци се суочавају са тешким изборима у које спадају стратегија предузећа, циљеви конкурентности и додела ресурса. Ови избори подразумевају заштиту техничких и информационих ресурса као и давање упутстава запосленима о понашању[8].

---

[3] Већина промета на Интернету није криптована. Помоћу већ постојећих софвера могуће је пратити и контролисати е-мејл, лозинке и пренос датотека

[4] Велики број услуга TCP/IP нису пројектоване да буду безбедне, па их познаваоци упада могу угрозити. Посебно су рањиве услуге које се користе за тестирање

[5] Многи сајтови су ненамерно конфигурисани за широко-отворен приступ Интернету не водећи рачуна о евентуалној злоупотреби са Интернета. Многи сајтови допуштају више услуга TCP/IP него што им је потребно за рад и не покушавају да ограниче приступ информацијама о својим рачунарима које би могле да послуже уљезима

[6] Веома често је конфигурисање и праћење команди за безбедан приступ хосту компликовано. Команде могу случајно да буду погрешно конфигурисане што за последицу може имати неовлашћени приступ

[7] Ово су типови политике који се спроводе како техничким командама система тако и командама руководства и оперативним командама

[8] John R. Vacca, *Practycal Internet Secyre*, Ohio: Pomeroy, 2007.

Углавном, политику одређује руководилац. У неким случајевима, међутим, може је одредити и група (одбор за одређивање политике у оквиру предузећа.

Основни елемент политике је тај да она представља одлуку. Политика одређује смернице неког предузећа. Да би политика била корисна, битно је да разне претхнодне смернице буду реално изабране. Како политика одређује смернице, она се може користити као основа за доношење осталих одлука нижег нивоа. Политика високог нивоа се не мора често мењати.

Битно је и то да се политика примењује тако да предузеће стварно иде у том смеру. Два уобичајена проблема са организационом политиком су: Политика је само нешто о чему се стално говори, а не одлука или смерница; и политика се, уствари, не примењује у предузећу. То је парче папира које се показује ревизорима, адвокатима, другим компонентама предузећа или клијентима, али оно не утиче на понашање. Неки примери могу да нам послуже да лакше објаснимо ове битне елементе политике.

Одлуке руководства по питањима безбедности рачунара веома се разликују. Њихова категоризација у три основна типа може помоћи у одређивању разлика између разних врста политика:

- *политика програма*
- *политике неких одређених питања*
- *политике неких одређених система.*

Политика програма: Политиком програма постављају се стратешке директиве предузећа у погледу безбедности и одређују ресурси за њену примену. Политика програма се користи за израду програма за безбедност рачунара предузећа. Руководилац, обично особа која је на челу предузећа, или руководилац администрације издаје политику програма за постављање (или реконструкцију) програма за заштиту безбедности рачунара предузећа и његове основне структуре. Политика високог нивоа:

1. Дефинише сврху програма и његов обим у оквиру предузећа.
2. Додељује одговорност (предузећа за безбедност рачунара) за директну имплентацију програма као и друге одговорности релевантних канцеларија као што је Организација за управљање информатичким ресурсима (*Information Resources Management, IRM).*
3. Бави се питањима усаглашености.

Политике неких одређених питања: Политика неких одређених питања бави се одређеним питањима која се тичу предузећа; док је намена политике програма широког обима и односи се на безбедности рачунара у целом предузећу. Приликом елаборације политике неких одређених питања, у центар пажње се стављају области које су тренутно релевантне и важне (а понекад контроверзне) за неко предузеће. Руководство може сматрати да је, на пример, потребно издати политику приступа предузећа

планирању у случају непредвиђених околности (централизовано насупрот децентрализованом) или примени неке одређене методологије у управљању ризиком по системе. Може се, на пример, издати и политика о правилној употреби најсавременије технологије (чија је рањивост у погледу безбедности још увек веома мало позната) у предузећу. Политика у погледу неког одређеног питања може бити потребна и када се појаве нова питања као што је примена недавно донетог закона којим се захтева додатна заштита одређене информације. Политика програма је обично довољно широка да не захтева много измена током времена док ће политика у погледу одређеног питања захтевати чешће ревизије јер долази до промена у технологији и одговарајућим факторима[9].

Политика неких одређених система: Политике неких одређених система[10] концентришу се на одлуке које доноси руководство да би се заштитио одређени систем. И политика програма и политика одређеног питања баве се политиком ширег нивоа која обично обухвата цело предузеће. Међутим, оне не пружају довољно информација или директива које би се, на пример, користиле за утврђивање листа за контролу приступа или у обуци корисника о дозвољеним поступцима. Политика одређеног система допуњује ову потребу. Она је усмеренија јер се бави само једним системом.

Многе одлуке у погледу политике безбедности могу се примењивати само на нивоу система, и у оквиру истог предузећа, могу варирати од једног до другог система. Мада може изгледати да су ове одлуке сувише детаљне да би биле политика, оне могу бити изузетно важне, са знатним утицајем на употребу система и безбедност. Ове врсте одлука може донети неки руководилац, а не технички администратор система[11].

