НАУЧНО-СТРУЧНИ СКУП СА МЕЂУНАРОДНИМ УЧЕШЋЕМ
Тара, 23-25. мај 2017. године

ПОЛИЦИЈА И ПРАВОСУДНИ ОРГАНИ КАО ГАРАНТИ СЛОБОДЕ И БЕЗБЕДНОСТИ У ПРАВНОЈ ДРЖАВИ

Том 1

Тематски зборник радова

КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКА АКАДЕМИЈА
ПРАВНИ ФАКУЛТЕТ УНИВЕРЗИТЕТА У КРАГУЈЕВЦУ
ФОНДАЦИЈА „ХАНС ЗАЈДЕЛ“
Београд, 2017.

ИНТЕРНЕТ ЦЕНТРИ ЗА ЖАЛБЕ ГРАЂАНА И САЈБЕР КРИМИНАЛ

Слободан Недељковић
Министарство унутрашњих послова Републике Србије
Проф. др Драган Ранђеловић
Доц. др Кристијан Кук
Криминалистичко-полицијска академија, Београд
Војкан Николић
Министарство унутрашњих послова Републике Србије

Апстракт: Од појаве првог компјутера средином 20. века, па све до данас, у протеклих педесетак година, дошло је до енормног пораста коришћења компјутера и њихове широке употребе у људској заједници. Може се рећи да су данас компјутери, који су интегрисани у рачунарске мреже и основа су рада различитих информационих система, пронашли своју примену у скоро свим областима живота и рада људи. Развијањем информационих технологија, Интернет, као мрежа свих мрежа, постао је један од најмоћнијих и широко доступних комуникационих медија на планети. Коришћење Интернета и информационих система базираних на Интернет технологијама у савременом друштву реална је последица глобализације и ере информационо-комуникационих технологија у којој се налази људско друштво. Како се помоћу Интернета преносе и чувају важни подаци и врше осетљиве комуникације, сваки корисник мора бити свестан и могуће њихове злоупотребе. Злоупотреба података и рачунарски безбедносни инциденти везани за Интернет данас су честа појава јер је убрзани развој информационо-комуникационих технологија и информатичке науке, с циљем стварања добробити за човека, нажалост омогућио и развој нових метода напада и угрожавања рачунарских система.

Због бројних и разноликих сигурносних претњи присутних на Интернету, сваки корисник врло лако може постати мета напада. Обезбеђивањем одговарајућег система заштите, и пре тога

превенције, та опасност се смањује, али не отклања. У том смислу, овај рад, који се бави Интернет центрима за жалбе грађана као једном битном претпоставком обезбеђивања сигурности на Интернету, представља скроман допринос том циљу.

УВОД

Од појаве првог компјутера, средином прошлог века, дошло је до енормног пораста њихове употребе. Може се рећи да су данас компјутери пронашли своју примену у свим областима живота и рада људи. С развојем информационих технологија, Интернет је постао један од најмоћнијих и широко доступних комуникационих медија на планети. Било ради забаве, учења, рада, међусобног комуницирања или обављања неке друге делатности, чињеница је да људи свакодневно користе услуге које им пружа Интернет. Коришћење тих услуга у данашњем, савременом друштву није привилегија појединаца већ реалност глобализације и ере информационо-комуникационих технологија. Брз, лак и једноставан приступ Интернету проширује могућности сваког човека да повећа продуктивност у раду, олакшава комуникацију и смањује трошкове рада. Знајући да се путем Интернета преносе и на Интернету чувају важни подаци и врше осетљиве комуникације, сваки корисник мора бити свестан могућности њихове злоупотребе[1].

Управо злоупотреба поверљивих података, рачунарски безбедносни инциденти, честа су појава у модерно доба. Убрзан развој технологије и рачунарске науке, иако са циљем стварања нечег доброг и корисног за човека, омогућио је и развој нових метода напада и угрожавања рачунарских система и мрежа. Због бројних и разноликих опасности које „вребају“ на Интернету, сваки корисник врло лако може постати мета напада. Обезбеђивањем адекватног система заштите и радом на превенцији, та опасност се смањује, али не и отклања у потпуности. Неопходна је стална опрезност, која захтева техничку стручност и познавање правне регулативе. Овај рад се бави Интернет центрима за жалбе грађана, као једном од значајних претпоставки за већу сигурност рада на Интернету.

ИНТЕРНЕТ

Почеци Интернета везују се за стварање ARPANET-а. То је пројекат министарства одбране САД из шездесетих година прошлог века, који је пре свега био намењен војним потребама. Средином осамдесетих година, након издвајања војног сегмента мреже, MILNET-а (*Military Network*), и прикљу-

1 Комлен-Николић, Л.: *Сузбијање високотехнолошког криминала*, Удружење јавних тужилаца и заменика јавних тужилаца у Србији, Београд, 2010.

чивања многобројних академских и комерцијалних чворова, настаје Инетернет.

Данас Интернет повезује велики број компјутера широм света и представља отворену информатичку мрежу која се свакодневно шири укључивањем нових компјутера и компјутерских мрежа. Термин „интернет“ користи се и са малим и са великим словом „И“. Интернет са малим „и“ означава мрежу рачунара повезаних тако да могу да комуницирају. Интернет са великим словом „и“ је посебан назив за мрежу која обједињава многе мање локалне, националне, регионалне и градске мреже, стварајући једну огромну глобалну мрежу која покрива целу нашу планету.[2]

Сагледавајући његове могућности, са сигурношћу можемо рећи да је Интернет један од највећих изума у области средстава за комуникацију. Омогућава једноставну комуникацију и представља производ спајања рачунара, медија и телекомуникација.

Срце Интернета је DNS (*Domain Name Service*). То је начин на који рачунари међусобно комуницирају и раде све ствари, међу којима и размену електронске поште или приказивање веб страна. IP користи информације о Интернет адресама и DNS да би испоручивао пошту и друге информације између рачунара.

DNS креира хијерархију домена и група рачунара и установљава име домена (познато као Интернет адреса) за сваки рачунар на интранету и Интернету, користећи слова и речи уместо бројева. Главни домени такође имају одговорност да одржавају листе адреса и домена који су испод њих. Следећи ниво је одговоран за домене испод и тако даље.

Данас је у стандардној употреби више познатих Интернет сервиса, иако су неки од њих непознати великој већини корисника:

• WWW (*World Wide Web*), као синоним за Интернет и основни сервис који подржава рад са мултимедијом уз помоћ прегледача (софтвера за читање *World Wide Web* презентација као што су *Mozilla Firefox*, *Google Chrome*, *Microsoft Internet Explorer* итд.);

• имејл сервис, који омогућава слање текста, звука, слика, видео снимака користећи одговарајуће софтверске алате три групе: сервера као што су *Sendmail*, *Microsoft Exchange Server*, *Postfix* и *Exim*, клијената као што су *Opera Mail*, *Mozilla Thunderbird* и *Windows Live Mail*;

• FTP (*File Transfer Protocol*) јесте сервис који омогућава пренос фајлова, али због компликованијег начина коришћења у односу на *World Wide Web* тај сервис преузима ту функцију преноса.

2 Ранђеловић, Д.: *Управљање информационим системима и њихова заштита*, КПА, Београд, 2014, стр. 48.

Рачунарство у облаку

Почетком 21. века на Интернету се појављује и и рачунарство у облаку (*Cloud Computing*) и његове апликације везане за Интернет, као што су *Office 365*, *OneDrive*, *SharePoint* итд. То је у суштини било који ИТ сервис који се налази (хостован) ван локације канцеларије и стана, свакако на напреднијој и моћнијој опреми која има много бржу Интернет конекцију него што је то случај у било којој обичној канцеларији и стану.

Office365

Office365 је бренд *Microsoft*-а који користи групу софтвера и услуга, који заједно пружају продуктивнији софтвер и пратеће услуге претплатницима. За кориснике, услуга омогућава коришћење апликације *Microsoft Office* на *Windows*-у и *MacOS*-у, даје простор за складиштење на *Microsoft cloud storage*-у помоћу сервиса *Onedrive* и бесплатне *Skype* минуте месечно. Нуди сервисе који пружају имејл и друштвене мреже хост верзијом *Exchange Server*-а, *SharePoint*-а и *Office Online*-а.

Microsoft SharePoint Designer

Microsoft SharePoint Designer је бесплатан HTML едитор произвођача *Microsoft*. Део је *SharePoint*-а који не долази са *Office*-ом већ се скида са интернета. *SharePoint Designer* и *Microsoft Expression Web* наследници су *Microsoft FrontPage*-а као програма који је у пакету *Office* био намењен веб дизајну.

Onedrive

Onedrive (познат по ранијем називу *SkyDrive*) јесте бесплатана апликација која омогућава аутоматску синхронизацију датотека на различитим рачунарима. Тај програм омогућава аутоматски приступ сопственим документима са различитих рачунарских платформи *Windows*, *Mac* или *iPad*, при чему је омогућено и дељење и рад на документима помоћу одговарајућих прегледача и едитор-апликација.

Internet of Things

Почетком 21. века на Интернету се појављује нова мрежа, Интернет ствари (*Internet of Things – IoT*), која се односи на мрежу физичких објеката или „ствари“ са уграђеном електроником, софтвером, сензорима и конективношћу који објектима омогућавају размену података са произвођачем, оператером и/или другим повезаним уређајима.

Термин *The Internet of Things* предложио је Кевин Ештон 1999. године. Појам Интернета ствари први пут је постао популаран преко центра за

AutoID Center на MIT у вези са тржиштем иако је о концепту разговарано још од 1991. Идентификатори радио-фреквенција (RFID) виђени су као предуслов за *The Internet of Things* у раним данима. Када би сви објекти и људи у свакодневном животу били опремљени идентификаторима, они би били меморисани у компјутеру. Поред коришћења RFID-а, означавање се може постићи помоћу технологија као што су приближна поља комуникације, баркод, QR код и дигитални водени жиг. Према Гартнеру (Gartner), биће скоро 26 милијарди уређаја на Интернету ствари до 2020. Због тога ће морати да користе протокол IPv 6 да прими изузетно велики адресни простор који је потребан.

