Kaznenopravno-forenzička zaštita kritične nacionalne infrastrukture od informatičkih (cyber) ugroza

dr. sc. Damir Brnetić, policijski savjetnik, viši predavač Visoke policijske škole
mr. sc. Damir Palavra, sudski vještak za informatiku
Marijana Cindrić, struč.spec.crim., viši stručni suradnik za promet i urbanu sigurnost

SAŽETAK

Računalne mreže temelj su suvremene infrastrukture. Cyber prostor je primjer infrastrukture koja je postala kritična jer predstavlja sučelje za društvene aktivnosti koje se odvijaju putem računalnih komunikacijskih mreža. Kritične infrastrukture danas su pod nadzorom i upravljanjem kontroliranih sustava, težnje prema potpunoj automatizaciji smanjile su mogućnost implementacije potrebnih sigurnosnih komponenti, uključujući standarde i postupke otkrivanja, sprječavanja i ublažavanja ugroza. Kritične informacijske infrastrukture mogu biti posebno osjetljive na napade hakera, kriminalaca i terorista. Kriminalne se aktivnosti poduzimaju iz inozemstva, što problematizira pitanje nacionalne, teritorijalno ograničene jurisdikcije. Kazneni zakon Republike Hrvatske propisuje kaznena djela koja kriminaliziraju napade na komunikacijske i informacijske tehnologije: Terorizam, Uništenje ili oštećenje javnih naprava, Neovlašteni pristup, Ometanje rada računalnog sustava, Oštećenje računalnih podataka, Neovlašteno presretanje računalnih podataka, Zlouporaba naprava. Osobitu teškoću predstavlja zahtjev da se trenutno fiksiraju dokazi s obzirom da počinitelji tih kaznenih djela relativno lako prikrivaju svoj identitet, a dokazi mogu biti brzo uništeni. Potpuna je enkripcija čvrstog diska veliki problem računalnim forenzičarima jer danas dostupnim metodama i alatima nije moguće pročitati podatke s kriptiranih sustava. Neophodna je kontinuirana edukacija svih osoba uključenih u istraživanje, otkrivanje i sprječavanje ovakvih djela kako bi se upoznali s novim tehnologijama i alatima. Problem zaštite kritičnih informacijskih infrastruktura ne spada ekskluzivno u područje računarstva. Nakon dublje analize nameće se zaključak da promišljanje o represivnim modelima postupanja treba proširiti izvan područja informatike. Detaljnije treba ispitati u kojoj je mjeri dopustivo zadirati u privatnost individualnog korisnika računala, osobito kada je riječ o

udaljenom, tajnom pristupu usmjerenom na prikupljanje podataka s računala i praćenje korisnikove aktivnosti. Usprkos mogućim ugrozama, zajamčena ljudska prava treba očuvati.

Ključne riječi: kritična nacionalna infrastruktura, cyber ugroze, kaznena djela protiv računalnih sustava, forenzički postupci

UVODNO O EVOLUCIJI TRADICIONALNE INFRASTUKTURE

Infrastruktura je sustav koji kombinira različite sadržaje i omogućuje složene aktivnosti, obuhvaća asfaltirane ceste, mostove i raskrižja koji omogućuju kretanje ljudi i robe, zračni promet, cjevovod koji provodi vodu iz crpilišta u domove, opskrba gorivom i slično. Jedna od karakteristika infrastrukture je ovisnost različitih područja djelovanja o sustavu. Ranije je ovisnost proizlazila samo od fizičkih ili geografskih karakteristika. Razvojem cyber prostora, koji uključuje komunikacijske sustave i računalne metode automatskog upravljanja i kontrole, kreiraju se nove veze koje stvaraju daljnju ranjivost. Stoga je osnovano razlikovati infrastrukturu u tradicionalnom smislu, te modernu uporabu tog pojma koji uključuje i cyber dimenziju. U informacijsko doba, tradicionalna infrastruktura postala je informacijska infrastruktura koja uključuje računala. Izgrađene su čisto informacijske kritične infrastrukture: kompjutorizirane baze podataka koje sadrže važne podatke u bankarskom sustavu, znanstvene i gospodarske baze intelektualnog vlasništva, programirani sustavi koji upravljaju proizvodnim i različitim poslovnim procesima. U informacijsko doba, pojam infrastrukture neizostavno uključuje računalne komponente, a time se i infrastruktura danas nužno odnosi na informacijske infrastrukture. Infrastruktura je označena kao kritična kada je vjerojatno da bi narušavanje njezine funkcije moglo dovesti do značajne društveno ekonomske krize s potencijalom da potkopa stabilnost društva i time izazove društvene i sigurnosne posljedice. Hrvatski Zakon o kritičnim infrastrukturama, donesen u Hrvatskom saboru na sjednici 26. travnja 2013. godine, propisuje da su „Nacionalne kritične infrastrukture su sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti.“[1] Različite zemlje ponudile su razne definicije

[1] članak 3. Zakona o kritičnim infrastrukturama objavljenog u Narodnim novinama br. 56/13

kritičnih infrastruktura. Ono što je svima zajedničko je postojanje kompjuteriziranih elementa kojima su povezani drugi fizički sustavi koji će u slučaju ugroze vjerojatno uzrokovati oštećenja na fizičkoj infrastrukturi. Sustavi kao što su električne ili telekomunikacijske mreže, neposredno ovise o infrastrukturi kao i većina procesa u današnjem društvu.

