FBIM Transactions

IZAZOVI INFORMACIONE BEZBEDNOSTI U SISTEMU ODBRANE REPUBLIKE SRBIJE

CHALLENGES OF INFORMATION SECURITY IN THE DEFENSE SYSTEM OF THE REPUBLIC OF SERBIA

Hatidža Beriša
Univerzitet odbrane, Vojna akademija, Beograd, Srbija

Katarina Jonev
Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, Srbija

JEL Category: **D82, F52**

Apstrakt

Informaciona bezbednost je aspekt bezbednosti koji se odnosi na bezbednosne rizike povezane sa upotrebom informaciono-komunikacionih tehnologija, uključujući bezbednost podataka, uređaja, informacionih sistema, mreža, organizacija i pojedinaca. Razvoj novih tehnologija donosi nesumnjive koristi za društvo, ali paralelno sa tehnološkim razvojem dolaze i novi bezbednosni izazovi. Visokotehnološki kriminal i hakerski napadi na informacione sisteme mogu bitno da ugroze kako funkcionisanje državne infrastrukture i nacionalnu bezbednost, tako i sistem odbrane Republike Srbije. Napadi na informacione sisteme mogu da bitno ugroze funkcionisanje sistema odbrane Republike Srbije, kao što je bio slučaj u Estoniji 2007. godine, kada je izvršen sajber napad na IKT sisteme državnih organa, kada je došlo do blokade informacionih sistema. Poznat je i slučaj unošenja računarskog virusa „Staksnet" u nuklearnu elektranu u Iranu 2010. godine, sa namerom da se izvrši sabotaža industrijskih sistema. Pored toga, postoje pretnje po odbranu koje se po međunarodnom pravu ne mogu svrstati u oblike oružane agresije, ali su prisutne u međunarodnim odnosima. Prema podacima Ministarstva unutrašnjih poslova, broj prijavljenih krivičnih dela iz oblasti visokotehnološkog kriminala raste 50% godišnje. Napadi na servere državnih organa sve su učestaliji i napredniji. U radu će sagledati sa kojim se izazovima informaciona bezbednost u sistemu odbrane Republike Srbije, Takođe u radu će se razmatraju neki od načina ugrožavanja savremenih komunikacionih i računarskih sistema i mreža

Ključne reči: *bezbednost, sistem odbrane, informaciona bezbednost, izazovi, Republika Srbija, ugrožavanje, mreža*

Adresa autora zaduženog za korespodenciju:
Hatidža Beriša
berisa.hatidza@gmail.com

Abstract

Information security is an aspect of security related to the security risks associated with the use of information and communication technologies, including the security of data, devices, information systems, networks, organizations and individuals.

The development of new technologies brings undoubted benefits to society, but parallel to technological development, new security challenges are coming. High-tech crime and hacking attacks on information systems can significantly jeopardize the functioning of state infrastructure and national security, as well as the defense system of the Republic of Serbia. Attacks on information systems can significantly jeopardize the functioning of the defense system of the Republic of Serbia, as it was the case in Estonia in 2007, when cyber-attack on the ICT systems of state authorities was carried out, when information systems were blocked. The case of the introduction of a computer virus "Stuxnet" in the nuclear power plant in Iran in 2010 to sabotage industrial systems is also known. In addition, there are threats of defense that cannot be classified under international law as forms of armed aggression but are present in international relations. According to the Ministry of Internal Affairs, the number of reported criminal offenses in the field of high-tech crime is growing 50% annually. Attacks on state authority servers are even more frequent and advanced. The paper will discuss the challenges of information security in the defense system of the Republic of Serbia. Also, in this paper will be considered some of the threats of using modern communication and computer systems and networks.

Keywords: *security, defense system, information security, challenges, Republic of Serbia, threats, network*

1 UVOD

Kineski filozof Konfučije (551-479. pre n. e.) rekao je „Upoznaj sebe i upoznaj protivnika, pa ćeš biti nepobediv“. Nemamo nameru apsolutizirati ovu izjavu, ali želimo istaći onaj deo koji govori o značaju upoznavanja neprijatelja.

Sigurno je da su, od kada je ratova, zaraćene strane još u pripremi ratnih dejstava, a u toku oružanog sukoba naročito, nastojale da o protivniku saznaju što više - s jedne strane i da prikriju što više podataka o sebi - s druge strane. Ova nepobitna činjenica i bitan preduslov uspeha u ratu i dobija na značaju sve više u savremenim kao i u eventualnim budućim ratovima.