Безбедност информација на Интернету[3]

Сваки корисник који користи рачунарских мрежа и Интернета мора бити свестан потребе основне безбедности на њима присутних информација, мора да зна како да заштити ресурсе своје фирме и податке на рачунарима, тј. у мрежи. Општи концепт безбедности, притом, даје неопходне основе, тј. он је тај који треба да омогући безбедну комуникацију са другим фирмама и изворима података. С друге стране, неопходно је и добро познавање техника које управо угрожавају безбедност информација у таквом амбијенту, тј. техника и метода угрожавања безбедности информација.

За сваку фирму подаци представљају богатство, каква год да је делатност фирме. Мада постоје подаци који су слободно доступни, постоје и подаци који морају бити заштићени и безбедни. Вредност информације је променљива и другачија за сваку фирму. У већини случајева информације представљају највеће вредности, а ако се униште, не могу се поправити или заменити; оне нестају заувек, што може створити непоправљиву штету. Сама вредност информације може бити реална или процењена. Што је њена цена већа, информација представља пожељнију мету за напад, чиме су и већи захтеви за њену заштиту.

Општи концепт безбедности информација

У циљу ублажења негативних последица и смањења губитака који настају због криминалних активности, са различитим врстама претњи и напада покушавају се изборити како администрације бројних држава, тако и међународне организације и асоцијације, али и „приватни сектор“ и сами корисници. Приватници и корисници постају значајна група у стварању добрих услова за заштиту самих приватних компјутерских мрежа и тако синергички делују са државним органима који су задужени за безбедност у јавним, глобалним мрежама.

3 *Sertificat Security* +, Microsoft Corporation, Beograd, 2004.

Развој сигурне Интернет инфраструктуре као основе безбедности информација у данашњем глобалном, информатичком друштву незамислив је без заједничких активности сваког од тих актера. Утврђивање општег концепта безбедности информација представља први и незаобилазни корак у испуњавању тог циља.

CIA тројство – основни циљ безбедности информација

Основни циљ који треба постићи обезбеђивањем неопходне безбедности информација јесте остваривање такозваног CIA тројства (*confidentiality* – поверљивост, односно да само овлашћено особље има приступ информацијама; *integrity* – интегритет, који обезбеђује да само овлашћено особље модификује информације; *availability* – расположивост, да овлашћено особље има приступ информацијама када год је то потребно).

Напоре за обезбеђивање поверљивости, интегритета и расположивости свакако треба удружити са физичком безбедношћу, чиме се остварује ефикасно безбедносно решење. Задатак специјалисте за информационе системе у једној фирми, односно стручњака за безбедност, јесте да пружи поуздане податке само оним лицима која треба да имају приступ, и то онда када им је приступ потребан. Стручњак за безбедност информација треба да сведе на минимум шансе да се CIA тројство сруши.

Контрола ризика

Контрола ризика је процес који се користи да се открије, контролише и ублажи могућа штета, да се умањи ризик одржавања CIA тројства.

Слика 1: *Контрола ризика*

Поступак (слика 1) почиње тако што се за безбедност информација прво утврде могући ризици, затим се на основу њих открију претње и рањиве тачке, и на крају сви они покушавају да се сведу на минимум према слици. Ризици, који се никада не могу потуно уклонити, своде се на минимум тако што се прво открију, па се потом направи план за њихово ублажавање, тј. ризици се чине мање штетним, тако што се, на пример, смањи број копија најповерљивијих информација, смањи број локација на којима су оне меморисане, ограничи број људи који имају приступ, као и начини остваривања тог приступа итд.

Ризик представља изложеност губитку или могућем оштећењу. У контексту безбедности информација, под ризицима се подразумева могућност да спољни фактори угрозе податке, што би изазвало губитке у времену новцу и репутацији фирме чији су подаци угрожени. Претње, у смислу безбедности информација, јесу све активности које представљају могућу опасност по информације. Могу се јавити у различитим облицима. Слабе тачке су пропусти у заштити информација, односно у безбедности система и мрежа, процесима и процедурама.

Ради безбедности информација CIA тројство се мора очувати, али никад по сваку цену (таква заштита није потребна). Постоји извесна граница вредности за остваривање заштите, па је зато потребно комбиновати знање о вредностима, претњама, рањивим тачкама и ризицима, како би се саставио изводљив и делотворан план. Прво је неопходно проценити вредност информација које треба да се штите, затим одредити што више ризика, претњи и слабих тачака и ублажити откривене ризике. Треба бити свестан да је увек могуће нешто превидети, као и чињенице да се ризик може само до извесне мере ублажити. То ублажавање понекад буде и скупље од штете коју би ризик могао да изазове, што доста зависи и од саме фирме, тј. стања њене радне снаге и буџета којим покрива умањивање ризика. Нека од најбитнијих питања која треба поставити да би се одредила ограничења функционисања одређене фирме могу бити:

- колика је вредност информације коју треба штитити?
- какви су изгледи да та информација буде угрожена?
- на који начин се приступа тој информацији?
- колико особа има приступ тој информацији?

На крају, за све предвиђене мере треба одредити трошкове, време и новац којим се обезбеђује информација и упоредити их са вредношћу информације, како би се одредиле неопходне мере безбедности.

Идентификација претњи[4]

Претње, имајући у виду свето тројство безбедности информација CIA – поверљивост, интегритет, аутентичност, могу бити: пресретање, измена и фабриковање.

• Пресретање (*interception*) представља напад на поверљивост (*confidentiality*). Пресретање се у пракси спроводи као прислушкивање тока информација, надзирање његовог интензитета, увид у саме информације и слично. У питању је пасиван напад који тешко се открива јер не мења податке и не утиче на рад информационог система; понекад је припремна фаза за другу врсту напада.

4 Ранђеловић, Д.: Сигурност рачунарских мрежа као основе за повезаност полиције, безбедности и високотехнолошког криминала, *Тем. збор. „Полиција, безбедност и високотехнолошки криминал"*, стр. 133–174, КПА, Београд, 2010.

• Измена (*modification*) представља напад на интегритет (*integrity*). То је активан напад који се дешава на преносном путу или унутар информационог система. Подразумева измену података, различитих приступних права, начина функционисања информационг система и слично. Иако као активан напад мења информације и/или сам информациони систем, може остати непримећен неко време, због непажње или због сложених техника које нападачи користе.

• Фабриковање (*fabrication*) јесте напад на аутентичност (*authenticity*). Тај активни напад нападач изводи производећи лажне податке (лажно представљање корисника, услуга, сервера, веб стране или неког другог дела информационог система).

Адресирање на Интернету[5],[6]

За комуникацију путем Интернета рачунар користи TCP/IP протоколе. Да би се повезао на Интернет, сваки уређај мора имати јединствену IP адресу, која га идентификује. Њу додељује *Network Information Center* и у IPv4 верзији она се састоји се од четири октета, од којих се сваки записује децимално у распону од 0 до 225 и који су одвојени тачкама (нпр. 187.63.9.29). IP адреса се састоји из два дела, мрежног броја и броја хоста, а може бити статичка и динамичка (статичка IP адреса је један IP број, док се динамичка приликом сваке конекције разликује).

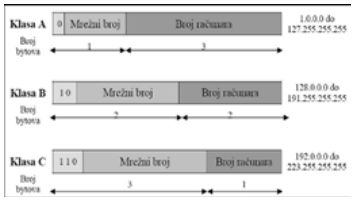
По укупном броју рачунара у мрежи, NIC дели мреже у класе према слици 2:

• *класа А* може имати отприлике 16 милиона рачунара и њој може припадати до 126 мрежа; предвиђена је за мреже с великим бројем рачунара;

• *класи Б* припадају мреже које имају до 65.536 рачунара, а таквих мрежа може бити 16.384;

• *класа Ц* је најмања и обухвата мреже које имају до 256 рачунара; у тој класи може бити до два милиона мрежа;

• *класа Д* која почиње са 1110, а након тога следи адреса, користи се за истовремено приступање групи рачунара (дифузија у групи); заузима IP адресе од 224.0.0.0 до 239.255.255.255.



Слика 2: *Мрежне класе*

5 Видаковић, Б.: *Рачунарске мреже*, Технички школски центар, Зворник, 2010.
6 Парезановић, Н.: *Рачунарство и информатика*, Научна књига, Београд, 1990.

Класа Е, која започиње са 11110 и заузима адресе од 240.0.0.0 до 247.255.255.255, служи за будуће коришћење.

Проблем код адресирања помоћу IP-а је у малом броју расположивих адреса, с обзиром на број рачунара на Интернету и брзо ширење. Због нагле експанзије Интернета данас се ради на новој верзији IP протокола IPv6 у којој су решени многи недостаци из IPv4. Најважније предности IPv6 су:

• адреса од 16 бита која осигурава скоро неограничен број IP адреса;

• поједностављено заглавље, које садржи седам поља (13 у IPv4) и омогућава рутерима да брже обрађују пакете;

• боља подршка за опције; поља која су у IPv4 била обавезна сада више нису, па рутери могу прескочити опције које нису њима намењене;

• велики напредак у сигурности; аутентификација и приватност су кључне особине IPv6;

• боља подршка врсти сервиса; IPv4 има осмобитно поље за тип сервиса, а IPv6 16-битно.

Пример IPv6 адресе: 3ffe:0501:0008:0000:0260:97ff:fe40:efab. Како IPv6 адресе имају 16 бита, на располагању је 2^{128} (приближно $3x10^{38}$) адреса.

Адресирање локалних мрежа

Када је потребно повезати локалну мрежу (са приватним IP адресама) на Интернет, користи се замена IP адреса – *Network Address Translation* (NAT) према слици 3.