Технички приступ политици: Постоји четврти тип политике дефинисан у литератури о безбедности Интернета. То је технички

---

[9] Углавном, политику одређеног питања и политику одређеног система издаје виши функционер. Што је више она глобалног, контраверзног карактера или што више ресурса захтева то је виши руководилац издаје.

[10] Систем се односи на скуп свих процеса, и оних који се ручно извршавају и оних који користе рачунар (ручно прикупљање података и накнадна манипулација путем рачунара), који врше неку функцију. Овде спадају и апликациони и системи за подршку као што је мрежа.

[11] John R. Vacca, *Practycal Internet Secyre*, Ohio: Pomeroy, 2007.

Технички администратор система, међутим, често анализира утицај ових одлука. Треба имати на уму да се политика не креира у вакууму. На пример, битно је разумети мисију система и начин на који ће се систем користити. Корисници, такође, могу играти важну улогу у одређивању политике.

приступ. У овом раду се технички приступ дефинише као анализа која даје подршку општој политици и одређеним правилима. Својим већим делом, он је сувише техничке природе да би руководиоци који креирају политику могли да га схвате. Он, сам по себи, није веома користан као политика. Он је, међутим, неопходан за дефинисање могућих решења којима би се дефинисали уступци који су битни елемент у одређивању политике.

Шта треба обухватити конструисањем политике: Корисна структура политике неког одређеног питања је разбијање политике на основне компоненте. Компоненте су следеће:

- констатовање питања
- изјава о ставу организације
- примењивост
- улоге и одговорности
- усаглашеност
- тачке за контакт и додатне информације

Констатовање проблема: Да би се формулисала политика неког питања, руководиоци морају да дефинишу то питање одговарајућим терминима, одредницама и условима. Често је корисно одредити циљ или оправдање за политику – што може бити од помоћи у добијању сагласности за политику. Када се ради о политици безбености Интернета, може бити потребно да се у предузећу разјасни да ли се политика односи на све конекције које раде преко Интернета или само на Интернет. Политиком се, такође, може констатовати да ли се, осим проблемима безбедности, она бави и другим проблемима везаним за Интернет као што су употреба конекција путем Интернета за личне потребе.

Изјава о ставу предузећа: Када се констатује питање и разговара о условима у вези с њим, следећи корак је да се дâ јасна изјава о ставу предузећа (одлука руководства) по овом питању. У њој ће се навести да ли је дозвољена конекција путем Интернета или није и под којим условима.

Примењивост: Политика у погледу одређеног питања треба да садржи и изјаве о примењивости. То значи да треба објаснити где, како, када, на кога и на шта се примењује одређена политика. Да ли се она примењује на све компоненте организације? Службе које се баве јавним пословима могу бити изузете од рестриктивне политике.

Улоге и одговорности: Потребно је, такође, одредити улоге и одговорности. Може бити потребно да се за сложена питања, какво је питање безбедности на Интернету, дефинишу техничке улоге које ће извршити анализу безбедности разних архитектура или ће, можда,

бити потребно да се дефинише улога руководства које даје одобрења. Може бити потребна и улога праћења.

Усаглашеност: Можда је за неке типове политика у погледу Интернета потребно детаљније описати недопустиве повреде закона и последице таквог понашања. Могу се изричито навести и казне, с тим што оне морају бити у складу са кадровском политиком предузећа и његовом праксом. Када се примењују, треба их координисати са одговарајућим руководиоцима и службама и, вероватно, јединицама које заступају запослене.

Тачке за контакт и додатне информације: Уз сваку политику неког одређеног питања, треба навести особе у предузећу од којих се могу добити нове информације, смернице и усаглашеност. Како радна места ређе имају тенденцију промене него људи који их заузимају, можда је боље да као тачке за контакт буду одређена поједина радна места.

Добијање одобрења: Политика (добра политика) може се написати само за одређену групу са сличним циљевима. Због тога ће можда бити потребно да се неко предузеће, уколико је сувише велико или сувише разнолико да би било предмет политике безбедности на Интернету, подели на компоненте, на пример NIST[12]. Мисија NIST захтева обимну научну сарадњу у отвореном окружењу. Друга компонента DOC има потребу да чува у тајности поједине статистичке упитнике. Са таквим различитим мисијама и потребама, централна политика безбедности на Интернету DOC-а вероватно није потребна. Чак и у оквиру NIST-а постоје знатне разлике у мисији и потребама, па је тако да већина политика безбедности на Интернету постављена на нижи ниво него у NIST-у.

Везе са другим областима политике: Интернет је један од многих начина интеракције неког предузећа са спољним ресурсима. Политика Интернета треба да буде у складу са другим политикама које посредују у приступу споља. На пример:

- физички приступ згради (зградама) или кругу предузећа
- интеракција са јавношћу/медијима
- електронски приступ

Физички приступ згради (зградама) или кругу предузећа: У неком смислу, Интернет представља електронска врата за улаз у предузеће. И добре и лоше ствари користе иста врата. Предузеће чији је физички круг отворен вероватно је већ донело одлуку, узимајући у обзир ризик, да је отвореност или битна за мисију

[12] NIST (Национални институт за стандарде и технологију) је организација која је део Министарства трговине (Department of Commerce (DOC).