U savremenim uslovima posedovanje informacija ima veliki značaj za sve oblike društvenih delatnosti, a posebno u oblasti bezbednosti i odbrane. Mnoge zemlje u svetu danas pridaju izuzetan značaj bezbednosti informacija i informacionih sistema.[1]

Jedan od zadataka osiguranja bezbednosti informacija kojima raspolaže neka organizacija je i zaštita od preuzimanja informacija o strane neovlaštenih lica i službi. Za preuzimanje na daljinu aktuelne su informacije koje cirkulišu posredstvom sredstava telekomunikacionog i informatičkog sistema. To su poverljivi podaci i informacije u vidu usmenih saopštenja u telefonskim razgovorima, video-konferencijama, radio i radio telefonskim vezama, dokumenta sa poverljivim sadržajima, podaci i informacije koje se obrađuju na računarima kao i razni podaci u računarskim mrežama, iz kojih protivnici mogu izvući korisne informacije za sebe.

Moguće je razmatrati tri aspekta sigurnosti informacija (Pleskonjić, Maček, Đorđević, & Carić, 2007, str. 2):

- napad na sigurnost - (engl. security attack) bilo koja akcija koja ugrožava sigurnost informacija;

[1] U okviru Saveta bezbednosti Ruske Federacije postoji Odeljenje za upravljanje informacionom bezbednošću. Saveznim zakonom o zaštiti podataka iz 1972. godine u SR Nemačkoj bile su definisane obaveze nadležnih u vezi sa bezbednošću informacionih sistema, na osnovu kojih je u Nemačkoj osamdesetih godine na poslovima referenata bezbednosti u informacionim sistemima radilo oko 10 hiljada ljudi.
U Americi je 1960. godine formirana DCA (Defense Communications Agency), kao agencija za “odbranu” komunikacija. Od 1991. godine DCA je prerasla u agenciju za odbranu informacionih sistema DISA (Defense Information Systems Agency), i kao ogranak NSA, zadužena je za pomoć u komandovanju, upravljanju, komunikacijama i informacionim sistemima predsedniku i potpredsedniku SAD, ministru odbrane i najvišim vojnim komandantima, odeljenjima Ministarstva odbrane u svim mirnodopskim i ratnim uslovima. U februaru 2003. godine, predsednik SAD, Džordž Buš potpisuje Nacionalnu strategiju bezbednosti “sajberspejsa” (National Strategy to Secure Cyberspace) kojom se stvaraju okviri za zaštitu informatičke infrastrukture od izuzetne važnosti za ekonomiju i uopšte bezbednost života.

- sigurnosni mehanizam - (engl. security mechanism) mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada;
- sigurnosna usluga (engl. security sevice) - usluga koja povećava sigurnost sistema za obradu i prenos podataka. Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.

2 IZAZOVI BEZBEDNOSTI INFORMACIONE DIMENZIJE

Složenost sajber prostora i njegove karakteristike, neminovno utiču i na informacionu dimenziju u kojoj savremeno društvo uspostavlja sve informacione tokove i obavlja svoje aktivnosti. Široka primena savremenih IKT uvećala je ranjivost društva, koje je u informacionoj dimenziji izloženo mnogim opasnostima i pretnjama, što je nekada bila karakteristika, isključivo, fizičkih domena ljudske delatnosti. Tehnološki razvoj, ekspanzija IKT i sajber prostor doneli su nove opasnosti po bezbednost u informacionom ambijentu − sajber pretnje. Informacioni ambijent povezan je sa skoro svim bezbednosnim izazovima koji se navode u strateškim razmatranjima nacionalne bezbednosti većine savremenih država, vojnih i bezbednosnih saveza i organizacija (Slavković, Kršljanin, 2015, str. 341).

Internet, kao osnova sajber prostora, nema centralizovano upravljanje, samim tim nema ni centralizovanu kontrolu, svačiji i ničiji, postao je zanimljiv za mnoge interesne grupe sa različitim pretenzijama. Danas, IKT čine osnovu infrastrukture svih esencijalnih sistema u jednoj državi. Energetski, transportni, finansijski, telekomunikacioni, bezbednosni i odbrambeni sistemi direktno su zavisni od funkcionisanja IKT. Time je savremeni svet doveden u paradoksalnu situaciju: baziranost na informacionim tehnologijama predstavlja i glavnu slabost zbog zavisnosti od tehnologija. Glavnu opasnost po sisteme zasnovane na IKT predstavljaju napadi na informacionu i telekomunikacionu (kritičnu) infrastrukturu.