Слика 3: *LAN IP рутерско адресирање*

Приватна IP адреса се замењује јавном IP адресом и онда се јавна адреса користи за даљу комуникацију. Објашњење ћемо размотрити на примеру три мале локалне мреже. Слика 3 показује пример коришћења подмрежавања. Слика приказује локални комплекс који се састоји од три LAN-а и два рутера. Остатак Интернета тај комплекс види само као мрежу класе Б са мрежном адресом 140.25.x.x, где су лева два октета број мреже, а десна два број хоста. Рутер који дели мрежу на подмреже конфигурисан је мас-

ком подмреже која има вредност 255.255.255.0. На пример, ако датаграм са одредишном адресом 140.25.2.1 стигне у рутер са остатка Интернета, рутер користи маску подмреже да би утврдио да се та адреса односи на подмрежу 1 и онда прослеђује датаграм том LAN-у, где нови рутер мора да утврди ком је хосту са тог LAN-а намењен пакет. Када утврди коме је пакет намењен, рутер га прослеђује хосту.

Рутер

Рутер би у поступку IP адресирања требало да се обради као посебно важан, из више разлога, а основни је то што он за свој саобраћај користи само *Network ID* адресе. Рутери у субмрежи (*subnet*) користе *Extended network prefix* за интернет саобраћај који се састоји од *network* класе и *subnet* броја. Тако су рутер адресе, на пример, 192.168.1.1 и 192.168.1.2. У пракси то значи да, ако имате један рачунар и подесите TCP/IP протокол, то не значи да ће он радити као што је подешен, јер између рачунара и мреже постоји рутер. Да би се подесио рутер, који, на пример, код већине наших провајдера има адресу 192.168.1.1., потребно је да му се приступи преко интернет прегледача. Приступ рутеру се прави тако што се у прегледач куца 192.168.1.1, а онда уносе корисничко име и лозинка (обично је за већину рутера подразумевано админ/админ).

DHCP (*Dynamic Host Configuration Protocol*)

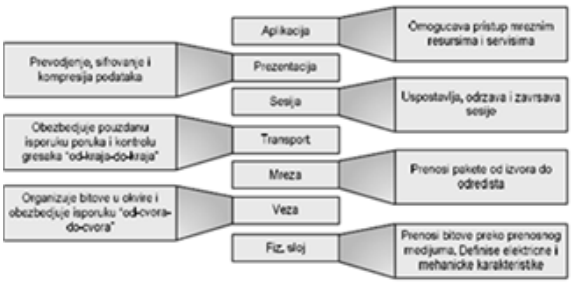
Добијање IP адресе је добро регулисан поступак. Захтев се упућује DHCP серверу, након чега он аутоматски додељује IP адресу. Додељивање се врши из одређеног опсега, који даје ARIN (*American Registry for Internet Numbers*). ARIN не додељује IP адресе појединачним корисницима. Он додељује опсеге, након чега нпр. неки интернет провајдер дели добијене адресе док их не потроши, после чега може поднети захтев за доделу нових IP адреса.

Не треба изоставити ни APIPA (*Automatic Private IP Addressing*), који клијентима са оперативним системом *Windows* (новијим оперативним системима), уколико DHCP сервер из неког разлога није доступан, омогућава да самостално конфигуришу IP адресу из опсега који је додељен „Мајкрософту“ и користе је док DHCP сервер не постане доступан.

Пакетни пренос података TCP/IP протоколом

Данас је комплет протокола TCP/IP присутан на скоро свим компјутерима; то је комплет протокола који се користи у комуникацији на Интернету. Сваки протокол тог комплета је придружен неком слоју седмослојног OSI комуникационог модела, који је стандард Међународне организације за

стандардизацију (*International Organization for Standardization – ISO*).[7] Када мрежни чвор (сви уређаји на мрежи) шаље податке, они се преносе наниже кроз OSI скуп, а затим се шаљу на мрежни медијум. Када чвор прима податке, они се преносе навише кроз скуп модела OSI, док поново не буду у облику који је подесан за корисника рачунара. Важна особина модела OSI је то што сваки слој у скупу пружа услуге првом вишем слоју од себе као на слици 4. Изузетак је слој апликације, који је највиши у скупу.



Слика 4: *Пренос података по слојевима OSI модела*

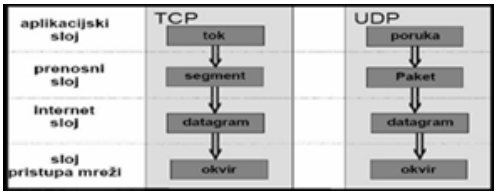
Физички слој (први слој) обично је имплементиран у хардвер и одговоран је за даље слање битова података и примање битова од комуникационих медијума, као што је коаксијални кабл.

Слој повезивања података (други слој) врши конвертовање пакета података примљених из слоја мреже и њихово кодирање у битове, као и примање битова из физичког слоја и њихову конверзију у пакете.

Мрежни слој (трећи слој) обезбеђује рутирање и комунацију и прави логичке путеве између два рачунара да би се формирало виртуелно коло. Тај слој је одговоран за рутирање, прослеђивање, адресирање, повезивање мрежа, поступање са грешкама, контролу загушења и распоређивање пакета. Када се приме пакети из транспортног слоја, мрежни слој обезбеђује да они буду довољно мали за мрежу која се користи. Уколико је пакет сувише велики, он га разбија на неколико ситнијих пакета; на рачунару који те пакете прима, он поново успоставља њихов редослед да би саставио оригинални пакет. Ако уређаји за међусобно повезивање не могу да издрже количину саобраћаја који се одвија, мрежни слој контролише и загушења.

Транспортни слој (четврти слој) преноси податке између крајњих система или чворова и одговоран је за исправку грешака и контролу протока између њих. Тај слој обезбеђује комплетан трансфер података између два система и то TCP као конекциони и UDP као бесконекциони протокол.

7 Ранђеловић, Д.: *Високотехнолошки криминал*, КПА, Београд, 2013, стр. 11.



Слика 5: *Структура података по слојевима*

Слој сесије (пети слој) успоставља и окончава везе између апликација на два рачунара и управља њима. Он успоставља, координира и окончава сву размену између апликација на оба рачунара и управља координацијом сесије и везе.

Презентациони слој (шести слој) обезбеђује хетерогено операционо окружење тако што преводи податке из апликације у формат комуникација мреже која се користи. Тај слој познат је и као „синтаксни".

Апликативни слој (седми слој) подржава процесе крајњих корисника и апликација. Утврђује партнере у комуникацији и квалитет нивоа сервиса, разматра проверу идентитета корисника и приватност и идентификује сва ограничења у синтакси података.[8]

Интернет протокол

Интернет протокол (IP) јесте протокол за везе. Помоћу њега једна страна шаље податке другој без претходног договора о почетку и завршетку тог преноса. Подаци се достављају путем мреже, а њихову тачност проверавају протоколи других слојева TCP/IP архитектуре. Функције Интернет протокола су:

- дефинисање датаграма,
- дефинисање шеме адресирања на Интернету,
- пребацивање података између слоја за приступ мрежи и преносног (транспортног) слоја,
- усмеравање датаграма до удаљених рачунара. [9]

Да би пренос података путем мреже уопште био могућ, они морају бити подељени на више малих пакета. Дељење је неопходно јер би у супротном пренос података трајао знатно дуже, што би подразумевало и загушење мреже, услед ког други рачунари не би могли да преносе сопствене податке. Ако се неки пакет оштети, само се он поново преноси, што је још једна предност у односу на пренос већих јединица података (поново би се преносила цела јединица).

8 Ранђеловић, Д.: *Високотехнолошки криминал*, КПА, Београд, 2013, стр. 11–12.
9 Ранђеловић, Д: Информатика и рачунарство, Свен, Ниш, 2000, стр. 69; Ранђеловић, Д: Основи информатике, КПА, Београд, 2013.

Пакети су сложене структуре и садрже заглавље са главним информацијама (нпр. адреса изворишта, адреса одредишта), корисничке податке и тзв. приколицу са информацијама о претходним подацима који су неопходни за проверу тачности.

На изворном рачунару подаци се организују у пакете, што представља први корак у процесу преноса података. Подаци затим пролазе кроз више слојева, где се на сваком од њих врши додатна форматизација пакета, након чега се они накратко складиште у чворовима мреже, па прослеђују ка следећим чворовима све до крајњег (одредишног). Последњи корак је обједињавање пакета који су стигли до жељеног рачунара у оригиналну форму.

Преглед TCP/IP комуникационог протока – датаграм

Када се од једног рачунара ка другом шаљу подаци апликације, информација полази од апликативног и иде до транспортног слоја.

Протоколи транспортног слоја посматрају информацију апликативног слоја као пошиљку (податак) која треба да буде испоручена и праве заглавље са информацијама као што су предајна и одредишна тачка да би потпомогли испоруку информација одредишном рачунару. Та информација се предаје Интернет слоју.

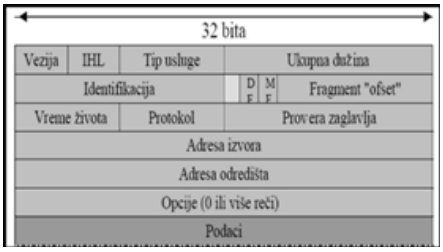
Протоколи Интернет слоја сматрају информацију из транспортног слоја пошиљком. Да би се датаграм испоручио одредишном рачунару, треба испоручити још и право IP заглавље које садржи информације као што је одредишна IP адреса. Те информације преносе се на слој мрежног интерфејса.

Протоколи слоја мрежног интерфејса сматрају информације Интернет слоја пошиљком коју треба испоручити. Они праве преамбулу и заглавље оквира које садржи предајне и одредишне MAC адресе, како би се помогло да пристигли датаграм буде испоручен на одредиште у локалној мрежи, као и информацију завршног записа (*trailer information*), која се назива „контролни збир“ (*checksum*) и садржи суму бита за пренос да би прималац могао да провери евентуално оштећење пакета при преносу. Контролни збир је метод за откривање грешака које могу да настану при преносу појединог бита. Информације се стављају на локалну мрежу.