NORMATIVNI OKVIR ZAŠTITE KNI

Pojam kritična nacionalna infrastruktura (Critical Infrastructure Sectors) počeo se koristiti u Sjedinjenim Američkim Državama i Ujedinjenom kraljevstvu, te je upotrijebljen i u Nacrtu Strategije nacionalne sigurnosti RH (2010. godine).[2] Međutim kritična nacionalna infrastruktura je mnogo širi pojam jer se ona ne odnosi samo na objekte već i na sve druge elemente društva koji su nužni za redovito funkcioniranje u miru i ratu. Članice NATO-a i Europske unije uvode pojam kritične infrastrukture a što se odnosi na infrastrukturu o čijem neprekinutom, kontinuiranom radu ovisi funkcioniranje društva uopće. Europska unija kritičnu infrastrukturu definira kao materijalne i informacijske resurse, mreže, usluge i imovinu koji u slučaju ometanja ili uništenja, imaju značajan negativan utjecaj na zdravlje, sigurnost, zaštitu i ekonomsku dobrobit građana i učinkovito funkcioniranje vlada država članica EU.[3] Iz navedene je definicije vidljivo da Europska unija definira kritičnu infrastrukturu kao širi pojam od objekata posebno značajnih za obranu zemlje, a odnosi se i na različite oblike vlasništva (državno, privatno, mješovito). Kritična infrastruktura javlja se u materijalnom i nematerijalnom obliku. I dok je određenje materijalne infrastrukture jasno, nematerijalna infrastruktura odnosi se na informacije o ključnim procesima koji su potrebni za normalno funkcioniranje društva (bankarske informacije, znanje pojedinca potrebno za rad pojedinih elemenata kritične infrastrukture…).

Europska komisija je 2006. godine usvojila The European Programme for Critical Infrastructure Protection (EPCIP) - Europski program za zaštitu kritične infrastrukture kojim želi zaštititi europske kritične infrastrukture (ECI) od terorizma. „Istovremeno namjera je Europske komisije da se koordiniraju i uvjere zemlje članice i javnost općenito kako je nužno zaštititi i informacijske sustave kako bi se zaštitili glavni elementi kritične infrastrukture.“[4] Europska komisija kritičnu infrastrukturu opisuje kao fizičku i informacijsku tehnologiju,

[2] http://www.morh.hr/aktualne-teme/sns/nacrt-strategije-nacionalne-sigurnosti.html - točka 3. 4., pristup 29. 04. 2013.

[3] Smiljanić B.: Kritična nacionalna infrastruktura

[4] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm, pristup 29. 04. 2013.

objekte, mrežu, uslugu i imovinu koja, ukoliko je poremećena ili uništena, može imati ozbiljne posljedice na zdravlje, sigurnost i gospodarstvo građana i učinkovito funkcioniranje vlade u državama članicama Europske Unije. EPCIP - Europski program za zaštitu kritične infrastrukture navodi slijedeće sektore europske kritične infrastrukture (ECI) koje je potrebno posebno štititi: energetika; nuklearna industrija; informacije, komunikacijske tehnologije i ICT tehnologija; voda; hrana; zdravlje; financije; prijevoz; kemijska industrija; prostor i istraživački objekti.[5] Svi navedeni sektori - elementi kritične infrastrukture - neophodni su za redovito funkcioniranje društva, jer bi napadi na njih mogli poremetiti funkcioniranje državnog aparata i gospodarstva i time prouzročiti katastrofalne posljedice. Zakonom o kritičnim infrastrukturama je u zakonodavstvo Republike Hrvatske preuzeta pravna stečevina Europske unije sadržana u Direktivi Vijeća 2008/114/EC od 8. prosinca 2008. o identifikaciji i određivanju europskih kritičnih infrastruktura i procjeni potrebe za unapređenjem njihove zaštite.[6] Tako je definirano da su Europske kritične infrastrukture, infrastrukture koje su od interesa za najmanje dvije države članice, ili jednu državu članicu, a nalaze se na teritoriju druge države članice.[7]

Posebni osvrt zaslužuje područje informacija, komunikacijske tehnologije i ICT tehnologije kao jedan od elementa/sektora kritične nacionalne infrastrukture, u skladu sa odredbom iz članka 4. Zakona o kritičnim infrastrukturama koji u prvom stavku naglašava da "sektori nacionalnih kritičnih infrastruktura mogu biti osobito:....– komunikacijska i informacijska tehnologija (elektroničke komunikacije, prijenos podataka, informacijski sustavi, pružanje audio i audiovizualnih medijskih usluga)." European Network and Information Security Agency (ENISA)[8] - Europska agencija za sigurnost mreža i podataka osnovana je sa zadaćom da radi za institucije Europske Unije i države članice na sprečavanju ugrožavanja informacijske sigurnosti, računalnog kriminala i cyber terorizma. ENISA daje naputke za poticanje suradnje između javnog i privatnog sektora, savjetuje i pomaže Europskoj komisiji i svim državama članicama na području informacijske sigurnosti, te pokušava riješiti sigurnosne probleme, prikuplja i statistički obrađuje podatke o sigurnosnim incidentima u Europskoj uniji, promiče izrade strategije za incidentne situacije, procjene rizika u slučaju informacijskih sigurnosnih prijetnji, te podiže svijest o nužnosti suradnje između svih aktera na području informacijske sigurnosti od običnog građanina, preko lokalne

[5] http://ec.europa.eu/dgs/home-affairs/what-is-new/eu-law-and-monitoring/infringements_ by_policy_critical _infrastructures_protection_en.htm, pristup 29. 04. 2013.

[6] SL L 345/75, 23. 12. 2008.

[7] članak 15. Zakona o kritičnim infrastrukturama

[8] http://www.enisa.europa.eu/about-enisa/activities, pristup 29. 04. 2013.

zajednice do države, te naposljetku Unije. Bitno je istaknuti da članice Europske unije nastavljaju razvijati i održavati baze značajne kritične infrastrukture na nacionalnoj osnovi te su odgovorne za razvoj i kontinuitet poslovanje u slučaju napada pod njihovim nacionalnim nadležnostima. Također dio elementa kritične infrastrukture (sigurnosne, kontrolne) zahtijeva uključivanje privatnih i javnih interesa u čemu nacionalne vlasti imaju isključivu nadležnost. Međutim obzirom na transnacionalnu međuovisnost svih uključenih subjekata nužno je da i Unija ima u tome određenu koordinacijsku ulogu.