Države, koje se oslanjaju na IKT, izloženije su i ranjivije na sajber napade, prekide rada ili uništenje informacionih dobara i tehnologije. Direktna zavisnost informacionih tokova od IKT čini industrijska društva ranjivijim, dok su zemlje sa nižim nivoom zavisnosti od IKT manje ranjive i mogu da iskoriste ranjivost razvijenijih zemalja za ostvarenje svojih strateških ciljeva.

Mogućnost izvršavanja destruktivnih akcija, sa ekonomskog, bezbednosnog i vojnog aspekta, sasvim je realna. Razvijanje ofanzivnih strategija u informacionom ambijentu ne zahteva visoke investicije kao za konvencionalno ratovanje, što ih čini dostupnim velikom broju aktera. Sajber oružje mogu razvijati pojedinci ili grupe, a za to su im potrebni jedino znanje i motivacija. Državama ili akterima, kojima do sada nije pridavan značaj u strateškom kontekstu, to omogućava drugačiju poziciju u sajber prostoru, jer ravnotežu moći određuje pre znanje nego količina vojnog arsenala.

Trend ispoljavanja pretnje u sajber prostoru ukazuje na stalni razvoj sposobnosti napadača za ugrožavanje IKT, napade na računarske mreže, ispoljavanje nasilja i nanošenje štete. Opasnosti su, pre svega, zasnovane na tehničkim i tehnološkim karakteristikama i ranjivostima Interneta i sajber prostora. Znatan uticaj na bezbednost Interneta ostvaruju i tradicionalne forme društvenih konflikata i sukoba jer su eskalirali u sasvim nove forme u globalnoj računarskoj mreži.

Sajber napadom se prevashodno ciljaju informaciona dobra, a prekid ili uništavanje kritične informacione infrastrukture i informacionih tokova, predstavlja značajnu ranjivost društvenih vrednosti, koja može dovesti do širokog dijapazona posledica i štete po društvo. Konvergencija fizičkih napada sa sajber napadima na kritične infrastrukture, opasne terorističke aktivnosti usmerene na ugrožavanje elektronskih i automatizovanih sistema, kojima su podržani energetski, komunikacioni, komercijalni i odbrambeni sektor, predstavljaju samo deo mnogobrojnih ranjivosti društva u informacionoj dimenziji. Sajber napadi na sisteme kontrole, koji su osnova kritične infrastrukture i pružaju povezanost između realnog i virtuelnog sveta, mogu rezultirati u velikim materijalnim gubicima i ljudskim žrtvama. Sajber napad na sisteme za prikupljanje podataka, nadzor, praćenje i upravljanje - SCADA sisteme (engl. Supervisory Control And Data Acquisition) može imati dramatične posledice po društvo. Trend povećanja međupovezanosti sistema kontrole

unutar Interneta, uz upotrebu standardnih protokola iz ekonomskih razloga i zbog povećanja uzajamne operativnosti, znatno povećavaju rizike i ugrožavaju IKT i društvene aktivnosti.

Koliko god se pretnja sajber napada činila kao precenjena, mere koje se danas preduzimaju radi suprotstavljanja nisu gubici ni vremena, ni energije, ni novca. Preventivne aktivnosti u polju zaštite od potencijalne sajber pretnje svakako da osnažuju mere koje se preduzimaju u borbi protiv onoga što je trenutno najveća pretnja informacionom ambijentu– zloupotreba sajber prostora u kriminalne svrhe.

2.1 Načini ugrožavanja informacione bezbednosti u računarskim mrežama i IKT sistemima

U osnovi napada su akcije koje su usmerene na ugrožavanje sigurnosti informacija u računarskim mrežama i telekomunikacionim sistemima. Postoje različite vrste napada, ali se one generalno mogu klasifikovati u četiri osnovne kategorije:

- **Presecanje**, tj. prekidanje (engl. interruption) predstavlja napad na raspoloživost (engl. availability). Presecanjem se prekida tok informacija, tj. onemogućava se pružanje neke usluge ili funkcionisanje nekog sistema. Ovakav napad je aktivan.
- **Presretanje** (engl. interception) predstavlja napad na poverljivost (engl. confidentiality). Presretanje može biti u praksi sprovedeno kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije ili slično. Kao pasivan napad, teško se otkriva jer ne menja podatke tj. ne utiče na unutrašnje funkcionisanje sistema. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.
- **Izmena** (engl. modification), predstavlja napad na integritet (engl. integrity). Po svojoj prirodi, to je aktivan napad. Ukoliko se dešava na prenosnom putu, može se, na primer, ispoljiti kao napad "čovek u sredini" (engl. man in the middle). Napad se može obaviti i unutar nekog računarskog sistema - u tom slučaju se radi o izmeni podataka, pristupnih prava, načina funkcionisanja programa ili sistema i slično. Iako menja podatke ili sistem, često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.
- **Fabrikovanje** (engl. fabrication), predstavlja napad na autentičnost (engl. authenticity). Napadač izvodi ovaj aktivan napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlašćene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, servera ,Web strane ili nekog drugog dela sistema.

Ako se razume osnovni pristup koji napadači koriste da "osvoje" neki sistem ili mrežu, lakše će se preduzimati odbrambene mere znajući šta je promenjeno i protiv čega.

Osnovni koraci napadačeve metodologije (Pleskonjić, Maček, Đoršević Carić, 2007, str. 4) su:

a. **Ispitaj i proceni.** Prvi korak koji napadač preduzima jeste istraživanje potencijalne mete i identifikovanje i procena njenih karakteristika. Te karakteristike mogu biti podržani servisi, protokoli s mogućim ranjivostima i ulaznim tačkama. Napadač koristi informacije prikupljene na ovaj načina kako bi napravio plan za početni napad.
b. **Eksploatiši i prodri.** Nakon što je istražio potencijalnu metu, napadač pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem. Ako su mreža ili umreženi računari (obično server) potpuno osigurani, aplikacija postaje sledeća ulazna tačka za napadača - napadač će najlakše upasti u sistem kroz isti ulaz koji koriste legitimni korisnici. Na primer, može se upotrebiti stranica za prijavljivanje ili stranica koja ne zahteva proveru identiteta.
c. **Povećaj privilegije.** Nakon što napadač uspe da ugrozi aplikaciju ili mrežu - na primer ubacivanjem koda u aplikaciju ili uspostavljanjem legitimne sesije na operativnom sistemu - odmah će pokušati da poveća svoja prava. Posebno će pokušati da preuzme administratorske privilegije tj. da uđe u grupu korisnika koji imaju sva prava nad sistemom. Definisanje najmanjeg nužnog skupa prava i usluga koji je neophodno obezbediti korisnicima aplikacije, primarna je odbrana od napada povećanja privilegija.
d. **Održi pristup.** Kad prvi put uspe da pristupi sistemu, napadač preduzima korake da olakša buduće napade i da prikrije tragove.

Čest način olakšanja budućih pristupa jeste postavljanje programa sa zadnjim vratima (engl. back door), ili korišćenje postojećih naloga koji nisu strogo zaštićeni. U prikrivanje tragova često spada brisanje dnevničkih datoteka (engl. log files) i skrivanje napadačevih alata. Uzevši u obzir da su dnevničke datoteke jedan od objekata koje napadač želi da modifikuje kako bi prikrio tragove, one treba da budu osigurane i da se redovno analiziraju. Analiza dnevničkih datoteka često može otkriti rane znakove pokušaja upada u sistem, i pre nego što nastane šteta.

e. **Odbij uslugu.** Napadači koji ne mogu da pristupe sistemu ili računarskoj mreži i da ostvare svoj cilj često preduzimaju napad koji prouzrokuje odbijanje usluge (engl.Denial of Sevice attack, DoS), kako bi sprečili druge da koriste aplikaciju. Za druge napadače DoS napad je cilj od samog početka.

Problemi bezbednosti i zaštite podataka u širokopojasnim telekomunikacionim mrežama mogu se uspešno rešavati samo ako su unapred poznate, ili realno procenjene pretnje kojima mreže mogu biti ugrožene.