Када информације стигну до одредишног рачунара, протоколи слоја мрежног интерфејса скидају преамбулу и контролни збир са пакета и пропуштају пошиљку на Интернет слој. Протоколи Интернет слоја скидају IP заглавље са пакета и пуштају пошиљку на транспортни слој. Протоколи транспортног слоја са пакета скидају TCP или UDP заглавље и пропуштају пошиљку на апликативни слој. Податке прима она апликација која управља њима.

Датаграм

Интернет протокол дефинише пакет под називом „датаграм“ као блок података који се шаље на мрежу као једна порука према слици 6.



Слика 6: *Структура IP датаграма*

Првих пет или шест 32-битних речи у датаграму резервисано је за управљачке податке (заглавље), а након заглавља следе подаци. Заглавље садржи све елементе потребне за предају пакета (тип услуге, укупну дужину, идентификацију, заставице, адресу извора, адресу одредишта). Поље „верзија“ (*version*) каже коју верзију протокола користи датаграм. С обзиром да је дужина заглавља променљива, у пољу IHL (*Internet Header Length*) назначена је дужина заглавља (пет или шест речи). У пољу „тип услуге“ (*type of service*) хост говори подмрежи коју врсту услуге жели (могуће су различите комбинације поузданости и брзине). Поље „укупна дужина“ (*total length*) даје укупну дужину датаграма (заглавље и подаци). Максимална дужина је 65.535 бита. Поље идентификација (*identification*) омогућава да одредишни хост одреди којем датаграму припада пристигли фрагмент. Следе неискоришћени бит, DF бит и MF бит. Бит DF (*Don't Fragment*) наређује да се датаграм не фрагментира, јер га одредиште не може сложити.

Осим задњег, сви фрагменти имају постављен бит MF (*More Fragments*) као знак да долази још фрагмената истог датаграма.

Поље „офсет“ фрагмента каже где се у датаграму налази тај фрагмент.

Поље „време живота пакета“ (*time to live* – TTL) представља бројач за ограничавање животног века пакета. Смањује се при сваком скоку и, кад досегне нулу, пакет се одбацује. То поље спречава пакет да кружи мрежом, што се може догодити ако се поремете табеле у рутерима. Поље „протокол“ говори мрежном слоју који ће се протокол преносног слоја користити. Поље за проверу заглавља (*header checksum*) проверава само заглавље. IP доставља датаграм тако да чита адресу одредишта (пета реч). Адреса одредишта је стандардна 32-битна IP адреса. Ако је адреса одредишта адреса у локалној мрежи, пакет се доставља директно. Ако адреса није у локалној мрежи, пакет се предаје рутеру за пренос. Поље „опција“ (*options*) служи за укључивање информација које ће бити потребне у следећим верзијама протокола (тренутно је дефинисано пет опција). Затим следи поље с подацима.

Рањивост TCP/IP протокола

Идентификовање могућих напада на слоју мрежног интерфејса

На слоју мрежног интерфејса пакет информација који се ставља на жицу познат је као „оквир". Пакет укључује три области: заглавље, пошиљку, и FCS (*Frame Control Sequence*) – секвенца провере оквира. Како се слој мрежног интерфејса користи за комуникацију на локалној мрежи, на њој би били изведени и евентуални напади. Неколико је начина на које се мрежни слој може искористити за угрожавање CIA тројства.

Лажирање MAC адресе. Заглавље садржи MAC адресу предајног и одредишног рачунара, и неопходно је да би се успешно послала усмерена порука од предајног до одредишног рачунара. Нападачи лако могу да лажирају MAC адресу другог рачунара. Сваки безбедносни механизам који се заснива на MAC адресама, подложан је овом типу напада.

Одбијање сервиса (DoS). Напад одбијањем сервиса преоптерећује систем тако да он више не може да пружа сервисе за које је конфигурисан. Напад на ARP протокол обара рачунар и тако га онеспособљава за подршку CIA тројству.

Тровање ARP кеша. ARP кеш у меморији чува MAC адресе рачунара са локалне мреже који су у одређеном периоду били контактирани. Ако се ARP кешу додају нетачни или лажирани уноси, рачунар не шаље информације до тачних одредишта.

Идентификовање могућих напада на Интернет слоју

На Интернет слоју формирају се IP датаграми. Пакет се састоји од два дела: заглавља и пошиљке. На овом слоју могуће је неколико напада.

Лажирање IP адресе. Ако су позната поља IP заглавља и његова дужина, IP адреса у IP датаграму се може лако открити и лажирати. Сваки безбедносни механизам који се заснива на IP адреси предајног рачунара, подложан је овом типу напада.

Посреднички напади. До њих долази када хакер себе постави између предајног и одредишног рачунара на такав начин да ниједан од њих не примети његово постојање. Нападач може модификовати пакете, или једноставно видети њихов садржај.

DoS. При DoS нападу на овом нивоу могу се искористити једноставни протоколи и по-моћни програми на IP нивоу, да би се преоптеретио рачунар и тако угрозило CIA тројство.

Погрешно поновно састављање фрагментисаних датаграма. Код фрагментисаних датаграма, поље „офсет" се користи при поновном састављању пакета. Ако се промени вредност тог поља, датаграм се погрешно формира приликом поновног састављања. То датаграму који иначе не би прошао мрежну баријеру, омогућује приступ интерној мрежи, што може пореметити CIA тројство.

Кварење пакета. Будући да датаграм може да прође кроз неколико рачунара пре него што стигне до одредишта, информације у пољима IP заглавља бивају прочитане и понекад измењене, као на пример кад информација стигне до рутера. Ако се догоди да је пакет пресретнут, може се променити информација заглавља, чиме се квари IP датаграм. То може довести до тога да датаграм никада не стигне до одредишног рачунара, а може и да промени протоколе и информације пошиљке.

Идентификовање могућих напада на транспортном слоју

На транспортном слоју се поруци додаје или UDP или TCP заглавље. Од апликације која је тражила сервис зависи који ће се протокол користити. Навешћемо неке од начина на које се транспортни слој може искористити да би се угрозило CIA тројство.

Манипулисање UDP или TCP портовима. Преко поља UDP и TCP заглавља и њихових дужина могу се идентификовати портови који се користе за комуникацију између предајног и одредишног рачунара. Та информација може се искористити или покварити.

DoS напад. Могу се искористити једноставни протоколи и помоћни програми на IP нивоу, да би се преоптеретио рачунар и тако сломило CIA тројство.

Отимање сесије. Након што је успостављена комуникациона веза између предајног и одредишног рачунара, трећи рачунар онеспособљава комуникацију једног од рачунара, да би затим имитирао тај рачунар.

Идентификовање могућих напада на апликативном слоју

Одбрана од напада на апликативном слоју спада међу најтеже, јер се у нападу користе слабе тачке апликација и незнање крајњих корисника о рачунарској безбедности. Ти напади такође могу бити различити.

Напад преко апликација електронске поште. Електронским порукама се могу приложити документи, који се испоручују у корисниково пријемно поштанско сандуче. Када корисник отвори пошту и покрене апликацију, приложени документ може да направи штету одмах, а може и да остане скривен и проради касније.

Напад преко веб претраживача. Када клијентски рачунар користи веб претраживач да би се повезао са Интернетом и учитао веб локацију, садржај те веб локације може бити активан. То значи да њен садржај није само статична информација, већ може бити извршни кôд. Ако је опасан, може да поремети ваше CIA тројство.

Напад преко FTP клијената. Протокол FTP се користи за пренос датотека од једног рачунара до другог. Када клијент треба да унесе корисничко име и лозинку ради провере аутентичности, ту информацију је могуће послати преко Интернета коришћењем само обичног текста.

За сваки циљни систем, ради остваривања описаних напада, прво се провери да ли је систем покренут, а затим утврди на којим његовим прикључцима се ослушкује. У ту сврху, хакер мора да прође три неопходне фазе, редом, снимање (*footprinting*), скенирање (*scanning*) и пописивање система (*enumeration*).

ПРАВНА РЕГУЛАТИВА ИНТЕРНЕТ КРИМИНАЛА У СВЕТУ И РЕПУБЛИЦИ СРБИЈИ[10]

Да би се пружање правне домаће и међународне помоћи могло спровести, одређено људско понашање мора бити кажњиво у кривичноправном смислу, тј. оно мора бити прописано и одредбама кривичног законодавства дате земље. Недостатак хармонизације материјалноправних прописа ускраћује могућност санкционисања одређеног противправног понашања, а самим тим људи и њихова имовина не могу бити сигурни.

Конвенција Савета Европе CETS 185 прописује минимум кривичноправних норми у домаћем законодавству. Односи се на земље потписнице конвенције, а оне могу направити додатну разраду кривичних дела прописаних конвенцијом у оквиру сопственог кривичног закона. Конвенција Савета Европе CETS 185 истиче неопходност међународне сарадње у области високотехнолошког криминала, као и њено проширење, тежећи да обухвати сва кривична дела везана за рачунаре, рачунарске податке и системе.

Европски парламент је 2013. године донео Директиву 2013/40/ЕУ. Циљ Директиве је борба против напада на информационе системе, као и упознавање земаља чланица ЕУ са тим проблемом. Такође Директивом се прописују кривична дела, као и санкције за њих, и тежи унапређењу сарадње надлежних државних органа, специјализованих агенција и других тела Европске уније (EUROJUST, EC3 итд.).

ОРГАНИЗАЦИЈЕ ЗА ПРУЖАЊЕ ПОМОЋИ НА ИНТЕРНЕТУ – CERT ОРГАНИЗАЦИЈЕ

Организације задужене за пружање подршке, размену информација, сарадњу са владом и међународним партнерима јесу CERT организације (*Computer Emergency Response Team*). Назив CERT додељује се стручним тимовима који се баве сигурносним инцидентима и они најчешће свом називу додају скраћеницу CERT или CSIRT (*Computer Security Incident Response Team*).