Republika Hrvatska u svrhu ostvarenja ciljeva obrane kritične infrastrukture organizira obrambeni sustav koji čini vojna i civilna obrana. Zakonom o obrani[9] i Pravilnikom o kriterijima za određivanje i zaštitu objekata posebno značajnih za obranu zemlje[10] određene su nadležnosti i postupanja vlasnika/korisnika objekata u svezi sa zaštitom objekata kojeg je Vlada Republike Hrvatske uvrstila na popis objekata posebno važnih za obranu. Temeljna obveza nositelja obrambenih priprema je izrada Plana obrane i ažuriranje istoga. Sadržaj Plana obrane nositelja obrambenih priprema propisala je Vlada Odlukom o metodologiji za izradu planova obrane[11] za sve nositelje, te tako i za pravne osobe posebno važne za obranu Republike Hrvatske. Sadržajno planom obrane moraju biti obuhvaćene zadaće koje se odnose na: organizaciju, snage, sredstva, mjere i postupke nositelja obrambenih priprema. Nadalje, Zakonom o kritičnim infrastrukturama jasno je propisana obveza vlasnicima/upraviteljima odgovornim za upravljanje kritičnom infrastrukturom, donošenja Sigurnosnog plana vlasnika/upravitelja koji će osigurati povjerljivost, cjelovitost i raspoloživost organizacijskih, kadrovskih, materijalnih, informacijsko-komunikacijskih i drugih rješenja te stalnih i stupnjevanih sigurnosnih mjera potrebnih za neprekidno funkcioniranje kritične infrastrukture. Radi zaštite kritične infrastrukture nužno je provoditi aktivnosti koje imaju za cilj osigurati funkcionalnost, neprekidno djelovanje i isporuku usluga/robe kritične infrastrukture te spriječiti ugrožavanje kritične infrastrukture.[12]

SIGURNOST INFORMACIJSKE INFRASTRUKTURE

Informacijska infrastruktura je kombinacija računalnih i komunikacijskih sustava koji služe kao temeljna infrastruktura javnim tijelima, industriji i gospodarstvu. Kritične

[9] Zakon o obrani (NN 33/02, 58/02, 100/04, /6/07, 153/09)

[10] Pravilnik o kriterijima za određivanje i zaštitu objekata posebno značajnih za obranu zemlje (NN 120/99)

[11] Metodologija za izradu planova obrane (NN 100/10)

[12] članak 2., Glava IV. Zakona o kritičnim infrastrukturama

infrastrukture kao što su prijevoz i distribucija električne energije nužno ovise o telekomunikacijskoj, javnoj telefonskoj mreži, internetu, zemaljskim i satelitskim bežičnim mrežama i povezanim računalnim resursima za upravljanje informacijama, komunikacijom i kontrolom. Ova povezanost ima nacionalnu sigurnosnu komponentu, jer informacijske infrastrukture omogućuju gospodarsku vitalnost kao i operativnost vojne i civilne vlasti. Pojam informacijske sigurnosti definiran je Zakonom o informacijskoj sigurnosti[13] koji je donio Hrvatski sabor Republike Hrvatske u srpnju 2007. godine. Informacijska sigurnost se definira kao očuvanje:

a) povjerljivosti – osiguranje da je informacija dostupna samo onima koji imaju ovlašteni pristup istoj;

b) integriteta – zaštita postojanja, točnosti i kompletnosti informacije kao i procesnih metoda;

c) raspoloživosti – osiguranje da autorizirani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva.

Kritične informacijske infrastrukture mogu biti posebno osjetljive na napade hakera, kriminalaca i terorista. Glavni alati koji se koriste za napad na kritične sustave su zlonamjerni softver (računalni virusi, crvi, logičke bombe, trojanci) koji mijenjaju i uništavaju podatke ili blokiraju računalne sustave. Alati za nadziranje razmjene informacija u računalnim mrežama kao i alati za modificiranje normalnog funkcioniranja računalne mreže i blokiranje pristupa njegovim servisima također se široko koriste za destruktivne svrhe. Ovi automatizirani alati omogućuju upade iz udaljenih sustava koji se mogu obaviti u roku od nekoliko sekundi, što omogućuje lako pokretanje napada internetom. To uvjetuje važnu osnovu za širi skup aktivnosti vezane uz nacionalnu sigurnost i pripravnosti komunikacije u kriznim stanjima. Širenje interneta uvodi nove sustave, aplikacije i sudionike u konceptualizaciju kritične informacijske infrastrukture i različite opcije za njihovu zaštitu. Pojava i širenje cyber prostora stvara stanje u kojem računalne mreže predstavljaju infrastrukturu samu po sebi. Cyber prostor je primjer infrastrukture koja je postala kritična, jer predstavlja sučelje za većinu društvenih aktivnosti povezanih s računalnim komunikacijskim mrežama. Kritične infrastrukture i informacije potrebne za njihovo pravilno funkcioniranje utječu na sva područja života građana. Danas smo svjedoci sve sofisticiranijih informatičkih napada i ugroza te slučajeva međunarodne špijunaže zlouporabom računalnih sustava. Istovremeno se kriminalne i terorističke organizacije služe informatičkim napadima kako bi brzo došle do novca koji onda koriste za financiranje drugih aktivnosti. Internet i računalni sustavi su postali

[13] Zakon o informacijskoj sigurnosti (NN 79/07)

sastavni dio života, poslovanja, pa i vođenja ratova. Poznato je kako su se metode računalnih napada koristile u zaljevskom ratu, prilikom napada na Irak, te da su danas računalne ugroze na vrhu liste opasnosti po moderni svijet. Europska politika mrežne i informacijske sigurnosti razmatra se u kontekstu postojećih telekomunikacijskih politika, politika zaštite podataka i politika kibernetičkog kriminala. Pri štićenju informacija potrebno je u najvećem broju slučajeva koristiti sve vrste sigurnosnih mjera koje su moguće jer je jedna vrsta kontrole najčešće nedovoljna. Tako treba razlikovati: fizičke kontrole - uključuje kontrolu pristupa koja sprječava neovlaštenim osobama pristup informacijskom sustavu, protupožarnim sustavima, sustavima za kontrolu temperature prostorija, zaštitu od požara, poplava i drugih nepogoda, sustave rezervnog napajanja; logičke kontrole - programirana je u informacijskom sustavu, a uključuje kontrolu pristupa, izvršavanja korisnika, te točno određenih njihovih prava (čitanje, pisanje, ispravljanje); te upravljačke kontrole - odnosi se na organizacijsku strukturu, opis radnih mjesta, edukaciju, proceduru rada kao i na sve dokumente koji iz toga proizlaze.