2.2 Ugrožavanja informacione bezbednosti putem kompromitujućeg elektromagnetnog zračenja

Kompromitujuće elektromagnetno zračenje (KEMZ) računara i telekomunikacione opreme je takođe jedan od mogućih načina za ugrožavanje sigurnosti podataka i informacija. Mikročipovi, monitori, štampači i bilo koji drugi elektronski uređaji i komponente emituju elektromagnetne talase. Kao posledica ove emisije može da se desi, zahvaljujući interferenciji, da na TV prijemniku uhvatite sliku sa monitora računara u susednoj prostoriji. Ova pojava je izuzetno važna za sve institucije i organizacije koje imaju poverljive podatke i informacije na svojim računarima i poznata je pod nazivom kompromitujuće elektromagnetno zračenje (KEMZ)[2]. Koristeći TEMPEST (Transient Electromagnetic Pulse Emanation Standard) tehnologiju[3] informacija sa bilo koje digitalne mašine može da bude sinuta i rekonstruisana obaveštajno korisno. Ova tehnologija je posebno korisna za prihvat podataka i informacija koje se nalaze na računaru, prikazuju na monitoru, štampaču, kucaju na tastaturi i prenose kroz kablove iz kompleta računara.

Teško je doći do konkretnih dokaza o slučajevima skidanja podataka i informacija sa računara koristeći KEMZ, a posebno utvrditi nivo i udaljenost sa koje se može signal rekonstruisati. Kod nas je ta mogućnost dokazana još davne 1988. godine na savetovanju u Institutu za bezbednost pod nazivom „Elektromagnetska kompatibilnosti i protivelektronska zaštita računara i računarskih mreža“ (Rodić, Đorđević, 2004, str. 35-37).

2.2.1 Računarski virusi kao oblik ugrožavanja

Od rizika koji nastaju korišćenjem mogućnosti koje pruža IKT sistem izdvajaju se rizici koji nastaju korišćenjem računarske tehnologije kao okosnice IKT sistema. Od savremenih zlonamernih (malicioznih) aktivnosti usmerenih prema IKT sistemu koji dovode do degradacije funkcionisanja

[2] KEMZ - Kompromitujuće Elektromagnetno Zračenje - predstavlja nenamerne elektromagnetne emisije prilikom prenosa, obrade ili čuvanja podataka, čijim prijemom i analizom se može otkriti sadržaj tih podataka (član 2. stav 1. tačka 18. Zakona o informacionoj bezbednosti).

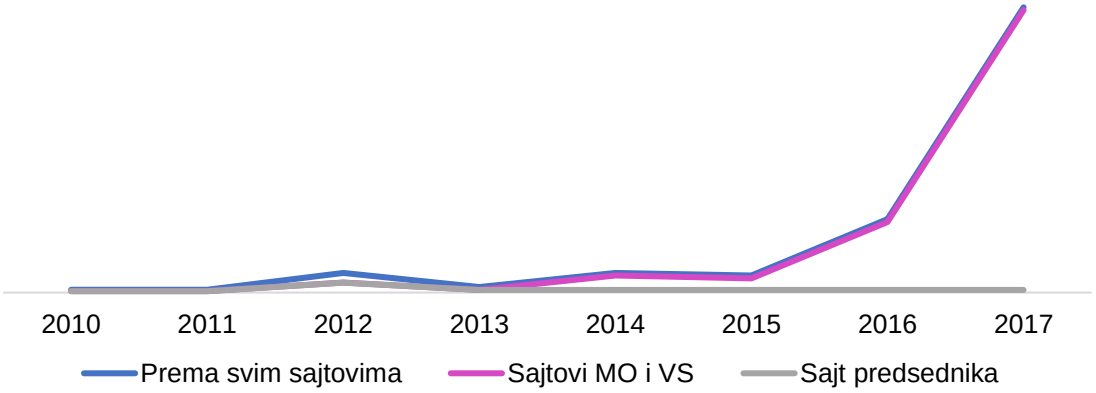
[3] TEMPEST je skraćenica od Transient Electromagnetic Pulse Emanation Standard - privremeni standard za emisiju pulsno modulisanog signala. Ovaj pre svega defanizvni standard je skup stavova o elektromagnetnom zračenju preko kog uređaji mogu da zrače bez kompromitacije informacija koje se nalaze u njima. TEMPEST istovremeno definiše opremu i uslove koji određuju procese koji imaju za cilj da preveniraju kompromitujuće zračenje. Uređaji koji su usklađeni sa ovim standardom nazivaju se TEMPEST sertifikovani uređaji. M TEMPEST (Transient Electromagnetic Pulse Surveillance Technology) je program američke vlade za evaluaciju elektronske opreme za prisluškivanje. Može se reći da su uređaji za vojne i državne primene (bezbednost) testirani u skladu sa strožim standardima. Navodno dva tipa standarda: NACSIM 5100 A (SAD) i AMSG 720 B (NATO). Oba standarda su primenljiva na svim delovima računarskog sistema, a ne samo na video jedinice ili terminale. Merne metode i standardi NACSIM nisu poznati izvan Amerike. AMSG standard je specijalan slučaj korišćenja vojnih i državnih aplikacija u zemljama NATO-a. Američki standard u vezi sa kompromitujućim elektromagnetnim zračenjem (KEMZ), naziva se memorandum o nacionalnoj bezbednosti komunikacija (direktiva za TEMPEST bezbednost) - NACSIM 5100 (National Communications Security Information Memorandum).