10 Дракулић, М.: Основи компјутерског права, Београд, 1996; Бодрожић, И.; Петровић, Т.: Сајбер простор као специфично место извршења кривичних дела високотехнолошког криминала, чланак, Београд, 2013; Милошевић, М.; Урошевић, В.: Крађа идентитета злоупотребом информационих технологија, Безбедност у постмодерном амбијенту, Зборник радова књига VI, центар за стратешка истраживањанационалне безбедности, Београд, 2009; Bishop, M.: Computer Security: Art and Science, Addison – Wesley Professional, 2003.

Да би неки тим био CSIRT, он мора пружати једну или више услуга у управљању инцидентима. Те услуге могу бити анализа инцидената, реаговање на инциденте на лицу места, пружање подршке, координација одговора на инцидент итд. У пракси можемо видети да CSIRT, поред ових основних, нуди и друге услуге у зависности од потреба своје изборне јединице, као што су давање упозорења, узбуне, обука, подизање свести људи итд. Све услуге које CSIRT пружа могу се поделити у три групе.

Реактивне услуге врше се на основу догађаја или захтева (нпр. извештај компромитованог домаћина). Тај извештај се може односити на злонамерни код, рањивост софтвера или нешто што је идентификово систем за детекцију упада.

Проактивне услуге односе се на пружање помоћи и неопходних информација у припреми, заштити и осигуравању система приликом исчекивања напада или неких проблема.

Услуге које се односе на квалитет безбедности нису карактеристичне само за управљање инцидентима. Најчешће се врше у другим деловима организације, као што су одељења технологије, ревизије, обуке. Уколико би CSIRT вршио или помагао ове услуге, то би помогло како у побољшању укупне безбедности организације тако и у идентификацији ризика, претњи и слабости система.

Као што је већ речено, реактивне услуге су дизајниране да одговоре на захтев за помоћ, извештаје о инцидентима од CSIRT јединица и било коју претњу или напад усмерен против система. Те услуге обухватају: упозорења и управљање инцидентима, слабостима, и артефактима.

Упозорења подразумевају ширење информација које описују компјутерски вирус, напад, рањивост система итд. Такође се добија и препорука начина деловања у конкретној ситуацији и суочавање са насталим проблемом.

Управљање инцидентима обухвата примање захтева и извештаја и разврставање (одређивање приоритета), затим следи одговор на захтеве и извештаје, и на крају анализа догађаја (инцидента). Одговори могу укључивати и: предузимање акције за заштиту угрожених система и мрежа; филтрирање мрежног саобраћаја; поправку система, обнову система или проналажење неког алтернативног решења.

Управљање слабостима (рањивостима) подразумева примање информација и извештаја о рањивости хардвера и софтвера, као и развој стратегија за откривање и поправку тих слабости.

Управљање артефактима подразумева примање информација о артефактима и њиховим копијама, који су коришћени за извиђање, упад или неке друге недозвољене радње. Артефакт је сваки фајл који се налази у систему и који може бити укључен у нападе на систем, или се може користи у онеспособљавању безбедносних мера.

Поред реактивних, CSIRT пружа и проактивне услуге. Њихова основна улога је избегавање инцидената и смањивање њиховог утицаја у односу на време појављивања. Самим тим, у први план се ставља побољшање инфраструктуре и безбедносних процеса. Проактивне услуге обухватају давање упозорења, праћење развоја нових алата који побољшавају заштиту система и мрежа, подижући је на виши ниво. CSIRT прати нова техничка достигнућа и трендове како би помогао у идентификацији будућих претњи. Такође, пружа преглед и анализу безбедностне структуре организације на њен захтев, као и услуге давања смерница за подешавање и одржавање алата, апликација и целокупне инфраструктуре.

Услуге које се односе на квалитет безбедности имају за циљ побољшање укупне безбедности организације. Анализа и процена ризика доприносе побољшању способности организације за процену реалне претње. CSIRT даје препоруке за избор адекватног одговора када се догоди инцидент, а путем различитих чланака, постера, билтена, веб сајтова итд., пружа савете о мерама предострожности које треба предузети.

Из свега претходно наведеног закључује се да је CSIRT организација задужена за примање, прегледање и одговарање на пријаве сигурносних инцидената, док се њене дужности односе на пружање помоћи и заштите, као и осигуравање критичних делова мреже. Од брзине откривања и решавања проблема зависи колику ће штету организација претрпети, што је управо и разлог што свака организација треба да има CSIRT. Он може постојати самостално или као део неке групе, али без обзира на то где се налази, мора да има управљачку структуру и потпору за посао који обавља.

THE INTERNET CRIME COMPLAINT CENTERS THE INTERNET CRIME COMPLAINT CENTER (IC3)[11]

Интернет центри за жалбе од великог су значаја како за жртве Интернет криминала, тако и за агенције задужене за спровођење закона и судско гоњење починилаца. За жртве Интернет криминала IC3 представља практичан и за коришћење једноставан механизам извештавања, који упозорава власти да постоји сумња да је извршено кривично дело[12]. Са друге стране, агенцијама задуженим за спровођење закона IC3 служи као „проводник".

11 Randjelovic, D, Kuk, K, Popovic, B, Cisar, P: The position and role of the internet complaint centers in managing cyber crime, Теоретические и прикладные аспекты информационной безопасности: материалы Междунар. науч.-практ. конф. (Минск, 31. марта 2016); Ранђеловић, Д.; Бајагић, М.; Царевић, Б.: Интернет у функцији тероризма, *Зборник радова „Сузбијање криминала и европске интеграције са освртом на високотехнолошки криминал"*, стр. 318–328, Висока школа унутрашњих послова, Бања Лука, 2012; Ранђеловић, Д.; Царевић, Б.: *Улога центара зе жалбе на Интернет криминал у САД у заштити људских права*, Култура полиса, 2012.

12 Ранђеловић, Д.; Царевић, Б.: Улога центара зе жалбе на Интернет криминал у САД у заштити људских права, Култура полиса, специјалн број са КПА, 2012.

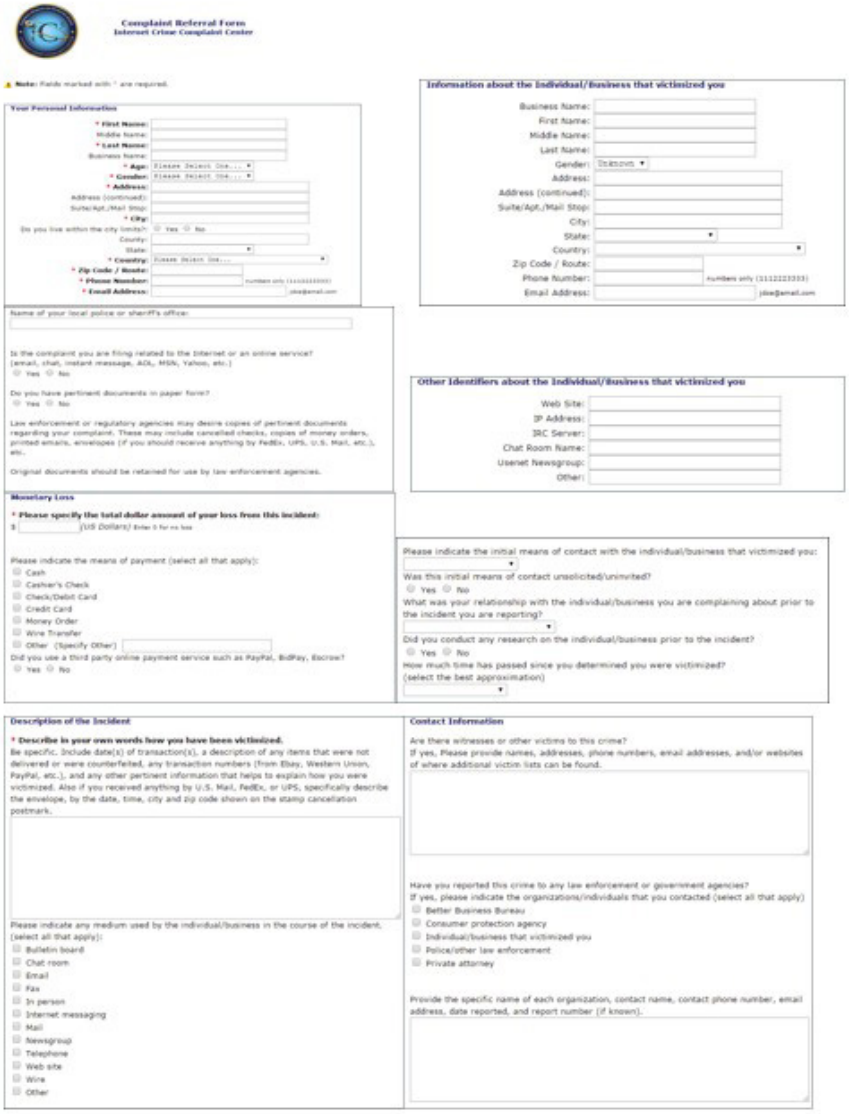
IC3 прима жалве везане за Интернет криминал, разматра их, а затим прави извештај који прослеђује надлежним органима или агенцијама, а они су ти који према потреби, на основу добијених информација спроводе истрагу. IC3 сарађује са FBI (*Federal Bureau of Investigation*) и NW3C (*National White Collar Crime Center*). Задатак FBI је да штити и брани САД од терористичких и страних обавештајних претњи и да спроводи кривични закон унутар САД.

Улога NW3C јесте да обезбеди обуку, истражну и истраживачку подршку агенцијама и ентитетима који су укључени у превенцију, истрагу и гоњење економског и високотехнолошког криминала. Пошто NW3C нема истражна овлашћења, он само помаже агенцијама у бољем разумевању примене закона и коришћењу алата у борби против економског и високотехнолошког криминала.