предузећа, или да је претња мала, или да је сувише скупо ублажавати је. Слична логика се може применити и на електронска врата. Међутим, постоје важне разлике. Физичке претње су директније везане за физичко место. Повезивање на Интернет је повезивање са целим светом. Предузеће чији се физички погон налази на далеком и питомом месту, рецимо у Монтани, може имати отворен физички круг, али му је, ипак, потребна рестриктивна политика у погледу Интернета .

Интеракција са јавношћу/медијима: Интернет може бити облик јавног дијалога. Многа предузећа, како у Србији тако и у свету, дају упутства својим запосленима о начину рада са јавношћу или са медијима. Вероватно ће бити потребно да се ове политике портују на електронске интеракције. Многи запослени можда нису свесни јавне природе Интернета.

Електронски приступ: Интернет није само средство за рад преко мреже. Предузећа користе телефонски систем (јавна телефонска мрежа) и неке друге јавне и приватне мреже за конекцију спољних корисника и рачунарских система на интерне системе. Конекцијом на Интернет и телефонски систем могу се избећи неке претње и рањивости .

2. СЛАБОСТИ ПРЕТРАЖИВАЧА

Ово поглавље се бави ризицима од рада преко Internet Explorer-а и Firefox-а. Ови се претраживачи најчешће злоупотребљавају због тога што се они најчешће користе.

Internet Explorer

Мајкрософт је, само током 2005. године, издао бројне надоградње којима су се исправљали многи проблеми у погледу безбедности. То су оне рањивости које је Мајкрософт препознао. Постоје и рањивости које Мајкрософт још није исправио и представљају чак и већу претњу јер за њих још увек нема пачова.

Овде одабран пример представља рањивост Internet Explorer-а која није пачована и коју ћемо детаљно објаснити. Рањивост се бави статусном линијом (*статус бар*), а то је простор у Internt Explorer-у (и свим другим претраживачима) у доњем левом углу који, између осталог, приказује дестинацију хиперлинка на који сте тренутно поставили свој курсор. Због бага у Internet Explorer-у могуће је направити линк који ће на статусној линији показати један веб сајт, а у стварности вас одвести на неки други веб сајт.

Ова рањивост садржи претњу јер ћете ви можда помислити да сте отишли на веб сајт своје банке, а уствари сте отишли на веб сајт

који је израдио нападач у покушају да прибави податке о вама путем фишинга. Важно је да имате у виду да ова рањивост постоји и у MS Outlook Expres-u[13].

Mozilla Firefox

Firefox је врло брзо стекао популарност као веб претраживач. То је скраћена верзија веб претраживача Mozilla. Он има неке предности у погледу безбедности, међутим не садржи подршку за технологије као што су MS Active X[14] које су, игром случаја, поставиле пред Internt Explorer многе проблеме у погледу безбедности. Не раде сви веб сајтови/апликације у Firefox-у, али се већина слаже да је он добар за опште претраживање веб-а. Наравно, као и сваки софтвер и Firefox има својих проблема у погледу безбедности. Он садржи баг сличан оном који је објашњен за Internt Explorer с тим што је за њега злоупотреба мало другачија. И он дозвољава злонамерном кориснику да „имитира" стварну дестинацију линка на веб сајту. У овом случају то успева само онда када се налазите на линку, кликнете десним дугметом и изаберете „Save Link As..." (*Сачувај линк као*...). Ова злоупотреба успева само са верзијом Firefox-а 1.0.1 а, како изгледа, у каснијим верзијама проблем је решен. Уколико то пробате код 1.0.3 и 1.0.4, можете видети „скривени" линк на http://www.google.com уколико кликнете и задржите дугме миша на линку или кликнете десним дугметом и изаберете „Save Link As".[15] Интересантно је да рањивост која је била намењена Firefox-у боље успева у Internt Explorer-у. Без обзира на то, још увек не постоји злоупотреба који добро успева код оба.

3. БЕЗБЕДНОСТ МРЕЖЕ

Приступ Интернету је постао неопходан за нормалан рад практично сваког предузећа. Судећи по аналитичарима, још је током 2006. године преко 90% свих испитаника оценило је Интернет као средње до изузетно важног извора информација. Студије показују да је у предузећима:

- Увелико допринео лакшој сарадњи између запослених, партнера, испоручилаца и клијената помоћу средстава као што су е-мејл, дељење датотека и веб конференције.

[13] http://windows.microsoft.com/en-US/internet-explorer/products/ie/home. 11.04.2011.
[14] http://www.microsoft.com/security/resources/activex-whatis.aspx.11.04.2011.
[15] http://www.google.com.12.04.2011

- Омогућио брз приступ информацијама путем претраге интернета, базе података и електронске обуке.
- Омогућио јефтино пружање услуге спољним предузећима преко веб сајтова, дистрибуције е-мејлова и апликација електронске трговине.