KAZNENOPRAVNO KVALIFICIRANJE OBLIKA NAPADA NA KNI

Kazneni zakon Republike Hrvatske[14] u aktualnom katalogu inkriminacija iz Posebnog dijela propisuje nekoliko kaznenih djela koja pokrivaju napade na komunikacijske i informacijske tehnologije. U članku 87. definirano je značenje izraza potrebnih za pravilno razumijevanje zakonskih opisa. Tako je „računalni sustav svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja, zaštite i održavanja; računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu; a računalni program je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju.“[15]

Kazneno djelo **Terorizma**, opisano u članku 97. KZ RH, između ostaloga, može se počiniti uništenjem državnih ili javnih objekata, prometnog sustava, infrastrukture uključujući i informacijske sustave, nepokretne platforme na epikontinentalnom pojasu, javnog mjesta ili privatne imovine koje može ugroziti živote ljudi ili prouzročiti znatnu gospodarsku štetu, odnosno ometanjem ili obustavom opskrbe vodom, električnom energijom ili drugim

[14] Kazneni zakon (NN 125/11, 144/12), u daljem tekstu KZ RH
[15] stavci 18., 19. i 20. članka 87.

osnovnim prirodnim resursima, čime je ugrožen ljudski život.[16] Kriminalizirana je već i sama prijetnja počinjenjem ovih kaznenih djela, a kvalificirani su oblici u slučaju uzrokovanja velikih razaranja odnosno prouzročenja smrti jedne ili više osoba. Ovakvim zakonskim opisom kaznenopravna zaštita dana je kako tradicionalnoj tako i suvremenoj informacijskoj infrastrukturi.

Povećana međuovisnost u kombinaciji s većom operativnom složenosti učinila je kritične infrastrukture posebno osjetljivim na prirodne nepogode, ljudske pogreške, tehničke probleme, kao i nove oblike cyber kriminala, terorizma i ratovanja. Svaki od tih događaja može dovesti do teškog pogoršanja funkcionalnosti ili izravne infrastrukturne štete. Razvoj tehnologije i težnje prema potpunoj automatizaciji smanjili su mogućnost ugradnje potrebnih sigurnosnih komponenti, uključujući standarde i postupke otkrivanja, sprječavanja i ublažavanja ugroza. Kritične infrastrukture danas su pod nadzorom i upravljanjem kontroliranih sustava, kao primjer se navode sustavi kontrole proizvodnje i distribucije unutar vodovodnog sustava, elektroenergetskih sustava i drugih velikih infrastruktura. Ovi sustavi obično su spojeni na mrežu, što ih čini ranjivim na cyber napade. Napadač zlonamjerno može poremetiti rad sustava blokirajući ili usporavajući protok informacija kroz kontrolne mreže, također može neovlašteno izmijeniti programirane upute u odgovarajućim kontrolnim uređajima što može dovesti do neispravnosti infrastrukture. Ova ranjivost ne utječe samo na komunalne usluge, nego i baze podataka i sustave koji sadrže razne osjetljive i povjerljive informacije. Mnogi od najkritičnijih sustava su izuzetno osjetljivi na prirodne katastrofe poput potresa ili poplava. Čak i kad nisu fizički ugroženi, iznenadni porast potražnje tijekom krize može izazvati preopterećenje, što dovodi do gubitka ili obustave funkcionalnosti. Slične se posljedice mogu pojaviti kao rezultat namjernog ili slučajnog ljudskog djelovanja. Kaznenim djelom **Uništenje ili oštećenje javnih naprava** iz članka 216. KZ RH kriminalizirano je namjerno uništenje, oštećenje, izmjena, činjenje neuporabljivim, uklanjanje, isključenje ili ometanje u radu naprave (postrojenja) javne uporabe za vodu, toplinu, plin, električnu ili drugu energiju, ili elektroničku komunikacijsku opremu, ako je time izazvan poremećaj u redovitom životu stanovništva.[17] I nehajno prouzročenje nefunkcionalnosti odnosno štete na infrastrukturi na opisani način kazneno je djelo.

Povjerljivost informacijske infrastrukture obuhvaća zaštitu podataka u sustavu od neovlaštenog pristupanja. Postoji opće mišljenje da je ovaj tip zaštite od najveće važnosti za državne institucije i vojsku jer svoje planove i mogućnosti moraju čuvati od mogućih

[16] Kazneno djelo protiv čovječnosti i ljudskog dostojanstva iz devete glave KZ RH, stavak 1. točke 4. i 8.
[17] Kazneno djelo protiv opće sigurnosti iz Glave dvadeset prve KZ RH, stavak 1.

neprijatelja, a može biti značajno i za kompanije koje imaju potrebu zaštititi poslovne planove i informacijske vrijednosti od konkurencije ili neovlaštenog pristupa. Najvažniji aspekt povjerljivosti je identifikacija korisnika i provjera autentičnosti. Identifikacija je proces prijave korisnika na sustav, pri čemu sustav zna da takav korisnik postoji. Provjera autentičnosti je proces kojim sustav želi biti siguran da je osoba koja se prijavljuje upravo osoba poznata sustavu. Najraširenij način provjere autentičnosti je unos lozinke, ali se i sve više razvija tehnička oprema koja jedinstvene ljudske osobine, poput otiska prsta ili mrežnice oka pretvara u digitalne signale. Povjerljivost može biti narušena na nekoliko načina, a neke od najčešćih ugroza povjerljivosti su hakeri, neovlaštena aktivnost, lažno predstavljanje, nezaštićeno preuzimanje podataka. Ovakve aktivnosti mogu se okvalificirati kao kazneno djelo **Neovlaštenog pristupa** iz članka 266. KZ RH koje će počiniti osoba koja neovlašteno pristupi računalnom sustavu ili računalnim podacima, odnosno osoba koja neovlašteno pristupi računalnom sustavu ili računalnim podacima tijela državne vlasti, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa.[18] Kažnjiv je i pokušaj nezakonitog pristupa tuđem računalnom sustavu odnosno podacima.