Као центар за примање жалби везаних за Интернет криминал, IC3 је основан 2000. године. Данас, у својој седамнаестој години рада, када је Интернет криминал постао глобални проблем и када се технолошка знања све више примењују у криминалне сврхе, IC3 остаје посвећен циљу да задовољи потребе спровођења закона широм света. Наставља са информисањем јавности, пружањем услуга и саветовањем о Интернет преварама. Жалбе које се подносе у IC3 односе се на читав низ недозвољених радњи као што су: крађа интелектуалне својине, рачунарски упади, економска шпијунажа, изнуде, међународно прање новца, крађа идентитета, аукцијске преваре, преваре у вези плаћања, фалсификовање, неиспоручивање робе итд.

Подносилац жалбе може бити особа која је жртва преваре или неко треће лице. Прилико подношења жалбе, подносилац попуњава образац у којем се од њега траже неопходне информације. Потребно је унети своје име, презиме, имел адресу, број телефона и уколико је могуће (доступно) име, адресу, број телефона, веб адресу појединца или организације за коју верујемо да нас је преварила. Потребно је навести и детаље о томе како и када је превара извршена и све друге информације за које подносилац сматра да су од користи. Веома је значајно сачувати све доказе који су везани за жалбу. То могу бити: отказани чекови, потврде путем електронске поште, потврде кредитних картица, телефонски рачуни итд. Пример формулара за подношење жалбе дат је на слици 7.

Након што је жалба поднета Интернет центру за жалбе, подносилац добија имејл поруку са потврдом о пријему исте и његовим именом и лозинком. Аналитичари разматрају приспеле жалбе, а затим прослеђују информације надлежним државним, локалним или међународним институцијама за спровођење закона или надлежним агенцијама. IC3 не спроводи истрагу па самим тим подносиоцу не може пружити информације о истражном статусу раније уложене жалбе. Жалба која је једном поднета IC3, не може бити одказана или поништена.



Слика 7: *Формулар за подношење жалбе (IC3)*
The European Cybercrime Centre (EC3)

Са циљем да се борба против Интернет криминала у Европској унији (ЕУ) побољша и подигне на виши ниво, а њени грађани заштите основан је Европски центар за сајбер криминал (*The European Cybercrime Centre – EC3*). Почео је с радом 2013. године. Интернет криминал у Европској унији је у

порасту, због чега је оснивање овог центра био један од приоритета у оквиру стратегије унутрашње безбедности Европске уније.

ЕС3 функционише у склопу Европола. Европол је организација са седиштем у Холандији (Хаг). Као полицијска агенција у ЕУ, Европол има за циљ да подржи њене државе чланице у превенцији и борби против тероризма и свих облика међународног криминала. Такође доприноси да Европа постане сигурније место за живот, зарад добробити свих грађана.

Европол користи своје информационе могућности и стручност особља да идентификује и прати највеће криминалне и терористичке мреже у Европи. Особље Европола долази из различитих грана полиције (има припадника редовне полиције, граничне полиције, царине, служби безбедности итд.). Европол нема извршна овлашћења, али прикупљањем, анализом и разменом информација помаже спровођење закона у ЕУ. Делује искључиво на захтев, али и сам може упутити захтев за спровођење истраге надлежним властима државе чланице.

Функционисање у оквиру Европола, омогућава ЕС3 не само да користи његове постојеће капацитете, већ да значајно прошири своје могућности, посебно у обезбеђивању оперативне и аналитичке подршке у истрагама.

ЕС3 се фокусира на следеће области:

• Интернет криминал организованих криминалних група који доноси велики профит (нпр. Интернет преваре);

• Интернет криминал који наноси велику штету жртвама (нпр. сексуална експлоатација деце путем Интернета);

• Интернет криминал који утиче на критичне инфраструктуре и информационе системе у ЕУ.

Комбинујући искуство и стручност у области анализе, превенције, информисања, обуке и форензике, стручњаци у ЕС3 стичу увид и покушавају да разумеју на који начин преваранти и криминалци у области Интернет криминала размишљају и раде.

У оквиру Европола, ЕС3 служи као централно чвориште за прикупљање и обраду обавештајних података и информација везаних за криминалне активности. ЕС3 пружа подршку током истраге и операција које спроводе државе чланице, путем оперативне анализе, координације и стручности. ЕС3 информише јавност, пружа подршку специјализованим техничким средствима, обезбеђује форензичку подршку истрагама, учествује у обукама, помаже изградње нових капацитета итд.

Обављајући велики број различитих функција, ЕС3 је значајан како за државе ЕУ, тако и за међународне партнере (*Interpol*, *FBI*, *Customs Enforcement* итд.). Државама ЕУ пружа оперативну подршку, коришћење напредних технологија, аналитичку и форензичку експертизу у истрагама.

ACORN – Аустралија

У Аустралији, као и у другим технолошки развијеним земљама, Интернет криминал је у порасту и представља проблем који утиче на већину Аустралијанаца. ACORN (*Australian Cybercrime Online Reporting* Network) јесте национална полицијска иницијатива земаља Комонвелта и територијалних влада. Као национални онлајн систем, омогућава безбедну пријаву Интернет криминала и даје савете људима како препознати и избећи уобичајене врсте Интернет криминала.

ACORN је једна од кључних карика у оквиру Националног плана за борбу против Интернет криминала (*The National Plan to Combat Cybercrime*), који одређује на који начин ће аустралијске агенције обављати дужности (сарађивати) да би ојачале Аустралију у борби против Интернет криминала. ACORN омогућава једноставну и брзу пријаву инцидената, подиже свест грађана о значају борбе против Интернет криминала и разумевању како исти утиче на њих саме.

ACORN-у се могу пријавити уобичајене врсте Интернет криминала, што обухвата хаковање, преваре, крађе идентитета, нападе на компјутерске системе, пријаве које се односе на недозвољен или незаконит садржај на мрежи итд. Након слања извештаја ACORN-у, пошиљалац путем имејла добија повратну поруку која садржи јединствен ACORN референтни број. Да би сам извештај био обрађен на најбољи могући начин, требало би да садржи све информације о инциденту које могу бити од значаја. Такође подносилац треба да сачува све расположиве доказе (нпр. имејлове, снимке итд.) у случају да буде контактиран од стране органа за спровођење закона.

ACORN прихвата анонимне пријаве, али сајт ипак памти IP адресе свих приспелих извештаја са циљем откривања злонамерног извештавања и адекватним одговарањем на њега. ACORN прихвата само онлајн извештаје, тако да на извештаје приспеле путем поште, телефона, факса или електронске поште неће реаговати.

CNNIC – Кина

Интернет је постао један од кључних фактора који утичу на друштвени и привредни развој Кине и начин живота њених држављана уопште. У јуну 1993. године уз сагласност надлежних органа, основан је CNNIC (*China Internet Network Information Center*), који преузима одговорност као национални Интернет информациони центар (*Internet Network Information Center*). CNNIC пружа апликационо орјентисане и ефикасне услуге преко безбедне и стабилне Интернет инфраструктуре за јавне интересе. Као једна од најважнијих карика кинеског информационог друштва, CNNIC је одговоран за сигурност рада основних Интернет ресурса. Такође, врши истраживање о развоју Интернета, пружа консултације, промовише сарадњу и размену тех-

нолошких искустава на глобалном нивоу итд. CNNIC има неколико главних одговорности:

• управља највишим нивоом домена од „.CN“ и кинеског DNS (*Chinese Domain Name System*) и пружа услуге регистрације домена 24 сата; члан је APNIC-a (*Asian – Pacific Network Information Centre*) као национални Интернет регистар (*National Internet Registry – NIR*); као сазивач савеза за расподелу IP адреса (*IP Address Allocation Alliance*), CNNIC је одговоран за расподелу и администрацију Интернет провајдера у Кини (*Internet Service Providers – ISPs*), као и за промоцију нове генерације Интернета базиране на IPv6;

• истражује, развија и осигурава центре националне мреже; такође, развија уређаје и софтвере зарад побољшања пузданости, безбедности и стабилности система основних мрежних ресурса у Кини;

• пружа услуге консултација, одговоран је за прикупљање информација о Интернету уопште, укључујући и информације о Интернету у Кини и његовом развоју; пружа истраживачку подршку и услуге консултација за развој Интернета за предузећа, истраживачке институте, као и за обичне кориснике, без профита;

• залаже се за отворену Интернет сарадњу и размену технике; прати развој нових технологија и сарађује са релевантним међународним организацијама и Интернет информационим центрима других земаља.

CNNIC је домаћин важних међународних конференција и других активности везаних за Интернет и као такав промовише међународну размену и примену научних достигнућа и залаже се за напредак Интернет технологије у Кини.

СТРАТЕГИЈЕ НАЦИОНАЛНИХ CERT-ОВА У НАШЕМ ОКРУЖЕЊУ[13]

Очигледно да је у данашњем, савременом друштву, употреба Интернета неизбежна и да је то постала свакодневница великог броја људи. Имајући у виду могућности које Интернет пружа и начине на које се може злоупотребити, у интересу је сваке државе да спречи или бар сведе на минимум шансу да до било каквог сигурносног инцидента дође, а уколико се инцидент ипак догоди, да његове последице буду минималне.

Следећи тај циљ, многе држава у свету, међу којима и доста њих из нашег окружења основале су националне CERT-ове. Свака од тих држава је према својој визији, циљевима и приоритетима, развила сопствену стратегију функционисања националних CERT-ова[14].