Употреба Интернета је веома распрострањена у већини предузећа чиме им је омогућено да повећају продуктивности и квалитет услуга, а истовремено, смање трошкове.

Са овом широко распрострањеном употребом дошло је до промена у односима корисника и руководства. Приступ Интернету више не представља луксуз. То је обавезан захтев за предузеће. На свим нивоима у предузећу приступ треба да буде неоптерећен, транспарентан и непрекидан.

3.1. РИЗИЦИ ПО БЕЗБЕДНОСТ У ОВОМ ТРЕНУТКУ

Нажалост, Интернет има и тамну страну. Онако како предузећу обезбеђује транспарентан приступ бројним спољним изворима, он може да обезбеди и спољним странама, од којих неке нису добронамерне, релативно лак приступ интерним рачунарима и информацијама предузећа. Постоји ризик за све врсте предузећа.[16] Чак су и високософистикована предузећа, каква су произвођачи рачунарских игрица, доживела упад путем Интернета. Информације и изворни код једног произвођача игрица чији је производ требало да буде пуштен у продају били су постављени на Интернет, упад који је имао озбиљне финансијске последице. Следе неке чињенице о безбедности мреже:

- просечни трошкови упада споља 2006. године: 660.000 долара
- просечни трошкови инфекције вирусом 2006. године: 125.000 долара
- просечни трошкови напада ускраћивањем услуге 2006. године: 631.000 долара

Запањујућа је разноврсност метода који се користе за злонамеран приступ рачунарима предузећа или напад на њих. Поврх свега, испоставило се да је неодговарајућа интерна употреба Интернета велики проблем.

[16] Један 22-годишњи хакер је из хира скенирао Интернет гејтвејове New York Times-a и успео да приступи бројним базама података које су садржале личне податке о изворима, запосленима и клијентима.

3.2. ПРОЦЕНА РИЗИКА

Свако ко се конектује на Интернет се суочава са много разних реалних претњи. Прво питање с којим се суочава свако предузеће са ограниченим ресурсима је: Уколико има претњи, која је од њих толико битна да оправда трошак и пажњу руководства. Почетна тачка карактерише податке праћења у току једне године, које су спровели FBI и Институт за безбедност рачунара (*Computer Security Institute*). Резултати показују да сада око 84% предузећа наводи Интернет као извор честих напада с тим што проценат тих честих напада стално расте. На жалост, не расте само обим напада, већ се повећава и њихова разноврсност и софистикованост. Недавни извештаји које су дали привредни аналитичари о водећим компанијама у области ИТ показују да је 67% до 86% водећих компанија у области ИТ код којих је урађена анализа током 2006. године претрпело пет врхунских облика *упада* (успешних напада)! Статистика ненамерно штетних претњи је подједнако битна. Наиме: 46% свих е-мејлова данас је спам; а у 2006. години, 65% од анкетираних запослених са приступом Интернету изјавило је да користи веб за обављање личних послова док је 62% изјавило да користи е-мејл за личне трансакције.

Ови подаци јасно показују да свако предузеће, без обзира на величину, има разлога да верује да ће бити мета великог броја разних претњи у вези са Интернетом. Економски утицај тих претњи је тешко квантитативно одредити јер се они разликују у зависности од врсте предузећа (комерцијалне организације, непрофитне организације итд.), природе упада, плата и тако даље. Међутим, неке опште статистике дају идеју о значају тог утицаја:

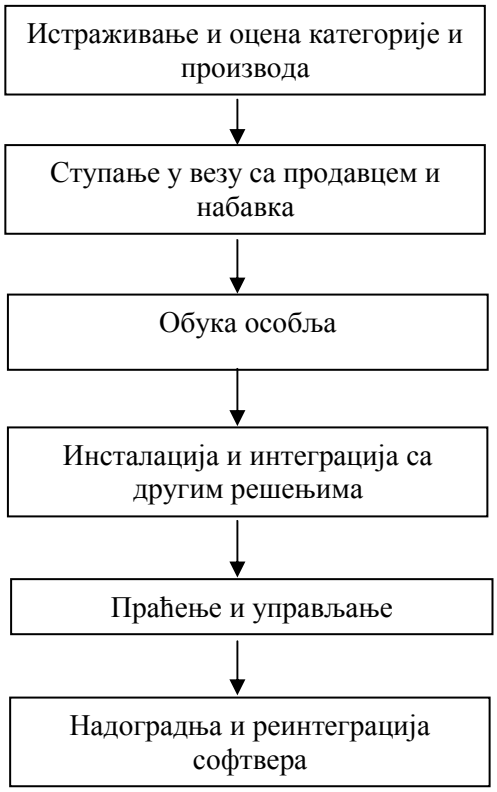
- Према извештају FBI/CSI о анализи 1.058 предузећа, просечни трошкови упада споља током 2006. године били су 771.000 долара.
- Просечни трошкови напада ускраћивањем услуге 742.000 долара .
- Према извештају ICSA, просечни трошкови инфекције вирусом (25 или више PC рачунара) током 2006. године били су 136.000 долара.
- Штете од тужби због рада у непријатељском окружењу кретале су се од 70.000 долара до више милиона долара.