Integritet predstavlja zaštitu podataka od namjernog ili slučajnog neovlaštenog mijenjanja. Dodatni element integriteta jest zaštita procesa ili programa kako bi se onemogućilo neovlašteno mijenjanje podataka. Glavni zahtjev državnih institucija jedinicama lokalne (regionalne) i područne samouprave te pravnim osobama s javnim ovlastima jest osigurati integritet podataka kako bi se izbjegle zlouporabe i greške. To znači da korisnici ne bi mogli mijenjati podatke na način da ih izbrišu, promjene ili učine ključne podatke nesigurnima. Najbolji primjer gdje je integritet podataka od ključne važnosti su: sustav za kontrolu leta, sustavi u financijskim ustanovama i slični sustavi. Prijetnje integritetu jednake su kao i kod povjerljivosti stoga je nužna zaštita koja se postiže: dodjeljivanjem ovlaštenja, razdvajanjem obveza i rotiranjem. Kaznenim zakonom sankcionirane su sve one radnje kojima se neovlašteno zadire u cjelovitost računalnih podataka ili programa, pri čemu nije odlučno je li im počinitelj neposredno pristupio ili je to učinio izradom i prijenosom nekog malicioznog programa. S obzirom na modalitete postupanja, napadač bi mogao ostvariti zakonski opis kaznenog djela **Oštećenje računalnih podataka** iz članka 268. KZ RH ako neovlašteno u cijelosti ili djelomično ošteti, izmijeni, izbriše, uništi, učini neuporabljivim ili nedostupnim ili prikaže nedostupnim tuđe računalne podatke ili programe, ili kazneno djelo

[18] Kazneno djelo protiv računalnih sustava, programa i podataka iz Glave dvadeset pete KZ RH

Neovlašteno presretanje računalnih podataka iz članka 269. KZ RH, ako neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ili drugome učini dostupnim tako pribavljene podatke. I kod ovih kaznenih djela biti će kažnjiv i sam pokušaj počinjenja.

Dostupnost infrastrukture je garancija ovlaštenim korisnicima sustava da će im sustav biti raspoloživ u svakom trenutku kad za njim imaju potrebu. S obzirom na sve širi prijelaz na elektroničko poslovanje, daljinski i online rad, sprječavanje ili ograničavanje dostupnosti računalnih sustava i podataka pohranjenih unutar njih može ugroziti njihovo nesmetano korištenje i nanijeti goleme štete korisnicima ili pružateljima usluga. To se najčešće čini istovremenim slanjem podataka s većeg broja računala, primjerice distribuirani napadi uskraćivanja usluga (DOS napadi). Kaznenim djelom **Ometanje rada računalnog sustava** iz članka 267. KZ RH sankcionirano je onemogućenje odnosno ometanje rada računalnog sustava, korištenje sustava, računalnih podataka ili programa te računalne komunikacije tako da se ovlaštenim korisnicima onemogući ili otežа nesmetano korištenje njegovih resursa ili međusobna komunikacija. Ugroza integriteta ili tajnosti podataka koji se nalaze unutar sustava nije nužna za opstojnost ovog kaznenog djela.

Kažnjivo je poduzimanje pripremnih radnji za počinjenje naprijed navedenih kaznenih djela Neovlaštenog pristupa, Ometanje rada računalnog sustava, Oštećenje računalnih podataka i Neovlašteno presretanje računalnih podataka. Kazneno će djelo **Zlouporaba naprava** iz članka 272. KZ RH počiniti osoba koja izradi, nabavi, proda, posjeduje ili čini drugome dostupne uređaje ili računalne programe ili računalne podatke stvorene ili prilagođene za počinjenje tih kaznenih djela s ciljem da ih se uporabi za počinjenje nekog od tih djela, ali i onaj tko izradi, nabavi, proda, posjeduje ili čini drugome dostupne računalne lozinke, pristupne šifre ili druge podatke kojima se može pristupiti računalnom sustavu. Radnja kaznenog djela sastoji se u izradi različitih uređaja za računalno krivotvorenje ili neovlašteno presretanje komunikacije, distribuciji računalnih programa za izradu malicioznih programa, pribavljanju tekstualnih, audio ili audiovizualnih podataka koji omogućuju neovlašteni pristup tuđem računalnom sustavu, neovlašteno pribavljanje korisničkih imena ili lozinki. Zbog osjetljivosti podataka koji se prikupljaju i obrađuju u javnom sektoru, teži, kvalificirani oblik predmetnih kaznenih djela, zapriječen težom zatvorskom kaznom do pet godina zatvora, propisan je u slučaju da je koje od tih kaznenih djela počinjeno u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa, osobito ako počinitelj prikriva stvarni identitet i uzrokuje zabludu o ovlaštenom nositelju

identiteta. Najteži oblik, zapriječen osmogodišnjom zatvorskom kaznom ostvaren je ako je neko od ovih kaznenih djela počinjeno sredstvom namijenjenim za izvršenje napada na veći broj računalnih sustava ili je kaznenim djelom prouzročena znatna šteta.[19] Zbog jedinstvene primjene neodređenih vrijednosti obilježja na pojedina kaznena djela od strane svih sudova, Kazneni odjel Vrhovnoga suda na sjednici održanoj 27. prosinca 2012. donio je pravno shvaćanje da zakonsko obilježje „znatna šteta" kod teških kaznenih djela protiv računalnih sustava, programa i podataka iz članka 273. stavka 3. KZ/11, postoji kad vrijednost štete prelazi 60.000,00 kn.[20]