13 Kossakowski, K.: *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001.

14 Pethia, Richard, D.; Wyk, K. R.: Computer Emergency Response: An International Problem, Pittsburgh, Pa.: CERT Coordination Center., Software Engineering Institute, Carnegie Mellon

Црна Гора

У складу са законом о информационој безбедности Црне Горе основан је црногорски CIRT. Основан је у оквиру Министарства за информационо друштво и телекомуникације (MITS). Као засебна организациона јединица MITS-а, црногорски CIRT је централно место за размену података у области Интернет безбедности. Црногорски CIRT на том пољу сарађује и са другим институцијама са циљем превенције и отклањања свих претњи које би могле да имају негативан утицај на државу и њене грађане. CIRT Црне Горе помаже агенцијама да пруже адекватан одговор када се инцидент догоди; саветује, едукује и упознаје становништво, државне службенике итд., у области Интернет криминала; координира радом локалних CIRT служби; размењује искуства и информације са националним CIRT службама других земаља итд.

Национални CIRT Црне Горе бави се инцидентима када је једна од учесница инцидента Црна Гора, тј. ако се ради о „.me" домену или црногорској IP адреси. Инциденте је могуће пријавити на: *www.cirt.me*.

Босна и Херцеговина

Следећи препоруку ЕУ о успостављању националних CERT-ова, а пре свега са циљем јачања сигурности, спречавања инцидената и последица које могу изазвати, основан је CERT Босне и Херцеговине. Пошто сигурносни инциденти могу нанети велике губитке и штету и држави и њеним грађанима, једна од основних мисија CERT-а БиХ јесте превенција и њихово сузбијање.

Сталном посвећеношћу, саветима и пружањем помоћи у сузбијању последица насталих сигурносним инцидентом CERT БиХ даје велики допринос решавању свих информационо-технолошких (ИТ) сигурносних инцидената. Иако нема могућност оперативног решавања сигурносних инцидената, он даје савете како побољшати сигурносне мере информационо-технолошких система.

CERT БиХ на основу пријава и прикупљених информација утврђује тежину насталог инцидента. Помаже у координацији операција решавања инцидената, врши едукацију о ИТ сигурности, спроводи обуке итд.

Оснивањем националног CERT-а у БиХ су дефинисани и одређени краткорочни, средњорочни и дугорочни стратешки циљеви. Између осталог, то су успостављање сарадње са националним CERT службама држава из окружења, успостављање сарадње са најзначајним CERT-овима у свету, иденти-

University, 1990; Pethia, Richard, D.: Developing the Response Team Network, Workshop on Computer Security Incident Handling, Pleasanton, CA, 1990; Pethia, Richard, D.: Forming and Managing a Response Team, Workshop on Computer Security Incident Handling, Pleasanton, CA, 1990; Killcrece, G.: Steps for creating national CERTs, Software Engineering Institute, 2009.

фикација критичних инфраструктура у БиХ, рад на побољшању сигурносног стања, едукација, подршка успостављању CERT-ова на нижим нивоима власти унутар БиХ итд.

Хрватска

CERT организације постоје и у Хрватској. Задужене су за пружање подршке приликом сигурносних инцидената и сарадњу са другим надлежним институцијама у решавању проблема из области Интернет криминала. Као посредник у решавању сигурносних инцидената у Хрватској, 1996. године основан је CARNet CERT.

CARNet CERT прикупља и анализира информације о сигурносним инцидентима; даје савете и препоруке за побољшање сигурности рачунарских система; врши едукацију; ради на спречавању инцидената; сарађује приликом решавања сигурносних инцидената у којема је барем једна страна из Хрватске; сарађује са другим CERT-овима на међународном нивоу итд[15].

Након пријаве инцидента у CARNet CERT, подносилац пријаве добија поруку о пријему пријаве. CARNet CERT анализира пријаву и, уколико постоји незаконита радња, прослеђује је надлежним органима. Пријава се може поднети на *www.cert.hr* или имејл адресе *ncert@cert.hr*. Национални CERT Хрватске пружа сва неопходна упутства, савете, препоруке и смернице у оквиру своје надлежности (ако се ради о домену „.hr“ или хрватској IP адреси).

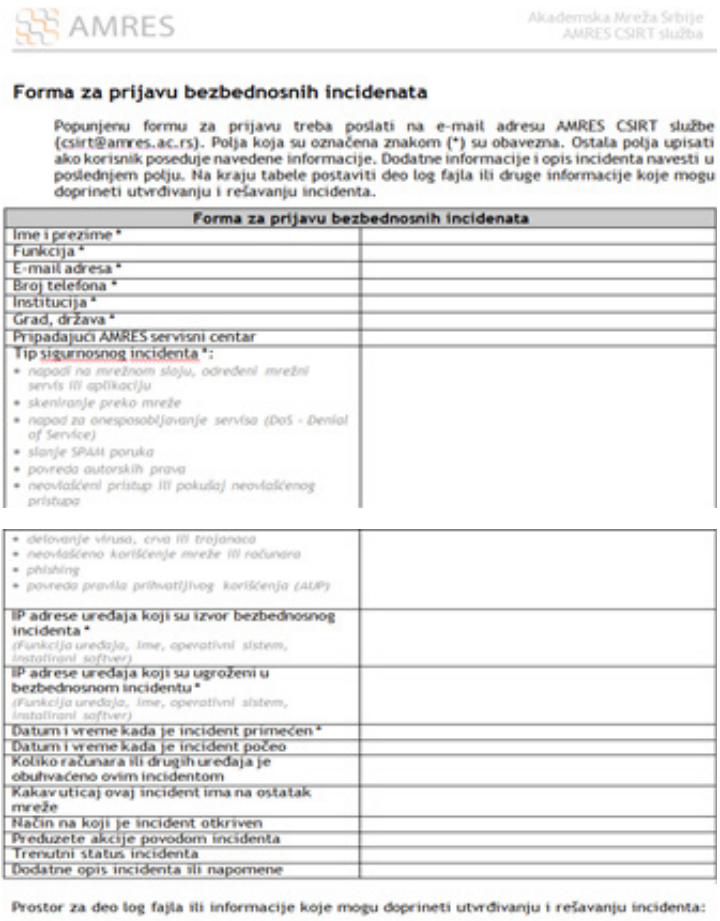
Академска мрежа Србије – AMRES CSIRT службе

Академска мрежа Србије (AMRES) јесте истраживачка и образовна мрежа Србије. AMRES нуди модерне информационо-комуникационе услуге. Сматра се најнапреднијом мрежом у нашој земљи и представља носиоца развоја њеног информационог друштва.

AMRES CSIRT је служба која одговара на безбедносне инциденте и њом управља AMRES. Граница деловања те службе одређена је границама AMRES-а.

AMRES CSIRT прима пријаве инцидената, сортира их, анализира и одговара на њих. У зависности од конкретног случаја, он покушава да дође до извора инцидента и идентификује одговорна лица. Преко телефона или имејла он својим корисницима пружа неопходну техничку помоћ, а доставља им и информације о новим безбедносним претњама (вируси, напади, црви итд.) и препоруке за заштиту од њих.

15 Brand, Russell, L.: Coping With the Threat of Computer Security Incidents, A Primer from Prevention Through Recovery, Version CERT 0.6. Pittsburgh, Pa., June 1990.



AMRES

Akademska Mreža Srbije
AMRES CSIRT služba

Forma za prijavu bezbednosnih incidenata

Popunjenu formu za prijavu treba poslati na e-mail adresu AMRES CSIRT službe (csirt@amres.ac.rs). Polja koja su označena znakom (*) su obavezna. Ostala polja upisati ako korisnik poseduje navedene informacije. Dodatne informacije i opis incidenta navesti u poslednjem polju. Na kraju tabele postaviti deo log fajla ili druge informacije koje mogu doprineti utvrđivanju i rešavanju incidenta.

Forma za prijavu bezbednosnih incidenata	
Ime i prezime *	
Funkcija *	
E-mail adresa *	
Broj telefona *	
Institucija *	
Grad, država *	
Pripadajući AMRES servisni centar	
Tip sigurnosnog incidenta *: • napadi na mrežnom sloju, određeni mrežni servis ili aplikaciju • skeniranje preko mreže • napad za onesposobljavanje servisa (DoS - Denial of Service) • slanje SPAM poruka • povreda autorskih prava • neovlašćeni pristup ili pokušaj neovlašćenog pristupa	
• delovanje virusa, crva ili trojanaca • neovlašćeno korišćenje mreže ili računara • phishing • povreda pravila prihvatljivog korišćenja (AUP)	
IP adrese uređaja koji su izvor bezbednosnog incidenta * (Funkcija uređaja, ime, operativni sistem, instalirani softver)	
IP adrese uređaja koji su ugroženi u bezbednosnom incidentu * (Funkcija uređaja, ime, operativni sistem, instalirani softver)	
Datum i vreme kada je incident primećen *	
Datum i vreme kada je incident počeo	
Koliko računara ili drugih uređaja je obuhvaćeno ovim incidentom	
Kakav uticaj ovaj incident ima na ostatak mreže	
Način na koji je incident otkriven	
Preduzete akcije povodom incidenta	
Trenutni status incidenta	
Dodatne opis incidenta ili napomene	

Prostor za deo log fajla ili informacije koje mogu doprineti utvrđivanju i rešavanju incidenta:

Слика 8: *Формулар за подношење жалбе (AMRES CSIRT)*

Како би смањио број безбедносних инцидената, AMRES CSIRT делује и превентивно[16]. Он прати развој нових безбедносних технологија (антивируса и др.), путем веб сајта или имејла обавештава кориснике о могућим рањивостима система и даје им безбедносне препоруке. На курсевима које организује упућује кориснике у питања информационо-технолошке безбедности[17].

16 Prabhakar, S.; Pankanti, S.; Jain, K.: IEEE Security & Privacy Magazine, 1 (2), стр. 33 – 42, 2003. Пантовић, В.; Динић, С.; Старчевић, Д.: Савремено пословање и Интернет технологије – Увод у дигиталну економију, Енергопројект – InGraf, Београд, 2002; Last, M.; Fifhting, A.: Terror in Cyberspace, World Scientific Publishing, 2005.