Очигледно да су економски и организациони утицаји толики да не само да гарантују већ и захтевају инвестирање у заштитне мере против сваке веће претње.

3.3. ПРОБЛЕМИ СА АРХИТЕКТУРАМА ЗА ЗАШТИТУ ЗАСТАРЕЛИХ МРЕЖА

Значајно питање је како ће се из застарелих компоненти (производа, продаваца и категорија безбедности) саставити делови ефикасног решавања питања безбедности. Као прво, свака компонента захтева инвестирање, не само у погледу трошкова за софтвер и хардвер, већ и у погледу претходног и константног рада. Јединствени услови инсталирања, параметри конфигурације, кориснички интерфејс и потребе руководства захтевају посебну обуку и административну процедуру.

Слика 1.: Главни трошкови решавања питања безбедности током њеног животног циклуса



У ситуацији када су кадрови ИТ који управљају постојећим апликацијама преоптерећени, додавање још једног софтвера и хардвера који захтевају стручност представља проблем, чак и уколико постоје финансијска средства (види сл.1.).

Мора се узети у обзир и укупан квалитет решења која се односе на безбедност. Безбедност је онолико јака колико и њена најслабија

карика. За већину предузећа велики број разноврсних појединачних решења која су потребна за стварање ефикасне одбране, разумевање и избор одговарајућих компоненти представљају оптерећење. Укратко, тренутни приступ изради заштитног штита повезивањем разноврсних појединачних производа представља проблем нарочито за предузећа са ограниченим бројем кадрова и средстава.[17]

3.4. РЕШЕЊЕ СЛЕДЕЋЕ ГЕНЕРАЦИЈЕ: ИНТЕГРИСАНА ПЛАТФОРМА ЗА ЗАШТИТУ МРЕЖЕ[18]

Да би се превазишли ови проблеми и удовољило потребама данашњег предузећа које има ограничене ресурсе, решење које се односи на безбедност треба да има следеће атрибуте:

- Да обухвата заштиту од свих најчешћих претњи тиме што ће, као минимум, обезбедити фајервол, заштиту од вируса, филтрирање УРЛ-а, ВПН, функционисање заштите бежичног система и заштите од спама.
- Да за сваку претњу обезбеди решења светске класе. Безбедност је само онолико јака колико и њена најслабија карика.
- Да ради на једној хардверској платформи која се са повећањем обима протока може надограђивати тако да се оно што је инвестирано у постојеће решење неће одбацивати.
- Да се инсталација свих компоненти, укључујући и безбеднији оперативни систем, врши са једног ЦД-а. Друга могућност је да он треба да буде испоручен претходно инсталиран на хардвер.
- Да се између свих компоненти врши размена информација о конфигурацији да би се смањили напори и грешке у администрацији.
- Да буде обезбеђен уобичајен управљачки интерфејс за све безбедносне функције и да помоћу парадигме пронађи и кликни, административни рад и потреба за обуком буду сведени на минимум.
- Да буде пројектован као софтверска платформа на тај начин да нове претње могу бити интегрисане чим се

[17]Preston Gralla, *How to Internet Works*, Indianapolis, IN : Que Pub, 2007.
[18] Sumith Gosh, Manu Manel, and Edvard A. Stork, *Guarding your Business, A menagment Aproach to Security*, Kluwer Academy, New York: Plaenum Publisher, 2009.

појаве, а да при том не мора да се одбаци постојеће решење.

- Да обезбеди аутоматску надоградњу функција свих безбедносних и оперативних система у једном Интернет извору уз минималне трошкове рада и минималне рупе у безбедносном систему.

И најзад, и аналитичари из ове области и многи продавци признају да је све ово неопходно. Међутим, продавци постојећих решења наилазе на велике препреке у испуњавању ових потреба:

- Уколико производ није посебно пројектован као интегрисана безбедносна платформа, водећи рачуна о томе како су различите апликације интегрисане у кориснички интерфејс, о конфигурацији и о нивоима времена извршавања програма, прилично је тешко ефикасно и без видљивих спојева „додати“ додатну безбедносну функцију.
- Производе који су везани за одређене хардвеске платформе успорава чињеница да нове функције софтвера мењају обраду података, меморију и потребну меморију хардвера што обично захтева нову платформу.
- Ниједан продавац нема ни ресурсе нити посебне вештине којима би обезбедио решења светске класе за разне претње које ће бити послате на његову адресу.

Овај проблем захтева нови приступ[19].

[19] Примедба**:** Предузећа теже приступу који подразумева интегрисане платформе за заштиту мреже. Чвршћом интеграцијом и заједничким управљањем решењима у погледу безбедности обезбедиће се боља блокада напада и мањи укупни трошкови власништва за клијенте.