OTKRIVANJE I KRIMINALISTIČKO ISTRAŽIVANJE

Prikrivanje identiteta u cyber prostoru jedan je od razloga zašto je napade na kritične infrastrukture od hakera, kriminalaca ali i terorista teško prevenirati i sankcionirati. Ove se aktivnosti lako poduzimaju iz inozemstva, što otvara pitanje nacionalne, teritorijalno ograničene jurisdikcije u provedbi vlastitih zakona. Usprkos teritorijalnim ograničenjima nadležnosti, zakonodavstvo ipak može dobro kontrolirati internetske prijenose iz inozemstva regulacijom usmjerenom prema osobama i imovini na teritoriju. Moguće je primjerice, strogo sankcionirati krajnje korisnike u državi, zaplijeniti lokalnu imovinu, hardver ili softver stranog davatelja usluga kroz koji su ostvarene kriminalne transakcije ili otežati odnosno onemogućiti uslugu pristupa internetu lokalnih financijskih posrednika koji olakšavaju neželjene transakcije. Ovim i drugim načinima, nacionalno zakonodavstvo unutar svog teritorija može posredno regulirati ponašanje inozemnog pružatelja sadržaja. Nažalost, ovi oblici normativnog nadzora krajnjeg korisnika i posrednika imaju teškoće sa cyber kriminalom i terorizmom počinjenim iz inozemstva. Budući da je riječ o najčešće jednokratnom, diskretnom kriminalu, lokalnim davateljima usluga je teško identificirati i sačuvati relevantne prekogranične tokove podataka. Osim toga, posebnu teškoću predstavlja potreba da se trenutno osiguraju dokazi o kriminalnom ponašanju s obzirom da je u počinjenju tih kaznenih djela relativno lako prikriti identitet i, možda najvažnije, dokazi mogu

[19] Teška kaznena djela protiv računalnih sustava, programa i podataka iz članka 273. KZ RH. Kao i prethodno opisana kaznena djela, ovo je kazneno djelo protiv računalnih sustava, programa i podataka iz Glave dvadeset pete KZ RH

[20] Nakon donošenja novog Kaznenog zakona 7. studenoga 2011. i Zakona o izmjenama i dopunama Kaznenog zakona od 21. prosinca 2012. Kazneni odjel Vrhovnoga suda Republike Hrvatske na sjednicama odjela održanim 26. listopada i 3. i 19. prosinca 2012. je raspravio, a 27. prosinca 2012. donio pravna shvaćanja (broj Su-IV k-4/2012-57) o visinama neodređenih vrijednosti koje su zakonsko obilježje kaznenih djela.

biti relativno brzo uništeni. Zbog toga se nadležna tijela suočavaju s različitim izazovima inozemnog cyber kriminala ili terorizma.

Radi pribavljanja dokaza, istražitelji moraju poduzeti hitne mjere identifikacije računalnih izvora kriminalne aktivnosti, osiguranja ili barem zamrzavanja informacija o relevantnim računalima prije nego što svi zapisi o kriminalnoj aktivnosti budu izbrisani. Dokazi o počinjenju kaznenog dijela često se niti ne nalaze u računalu već se nalaze u računalnoj mreži koja je sastavni dio ogromne većine informatičkih sustava, tako da je nužno dugogodišnje čuvanje i arhiviranje komunikacije unutar računalnih mreža u svrhu detekcije potencijalnih opasnosti, kao i dokazivanja kaznenih dijela nakon počinjenja. Direktivom EU 2006/24/EC[21] propisana je obaveza čuvanja podataka o elektroničkoj komunikaciji uporabom javnih telekomunikacijskih mreža uključujući i pristup internetu. Države članice su dužne čuvati takve podatke u periodu od 6 do 24 mjeseca. Direktiva propisuje da su sigurnosne agencije ovlaštene da traže podatke kao što su: IP adresa i vrijeme korištenja svakog e-maila, telefonskog poziva, tekstualne poruke poslane ili primljene. Dozvolu pristupa takvim podacima daje sud. S druge strane, dio nacionalne kritične infrastrukture mogu biti i privatne tvrtke te je vrlo bitno skupljanje i čuvanje takvih podataka na lokalnoj razini unutar takvih subjekata. Poznate su metode hakerskih napada koji su izvedeni ciljano na manje tvrtke čak i godinama prije nego li je takve tvrtke preuzela tvrtka ili tijelo koje je pravi cilj napada. U takvim slučajevima „inficirana“ tvrtka postaje svojevrsni trojanski konj koji omogućava hakerima pristup željenim podacima.

ENKRIPCIJA KAO FORENZIČKI PROBLEM

Današnji nivo računalne znanosti i tehnologije stavlja forenzičke istražitelje i policijske službenike kao i cijeli pravosudni sustav kod procesiranja slučajeva koji uključuju računalni kriminalitet u veoma težak položaj. Ovo je naročito naglašeno kod slučajeva međunarodnog terorizma jer se radi o skupinama i organizacijama koje imaju sredstva, znanja, te pristup tehnologijama koje mogu onemogućiti otkrivanje forenzičkih računalnih dokaza počinjenja kaznenog djela. Najveći je problem kod otkrivanja dokaza počinjenja ovakvih djela, nemogućnost probijanja kriptografske zaštite podataka na računalu, pametnim telefonima, tabletima, a ta zaštita je legalna i danas komercijalno dostupna. Potpuna enkripcija čvrstog diska, ukoliko je pravilno implementirana predstavlja nerješiv problem računalnim

[21] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML, pristup 29. 04. 2013.