17 Петровић, Л.: *Дигитални докази*, Интернет, 2009; Петровић, Р. С.: *Полицијска информатика*, КПА, Београд, 2007; Петровић, Р. С.: *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004; Грубор, Г.: *Еволуција модела дигиталне форензичке истраге*, Интернет, 2010; Devargas, M.: The Total Quality Management Approach to IT Security, Oxford: NCC Blackwell, 1995; Kaufman, C.: Perlman, R.: *Network Security: Private Communication in a Public World, Englewood Cliffs*, N.J.: Prentice Hall, 1995.

Пријава безбедносних инцидената шаље се у AMRES CSIRT на једну од следећих имејл адреса: *csirt@amres.ac.rs* или *abuse@amres.ac.rs*. Приликом попуњавања пријаве важно је доставити сваку информацију која може бити од користи. Пример формулара за пријаву безбедносног инцидента дат је на слици бр. 8.

Безбедносни инциденти које је могуће пријавити обухватају следеће:

- напади на мрежни слој, одређени мрежни сервис или апликацију,
- скенирање преко мреже,
- напад за онеспособљавање сервиса (*DoS – Denial of Service*),
- слање SPAM порука,
- повреда ауторских права,
- неовлашћени приступ или покушај неовлашћеног приступа,
- деловање вируса, црва и тројанаца,
- неовлашћено коришћење мрежних ресурса или рачунара,
- фишинг,
- повреда правила прихватљивог коришћења.[18]

ЗАКЉУЧАК

Интернет је постао један од најмоћнијих и широко доступних медија на планети. С обзиром на масовност примене и могућности које пружа, представља погодно тло за реализацију бројних криминалних активности. Интернет криминал се сврстава међу најопасније видове криминала, а штета коју наноси мери се милијардама долара.

Данас многе међународне организације сарађују у борби против Интернет криминала. Размена информација и искустава, како на националном тако и на међународном нивоу, од кључног је значаја њихов рад. Да би цео процес (од подношења жалбе до спровођења и евентуалних хапшења) био ефикаснији, многе државе основале су националне CERT-ове, што представља велики корак у превенцији и уклањању Интернет претњи.

Упркос свим напорима, Интернет криминал се не може у потпуности искоренити. Ипак, жртвама преваре треба обезбедити брз и једноставан начин пријављивања инцидента и тражења помоћи. Када се инцидент догоди, интернет центри за жалбе имају незаменљиву улогу. Жртве преваре на адресу тих центара шаљу жалбе са неопходним информацијама и доказима. Оне се, када за то има елемената, прослеђују надлежним органима или агенцијама за спровођење закона. Иако немају извршна овлашћења, ти центри неспорно доприносе сузбијању Интернет криминала.

У Републици Србији још увек нису развијени овакви центри. У оквиру Академске мреже Србије (AMRES) постоји AMRES CSIRT служба која од-

18 AMRES CSIRT.

говара на безбедносне инциденте и којом управља AMRES, али она делује само у оквиру те мреже.

Имајући у виду препоруке Европске уније о успостављању националних CSIRT организација, надлежни органи би требало да се што пре посвете решавању овог питања.

Криминалистичко-полицијска академија пример је установе у којој би се могао основати Интернет центар за жалбе. С обзиром на знање и стручност особља те образовне установе, центар за жалбе би у оквиру ње функционисао беспрекорно и на најбољи могући начин служио грађанима Републике Србије. Наравно, то је само предлог чије разматрање и евентуалну реализацију треба препустити особама компетентним за то.

ЛИТЕРАТУРА

1. Ранђеловић, Д.: *Управљање информационим системима и њихова заштита*, КПА, Београд, 2014.
2. Ранђеловић, Д.: *Високотехнолошки криминал*, КПА, Београд, 2013.
3. Ранђеловић, Д.: *Информатика и рачунарство*, Свен, Ниш, 2000.
4. Randjelovic, D.: *Osnovi informatike*, KPA Beograd, 2013.
5. Bishop, M.: *Computer Security: Art and Science*, Addison – Wesley Professional, 2003.
6. Бодрожић, И.; Петровић, Т.: *Сајбер простор као специфично место извршења кривичних дела високотехнолошког криминала*, чланак, Београд, 2013.
7. Brand, Russell, L.: *Coping With the Threat of Computer Security Incidents, A Primer from Prevention Through Recovery*, Version CERT 0.6. Pittsburgh, Pa., June 1990.
8. Vestbi, R. Dž.: *Међународни водич за борбу против компјутерског криминала*, Америчка адвокатска комора, Чикаго, 2009.
9. Видаковић, Б.: *Рачунарске мреже*, Технички школски центар, Зворник, 2010.
10. Devargas, M.: *The Total Quality Management Approach to IT Security*, Oxford: NCC Blackwell, 1995.
11. Дракулић, М.: *Основи компјутерског права*, Београд, 1996.
12. Грубор, Г.: *Еволуција модела дигиталне форензичке истраге*, Интернет, 2010.
13. Kaufman, C.; Perlman, R.: *Network Security: Private Communication in a Public World*, Englewood Cliffs, N. J.: Prentice Hall, 1995.
14. Killcrece, G.: *Steps for creating national CERTs*, Software Engineering Institute, 2009.
15. Комлен – Николић, Л.: *Сузбијање високотехнолошког криминала*, Удружење јавних тужилаца и заменика јавних тужилаца у Србији, Београд, 2010.
16. Kossakowski, K.: *Information Technology Incident Response Capabilities*, Doktor Thesis at the University of Hamburg, Germany. Hamburg: Books on Demand, 2001.

17. Last, M.; Fifhting, A.: *Terror in Cyberspace*, World Scientific Publishing, 2005.
18. Милошевић, М.; Урошевић, В.: *Крађа идентитета злоупотребом информационих технологија, Безбедност у постмодерном амбијенту*, Зборник радова књига VI, центар за стратешка истраживањанационалне безбедности, Београд, 2009.
19. Пантовић, В.; Динић, С.; Старчевић, Д.: *Савремено пословање и Интернет технологије – Увод у дигиталну економију*, Енергопројект – InGraf, Београд, 2002.
20. Парезановић, Н.: *Рачунарство и информатика*, Научна књига, Београд, 1990.
21. Петровић, Л.: *Дигитални докази*, Интернет, 2009.
22. Петровић, Р. С.: *Полицијска информатика*, КПА, Београд, 2007.
23. 23. Петровић, Р. С.: *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004.
24. 24. Pethia, Richard, D.: *Forming and Managing a Response Team*, *Workshop on Computer Security Incident Handling,* Pleasanton, CA, 1990.
25. 25. Pethia, Richard, D.: *Developing the Response Team Network*, *Workshop on Computer Security Incident Handling,* Pleasanton, CA, 1990.
26. Pethia, Richard, D.; Wyk, K. R.: *Computer Emergency Response: An International Problem*, Pittsburgh, Pa.: CERT Coordination Center., Software Engineering Institute, Carnegie Mellon University, 1990.
27. Плескоњић, Д.; Мачек, Н.; Ђорђевић, В.; Царић, М.: *Сигурност рачунарских система и мрежа*, Београд, Микро књига, 2007.
28. Prabhakar, S.; Pankanti, S.; Jain, K.: *IEEE Security & Privacy Magazine*, 1 (2), стр. 33 – 42, 2003.
29. Ранђеловић, Д.: *Сигурност рачунарских мрежа као основе за повезаност полиције, безбедности и високотехнолошког криминала*, Тем. збор. „Полиција, безбедност и високотехнолошки криминал“, стр. 133 – 174, КПА, Београд, 2010.
30. Ранђеловић, Д.; Царевић, Б.: *Улога центара зе жалбе на Интернет криминал у САД у заштити људских права*, Култура полиса, специјалн број са КПА, 2012.
31. Ранђеловић, Д.; Бајагић, М.; Царевић, Б.: *Интернет у функцији тероризма*, Зборник радова „*Сузбијање криминала и европске интеграције са освртом на високотехнолошки криминал*“, стр. 318 – 328, Висока школа унутрашњих послова, Бања Лука, 2012.
32. Randjelovic, D., Kuk, K., Popovic, B., Cisar, P.: The position and role of the internet complaint centers in managing cyber crime, Теоретические и прикладные аспекты информационной безопасности: материалы Междунар. науч.-практ. конф. (Минск, 31 марта 2016).

INTERNET CENTERS FOR CITIZENS' COMPLAINTS AND CYBER CRIME

Slobodan Nedeljković
Ministry of Interior of the Republic of Serbia
Full Professor Dragan Ranđelović, PhD
Assistant Professor Kristijan Kuk, PhD
Academy of Criminalistic and Police Studies, Belgrade
Vojkan Nikolić
Ministry of Interior of the Republic of Serbia

Abstract: The use of electronic services, especially computer networks, which in today's global, information society is inevitably provided by the Internet, is not a privilege of individuals, but the common good of humanity which is provided by modern information-communication technologies. It is a necessary evil that along all the benefits provided to the Internet users, there is also a "dark" side of the computer security incidents on the Internet which are common in the modern era. The rapid development of information technologies has enabled the development of new and more powerful methods and techniques of attack and compromising computers on the Internet. For the prevention and elimination of security threats on the Internet, which are numerous and various, and to limit the activity of malicious attackers, the procedure for resolving security indicidents is technically and legally defined and regulated.

The main objective of this study is precisely the suppression of cybercrime, analyzing a particular place and the role that Internet centers for complaints must have, which as an organization for reception and assistance in resolving complaints about work on the Internet are closely associated with an organization that is responsible for receiving, reviewing and responding to requests giving security incidents - CSIRT (Computer Security Incident Response Team). The organization may provide services to government institutions and corporations in the region or the country, but above all to citizens and its duty is to provide assistance, protection and provision of critical parts of the Internet, which is the subject of this paper. The paper deals with the experience of the most developed countries in the world, the immediate environment and the state of Serbia itself.