Интернет је незамењив елемент пословања. Његова популарност привлачи све већи број непожељних елемената који све више и све чешће лансирају софистиковане и разноврсне нападе. Да би изашли на крај са непријатељским окружењем, корисницима је потребан комплетан безбедносни штит. И најзад, предузећа са ограниченим бројем кадрова и ограниченим средствима нису у стању да изграде штит од разних производа који потичу од разних продаваца. Нити је такав приступ пожељан из перспективе безбедности или управљања.

4. КОНТРОЛА ПРИСТУПА

У комплексном пословном свету данашњице који се стално мења свима - и запосленима, и партнерима, и клијентима, и продавцима, и извођачима радова - су потребни различити нивои приступа различитим областима локалне мреже (LAN) у различито време, за различите пословне циљеве. Због тога предузећа морају имати решења безбедног пословања која, у свакој тачки приступа мрежи, пружају могућност детекције и гоњења. У ту сврху предузећима је потребан свеобухватан, стратешки приступ контроли приступа. Звучи прилично једноставно: ко улази, а ко не. Међутим, проблеми у вези с тим могу бити сложени, а претње су стварне и све су веће.

Замислите ово: више од 90 посто од 530 компанија које су биле анкетиране у једној анализи у овој области признало је да је претрпело упаде кроз безбедносни систем. То не изненадјује, 82 посто од предузећа идентификовало је спољне претње као што су хакери као вероватан извор ових упада, али је 77 посто ових предузећа идентификовало и незадовољне запослене као други вероватни извор. Због тога паметна предузећа не посвећују посебну пажњу само спречавању неовлашћеног приступа, већ и политици детекције и гоњења у свакој тачки приступа за све овлашћене кориснике.[20]

Проблем број један је опште уљуљкивање да ће, уколико до њега дође, упад кроз систем безбедности слабо утицати на предузеће. Веома велики број предузећа, чак ни она боља и већа, не дају довољно ресурса за стратегију превентиве, а троше огромне количине ресурса када дође до невоље или када настане проблем.

Међутим, знатан број мрежа предузећа још увек има рањивости, укључујући и незаштићене LAN портове, који представљају лак плен за вирусе, хакере и злонамерне кориснике. У Анализи рачунарског криминала и безбедности коју је издао Институт за рачунарство FBI за 2006. год.[21] констатује се да многа предузећа једноставно не знају шта се дешава на њиховим мрежама.

Ова се предузећа суочавају са великим ризиком и имају мале шансе даураде пробно одитовање да би пронашли како или зашто је дошло до неког инцидента. Међутим, постоји бољи начин.

[20] Sumith Gosh, Manu Manel, and Edvard A. Stork, *Guarding your Business, A menagment Aproach to Security*, Kluwer Academy, New York: Plaenum Publisher, 2009.

[21] (The 2006 FBI/Computer Science Institute Computer Crime and Security Survey)

Ивица мреже је место где се корисници и апликације конектују, где улази проток података и где мрежа мора да одреди како треба манипулисати тим протоком. Ивица је место где се најефикасније може спровести политика безбедности, где корисник добија приступ када га провери централни командни извор. Ово поглавље истражује на који начин овај свеобухватни приступ поједностављује управљање приступом мрежи, ствара безбедно, интелигентно ожичено и бежично окружење и обезбеђује финансијски доступну безбедност мреже која детектује све кориснике и спроводи све политике предузећа у свакој тачки приступа.

4.1. ЗАШТО КОРИСТИТИ КОНТРОЛУ ПРИСТУПА?

Када дође до контроле приступа многа предузећа оставе своја виртуелна врата отворена и своје вирутелне прозоре откључане чиме дају неометани приступ разним крајњим корисницима. Недостатак инфраструктуре представља лак задатак за злонамерне кориснике и то је један од разлога што је 80 посто предузећа од оних која су била предмет анализе у Анализи рачунарског криминала и безбедности Института за рачунарство FBI за 2006. годину пријавило интерне инциденте који су се тицали безбедности.

И недостатак мера за контролу приступа представља огромну одговорност за предузећа. На пример, практично нема предузетих мера за контролу приступа. Гост може да приступи LAN-у који садржи осетљиве податке о истраживању и развоју из предворја или са паркинга предузећа. Недостатак мера за контролу приступа може лако да значи губитак тешко стечене интелектуалне имовине предузећа или предности у конкуренцији.

4.2. БЕНЕФИТИ У ПОСЛОВАЊУ

Сваким комплетним решењем контроле приступа морају се идентификовати појединачни корисници, одредити услуге за које ће добити овлашћење и, у складу с тим, одредити нивое њиховог приступа. Једно решење треба да садржи четири кључна елемента:

- Централизовану команду: Она даје могућност предузећу да конструише интелигентно решење контроле приступа којим се нуди централно командовање мрежом.
- Контрола приступа на ивици LAN: Помоћу ње се свичевима и софтверу који се налазе на самој ивици мреже LAN ефикасно додељује могућност приступа, провере и трагања. Када се

контрола приступа доведе на ивицу LAN-а, могуће је одмах доносити одлуке, а не одлагати их до језгра. Тиме се спречава и да евентуални злоћудни проток података добије приступ на LAN.