forenzičarima te danas dostupnim metodama i alatima nije moguće pročitati podatke sa takvih sustava. Kriptografija ili enkripcija je šifriranje (zaštita) podataka na način da je sami podatak dostupan isključivo onome kome je podatak i namijenjen. Mehanizam zaštite je tajna (šifra, ključ) koji se koristi za transformaciju podatka iz čitljivog u nečitljivi oblik i obrnuto. Tajne mogu biti i hardverski uređaji (USB tokeni) kartice, prsteni, mobiteli, na kojima ipak postoje korisničke tajne (PIN ili lozinka) koji ovlaštenim korisnicima omogućavaju korištenje ovih tajni. Danas su tehnike i alati napredne kriptografske zaštite široko raširenі, dostupni i jednostavni za korištenje.[22] Pametni telefoni imaju mogućnost enkripcije sadržaja, pri čemu se to ponekad uključuje jednostavnim odabirom opcije u postavkama. S druge strane postoje i komercijalni alati za kripto-analizu: Passware Forensic,[23] Elcon Soft Disk Encryptor,[24] on-line servisi za dekripciju određenih sadržaja,[25] alati i softveri otvorenog koda za čiju je primjenu potrebno veliko specijalističko znanje i sposobnosti iz domene računalnih tehnologija i znanosti. Naprednije kripto alate i tehnike je praktički nemoguće probiti bez znanja lozinke ili bar dijela lozinke. Kriptografija predstavlja izazov i za korisnika budući da niti sam korisnik ne može doći do podataka ukoliko nema pristup lozinki. Ipak, postoje načini na koji se forenzički stručnjaci bore sa ovim problemima ali su oni svi jako ograničeni u svojoj uspješnosti. Neke tipične tehnike otkrivanja su: pogađanje lozinke, brute force attack, poznati uzorci, djelomično poznata lozinka. Važno je napomenuti da mnogi alati podržavaju takav mehanizam zaštite kriptiranog sadržaja koji korisniku omogućuje tvrdnju kako uopće nema podatke na svojem računalu, jer nije moguće, sa dovoljnom razinom sigurnosti, utvrditi da se na disku nalaze bilo kakvi podaci. Neke starije verzije kripto alata imaju propuste što forenzičarima omogućava otkrivanje podataka koji su zaštićeni takvim alatima. Propusti se mogu podijeliti na dvije kategorije: propusti u samom alatu (pogreške u programima) i propusti u primjeni alata od strane korisnika.

Neophodna je kontinuirana edukacija osoba uključenih u istraživanje, otkrivanje i sprječavanje ovakvih djela koja bi bila u trendu sa novim tehnologijama i alatima. Primjerice prilikom izuzimanja dokaza, osim samih računala potrebno je izuzeti i druge predmete koje mogu sadržavati „tajnu riječ" ili „ključ": CD, DVD, USB stickove, vanjske uređaje za pohranu podataka, bilješke, zapise, bilježnice, papire. Potrebno je poduzimati specijalne

[22] Navode se samo poznatiji:Truecrypt – otvoreni kod (*opensource*), Microsoft Windows Bit Locker – komercijalni, SafeBoot – komercijalni, McAfee Endpoint Encryption – komercijalni, PGP – otvoreni kod.

[23] http://www.lostpassword.com/kit-forensic.htm, pristup 20. 04. 2013.

[24] http://www.elcomsoft.com/efdd.html, pristup 20. 04. 2013.

[25] Primjerice Amazon Cloud Service ACS, za dekripciju nekih verzija Microsoft office datoteka.

računalne postupke kao što su snimanje radne memorije prije gašenja računala.[26] Kad je riječ o mobilnim telefonima novijih generacija koji se oduzimaju a pronađeni su uključeni, njih nakon oduzimanja treba pohraniti na led do donošenja mobitela forenzičkom stručnjaku, kako bi se očuvala radna memorija mobitela od gubitka podataka. Nužna je i promjena, odnosno prilagodba zakonskog okvira u cilju legaliziranja postupanja primjenom novih tehnologija. Od listopada 2007. je u Velikoj Britaniji zakonom policiji omogućeno narediti otkrivanje enkripcijskih ključeva (tajni) ili dekripciju kriptiranih podataka pod prijetnjom zatvora u trajanju do dvije godine ili u trajanju do pet godina kad je riječ o slučajevima nacionalne sigurnosti ili zlouporaba na štetu djece.

ZAKLJUČAK

Kako je cjelokupna infrastruktura zahvaćena informacijskim promjenama, brze tehnološke promjene stvaraju novu, dodatnu sigurnosnu prijetnju. Priroda cyber prostora omogućuje napadaču ugrožavanje funkcioniranja kritične infrastrukture bez fizičkog pristupa u blizinu cilja sa smanjivanjem rizika od otkrivanja. Informatička struka omogućava i druge, invazivnije metode pri borbi protiv hakera i računalnih kriminalaca. Primjerice moguć je razvoj i distribucija zakonski odobrenih alata za praćenje i snimanje računala. Postoje dokazi distribucije legalnih virusa, koje antivirusni programi ne detektiraju, primjena kojih omogućava istražiteljima i forenzičarima otkrivanje tajni i pristup podacima. Ovakvi programi omogućavaju i udaljeno, mrežno, praćenje aktivnosti na suspektnom računalu. Iako se na prvi pogled čini se da pitanje zaštite kritičnih informacijskih infrastruktura spada u područje računarstva, nakon daljnjeg razmatranja postaje jasno da aktivnosti treba proširiti izvan tehničkog aspekta. Svakako treba detaljnije ispitati u kojoj mjeri je dopustivo zadirati u privatnost individualnog korisnika računala, osobito kada je riječ o udaljenom, tajnom pristupu usmjerenom na prikupljanje podataka sa računala i praćenje korisnikove aktivnosti. Izazov u zaštiti kritične infrastrukture od cyber prijetnji nije samo tehnički, nego strateški i društveni. Informacijske prijetnje kritičnim infrastrukturama su možda najznačajnije pitanje u području cyber sigurnosti. Samo promišljeni proces može oblikovati politiku učinkovite zaštite kritične infrastrukture od cyber prijetnji i na taj način smanjiti rizike iz virtualnog svijeta s kojim se suočava moderna država. Potrebno je proširiti javnu raspravu o cyber sigurnosti uključivši pri tome socijalne i kulturne aspekte, što će omogućiti optimalni odgovor