- Безбедност и једноставност употребе: Обезбеђује се рачунарско окружење које је безбедније, а једноставније јер је она подешена да, сваки пут када се крајњи корисници улогују на њу, препозна ко су они и шта треба да раде.

То је из основа другачији приступ у односу на систем за контролу приступа који многа предузећа тренутно имају и потребно је прећи еволутивни пут да би се стигло до њега. Ово је посебно важно јер ће корисници радо прихватити нове процедуре само уколико су оне лаке, једноставне и граде се на њиховој већ постојећој инфраструктури. Паметна архитектура и јасан пут преласка на њу су битни састојци градње интелигентне мреже која може да пружи безбедност предузећу .

4.3. ПРЕГЛЕД РЕШЕЊА КОНТРОЛЕ ПРИСТУПА

Контрола приступа мрежи личи на аеродром – постоје различити нивои приступа за разне запослене, људи долазе и одлазе у свако доба и морају да провуку картицу за приступ или дају личну карту да би ушли у одређене зоне. Овим се доприноси безбедности разних зона – и заштити и запослених и гостију[22].

У оквиру стратегије командовања/контроле за целокупну архитектуру мреже, предузећа би требало бар да размотре прелазак на систем за контролу приступа у две тачке којим се повезују крајњи корисници са одређеним рачунарима и са одређеним мрежама. Ова провера у две тачке у суштини доводи у везу корисника и рачунар и обезбеђује однос један на једног. Самим овим може се знатно повећати безбедност постојеће мреже. Ефикасна контрола приступа је битни чинилац за предузећа која покушавају да безбедност предузећа и информисање клијената доведу до максимума.

[22] David Hucaby, *CCNP BCMSN-Званични уџбеник за полагање испита* (Четврто издање), 2007. Решавање безбедности контролом приступа треба да понуди комплетно решење од хардвера, софтвера и услуга управљања до апликација, услуга и подршке. Сам хардвер не може да обезбеди укупну контролу приступа, али комбинација хардвера и софтвера плус комплетан сет алата даје основу за потпуно решавање безбедности контролом приступа.

4.4. ИНТЕЛИГЕНТНЕ БЕЗБЕДНЕ МРЕЖЕ

Добро конструисане интелигентне мреже ће, у будућности, имати системе за контролу приступа који ће спречавати 95 посто напада и драстично смањити ризик од интерних проблема пружајући јасан процес пробног одитовања и провере којим ће се купцима омогућити брз приступ и провера. Традиционалне мреже спроводе мере обезбедјења на одређеној тачки што злоћудном протоку пружа прилику да се инфилтрира у језгро мреже. Због тога је веома важно да се заустави неовлашћени проток података на ивици мреже и уђе у траг неовлашћеним корисницима у целој мрежи[23].

4.5. СЦЕНАРИО РЕШАВАЊА ПИТАЊА БЕЗБЕДНОСТИ ПОМОЋУ КОНТРОЛЕ ПРИСТУПА

Решавање питања безбедности мреже помоћу контроле приступа треба да омогући раздвајање мрежа. На пример, LAN је подељена на две серије приступних зона. Уколико запослени неко време ради у безбедној зони, као што је лабораторија за истраживање и развој, он или она мора да има приступ и приватној LAN истраживања и развоја и јавном Интернету. Међутим, уколико изађе из безбедне зоне, његов или њен приступ може бити ограничен само на јавни Интернет да неовлашћени људи не би случајно могли да виде осетљиву информацију. Ово је могуће постићи и без потребе да запослени предузме било какав корак. Мрежа се једноставно подешава на основу њене или његове локације. Исто тако, ако гост посети предворје предузећа пре 9^h, неће моћи да приступи јавном Интернету или LAN-у предузећа. У 9^h гост може да приступи јавном Интернету, али још увек не може да приступи LAN-у предузећа. Најзад, по овом сценарију, путем контроле приступа администратор мреже предузећа може да провери кориснике LAN-а на основу

[23] Постоји чудна дисонанца када 90 посто предузећа извештава о упаду у систем, а многа од њих немају појма о томе шта се дешава у њиховој мрежи. Време је да се суочимо са чињеницама: потреба за комплетним решењима путем контроле приступа никада није била хитнија. Добра вест је та што је контрола приступа проблем који предузећа могу решити. Да би решила овај проблем и заштитила свој LAN, предузећа морају, као прво, изградити серију електронских „врата“ која воде неовлашћене кориснике у одговарајуће „зоне“ информација и услуга – и нигде више. Овим вратима и зонама спречиће се неовлашћена употреба и обезбедити спроводјење политике предузећа у свако доба и на свим местима. Комплетни системи контроле приступа са архитектуром као што је ова могу се градити на постојећој инфраструктури да би, најзад, обезбедили најбезбеднију могућу контролу приступа LAN-у предузећа .

разних фактора у које спадају и припадање некој одређеној групи, идентитет особе, доба дана, физичко место и улога у послу или одговорност. А најважније од свега – продуктивнији крајњи корисници и безбеднија мрежа.[24] Контрола приступа мрежи је огроман задатак – и остаће тако док трендови Интернета, мобилних рачунара и конвергенције настављају да мењају начин рада предузећа.

ЗАКЉУЧАК

Приступ Интернету је постао неопходан за нормалан рад практично сваког предузећа. Судећи по аналитичарима, још током 2006. године преко 90% свих испитаника оценило је Интернет као средње до изузетно важног извора информација. Употреба Интернета је веома распрострањена у већини предузећа чиме им је омогућено да повећају продуктивност и квалитет услуга, а истовремено, смање трошкове.

Студије показују да је Интернет у предузећима:

- Увелико допринео лакшој сарадњи између запослених, партнера, испоручилаца и клијената помоћу средстава као што су e-mail, дељење датотека и веб конференције.
- Омогућио брз приступ информацијама путем претраге интернета, база података и електронске обуке.
- Омогућио предузећима и компанијама већу конкурентност на тржишту.
- Омогућио јефтино пружање услуге спољним предузећима преко веб сајтова, дистрибуције е-мејлова и апликација електронске трговине.

Са овом широко распрострањеном употребом дошло је до промена у односима корисника и руководства. Приступ Интернету више не представља луксуз. То је обавезан захтев за предузеће. На свим нивоима у предузећу приступ треба да буде неоптерећен, транспарентан и непрекидан.

Рачунари предузећа углавном су доступна већем броју људи, неки можда чак и клијентима. Самим тим, сигурност свих наведених система зависи и од успешног ограничавања активности које су на њима допуштене. Успешна брига о рачунарској сигурности предузећа подразумева праћење развоја сигурносних стандарда и

[24] Примедба: Нови модел контроле приступа мрежи захтева заштиту података где год се они налазе и не сме се веровати никоме у потпуности ма где се он налазио.

технологија. Пожељно је унутар предузећа имати особу чији је то задатак.

Улагање у безбедност можда представља трошак за пословање, али онима који се припреме за могуће претње биће од велике користи дугорочно.

ЛИТЕРАТУРА

1. Bhunia, C. T. (2005). *Information Tehnology Network and Internet*, New Delhi: New Age International.
2. Бајагић, М. (2007). *Основи безбедности*, Београд: Криминалистичко-полицијска академија.
3. Centers for Disease Control (http://www.bt.cdc. gov/).
4. Central Intelligence Agency (https://www.cia.gov/,
5. Centre for Defense & International Security Studies (http://www.cdiss.org.)
6. Comer, D. E. (2008). *Computer Network and Internet*, Indiana: Purde Universety.
7. Defler, F. (2008). *How Networks Work*, Michigen: Digital Technologies and the New Media.
8. DARPA Defence Advanced Research Projects Agency (http://www.darpa.mil/)
9. FBI Unit Chief Internet Crime Complaint Center (www.ic3.gov)
10. Gershwin, L. K. (2008). *Cyber Threat Trends and US Network Security*, www.cia.gov.
11. Gralla, P. (2007). *How to Internet Works*, Indianapolis, IN : Que Pub.
12. http://www.coming.rs/business_it/business_it_4/informaciona_bezbednost_pretnje_za_koje_se_moramo_pripremiti
13. http://www.symantec.com/security
14. InfraGard (http://www.infragard.net/)
15. Jo, K. Y. (2010). *Satellite Communication Network Desing and Analysis*, London:Artesh House.
16. Kahn, D. (1996). *The Codebreakers*, New York: Scribner.
17. Niels, F., Shneier, B. (2003). *Practical Crictografhy*, Indianapolis: Wily Publishing.
18. Pratt, P. (2007). *Concept of Database Menagment*, Boston: GEX Publishing.
19. Ranđelović, D., Jaćimović, S. (2010). *Policijska informatika*, Beograd: KPA.
20. Standing, C. (2000). *Internet Commerce Development*, London: Artech House.

21. Steling, W. (2006). *Criptografi and Network security*, New Delhi: New Age International.
22. The Royal Institute of Navigation (RIN) (*http://www.rin.org.uk/*).
23. Trajković, S., Milosavljević, B., Milosavljević, S. (2015): *Повећање безбедности пословања српских предузећа на интернету као услов њихове конкурентности на тржишту*, Међународни научни скуп УКСП-ИС 2015., 5. и 6. новембар 2015, Косовска Митровица
24. Vacca, J. R. (2001). *The Essential Guide To Storage Area Networks*, New Jersey: Prentice Hall.
25. Vacca, J. R. (2003). *Electronic Commerce*, New York: Charles River Media.

Рад је примљен: 08.11.2015.
Рад је прихваћен за штампање: 20.11.2015