[26] Ukoliko se snimi radna memorija prije gašenja računala, umnogome se povećava vjerojatnost da će se otkriti podaci na zaštićenim diskovima.

ugrozama na strateškoj nacionalnoj razini. Prevencija do danas predstavlja najjače oružje protiv računalnih (cyber) ugroza, kao što je i ENISA objavila u nedavnom izvješću. [27]

ABSTRACT:

Computer networks are the basis of modern infrastructure. Cyber space is an example of infrastructure that has become critical as it is an interface for social activities which take place through computer communication networks. Critical infrastructures are now under the control and management of the controlled systems, aspirations towards full automation have reduced the possibility of implementing the necessary safety components, including standards and procedures for the detection, prevention and mitigation of threats. Critical information infrastructure can be particularly vulnerable to attacks by hackers, criminals and terrorists. Criminal activities are undertaken from abroad, which raises the issue of national, territorially limited jurisdiction. Croatian Criminal Code criminalizes certain acts that include attacks on communications and information technology: Terrorism, Destruction or Damage of Public-use Devices, Unauthorised Access, Computer System Interference, Damage to Computer Data, Unauthorised Interception of Computer Data, and Misuse of Devices. A particular difficulty is the requirement to document the evidence immediately because perpetrators of these crimes relatively easily conceal their identities and evidence can be quickly destroyed. A full hard disk encryption is a serious problem for computer forensics because available methods and tools cannot read data from the encrypted systems. It is necessary to continue with the education of all persons involved in the investigation, detection and prevention of such acts in order to get acquainted with new tools and technologies. The problem of protection of critical information infrastructure does not belong exclusively to the field of computing. Based on a deep analysis, a conclusion has been reached that the repressive ways of treatment should be extended beyond the field of information technology. It should be examined in great detail to what extent a violation of privacy of individual computer users is allowed, especially the one relating to the remote, secret access for the purpose of collecting data from a computer and monitoring users activities. Despite such threats, guaranteed human rights should be protected.

Keywords: critical national infrastructure, cyber threats, crimes against computer systems, forensic procedures

[27] http://www.enisa.europa.eu/media/press-releases/urgent-action-is-needed-in-order-to-combat-emerging-cyber-attack-trends, pristup 20. 04. 2013.

LITERATURA:

1. Antoliš K. (2010.): Internetska forenzika i cyber terorizam, Policija i sigurnost, (Zagreb), godina 19. broj 1
2. Badžim J., Baljkas B., Filipović I., Klaić A., Košutić D., Smiljanić B. (2008.): Zbornik radova, „Informacijska sigurnost i zaštita podataka“, Zagreb
3. Bilandžić M., (2012.): Prema strategiji „nacionalne“ sigurnosti Europske unije? – Analiza Strategije unutarnje sigurnosti Europske unije, Pregledni znanstveni članak u okviru istraživačkog projekta „Vojna kultura i identitet OS RH“, Filozofski fakultet, Zagreb
4. Butrimas V., Bruzga A. (2012.): The Cyber Security Dimension of Critical Energy Infrastructure, per Concordiam Volume 3, Number 4
5. Delak B. (2012.): (Ne)varnosti računalništva v oblaku, Korporativna Varnost št. 2
6. Dragović F., Mikac R. (2012.): Stvaranje sigurnosnih politika EU, Policija i sigurnost, (Zagreb), godina 21. broj 1
7. Horjan A., Šuperina M. (2012.): Izgradnja strategije unutarnje sigurnosti EU, Policija i sigurnost, (Zagreb), godina 21. broj 1
8. Jelić M. (2012.): Informacija – najveća svjetska moć, CSO, godina 4. broj 4
9. Smiljanić B. (2008.): Kritična nacionalna infrastruktura, Zbornik radova „Poslovanje i sigurnost“, Zagreb
10. Solomun D. (2001.): Nacionalna sigurnost, Policija i sigurnost, (Zagreb), godina 10. broj 1-6
11. Solomun D. (2010.): Hrvatska platforma za smanjenje rizika od katastrofa, Zbornik radova, Zagreb
12. Protrka N. (2011.): Računalni podaci kao elektronički (digitalni) dokazi, Policija i sigurnost, (Zagreb), godina 20. broj 1

PROPISI:

1. Kazneni zakon Republike Hrvatske (NN 125/11, 144/12)
2. Metodologija za izradu planova obrane (NN 100/10)
3. Pravilnik o kriterijima za određivanje i zaštitu objekata posebno značajnih za obranu zemlje (NN 120/99)
4. Pravno shvaćanje Kaznenog odjela Vrhovnoga suda Republike Hrvatske broj Su-IV k-4/2012-57 o visinama neodređenih vrijednosti koje su zakonsko obilježje kaznenih djela od 27. prosinca 2012.
5. Zakon o informacijskoj sigurnosti (NN 79/07)
6. Zakon o kritičnim infrastrukturama (NN 56/13)
7. Zakon o obrani (NN 33/02, 58/02, 100/04, /6/07, 153/09)

WEB STRANICE:

1. http://www.morh.hr/aktualne-teme/sns/nacrt-strategije-nacionalne-sigurnosti.html, pristup 29. 04. 2013.
2. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm, pristup 29. 04. 2013.
3. http://ec.europa.eu/dgs/home-affairs/what-is-new/eu-law-and-monitoring/infringements_by_policy_critical_infrastructures_protection_en.htm, pristup 29. 04. 2013.
4. http://www.enisa.europa.eu/about-enisa/activities, pristup 29. 04. 2013.
5. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML, pristup 29. 04. 2013.
6. http://www.lostpassword.com/kit-forensic.htm, pristup 20. 04. 2013.
7. http://www.elcomsoft.com/efdd.html, pristup 20. 04. 2013.
8. http://www.enisa.europa.eu/media/press-releases/urgent-action-is-needed-in-order-to-combat-emerging-cyber-attack-trends, pristup 20. 04. 2013.