i bezbednosti sadržaja pohranjenih u informacionim sistemima izdvajaju se:

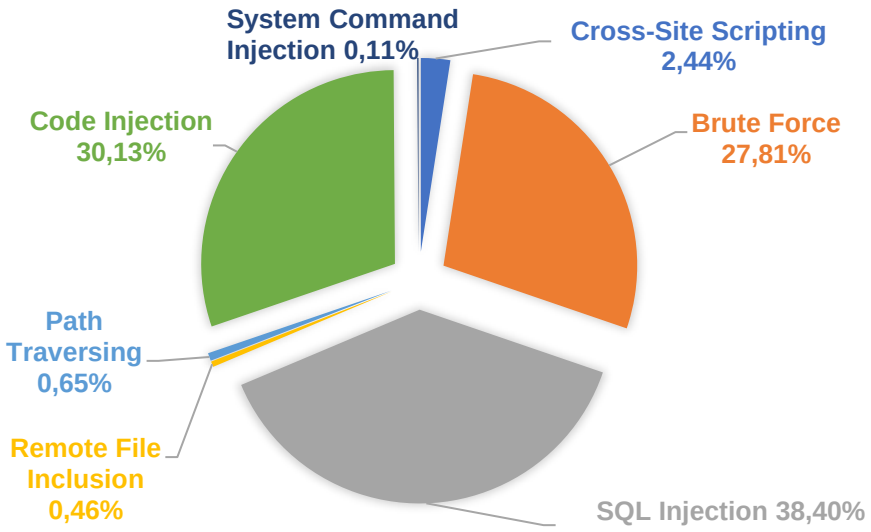
1. Crv (engl. worms) je program kreiran da se samostalno kreće i prebacuje sa računara na računar. Tipičan crv je dizajniran tako da može da otkrije druge kompjutere u okruženju sa specifičnim osobinama koje mu omogućuju da uspešno napadne sledeći računar i samostalno se instalira na isti. Nakon toga crv skenira neposredno okruženje novoosvojenog domaćina i ciklus se ponavlja dokle god ima novih računara pogodnih za osvajanje.
2. Trojanski konj (trojanac) je drugi tip štetnog softvera.Za razliku od crva, trojanac zahteva intervenciju čoveka da bi se prebacivao sa sistema na sistem. Trojanski konj je dobio ime jer liči na nešto bezopasno. Može da bude ugrađen u kompjuterski program kao da je igrica, čuvar ekrana ili neki drugi program. Ali jednom aktiviran trojanac će napraviti štetu za koju je dizajniran. Može to da bude skeniranje okolne mreže u cilju pronalaženja nove žrtve, skeniranje sistema u cilju pronalaženja važnih podataka ili instalacija drugog malicioznog softvera.
3. Napadi zagušenja bafera je specifična vrsta napada gde je napad dizajniran tako da izvršavanjem instrukcija napadača zbuni napadnuti IKT sistem. Napadački program uspostavlja komunikacionu sesiju sa specifičnim komponentama za napadnuti IKT sistem i šalje specijalno napravljene poruke za isti. Takve poruke namerno šalju veliku količinu podataka u ulazni bafer napadnutog IKT sistema. Tako velika količina podataka u programima osetljivim na ovu vrstu napada može da dovede do izvršavanja napadačevih instrukcija umesto izvornih. Takve nove instrukcije obično sadrže kod kojim se „otvara“ napadnuti IKT sistem i dozvoljava delimično ili potpuno preuzimanje kontrole nad napadnutim sistemom. Ova vrsta napada je komplikovana za razvoj i pretpostavlja detaljno znanje o internoj arhitekturi ciljanog IKT sistema (hardver i softver) kao i detaljno znanje o programu ili servisu koji se napadaju. Crvi, trojanci, virusi i drugi maliciozni softveri veoma često koriste ovu vrstu napada radi ubacivanja u novi sistem žrtve.
4. Špijunski softver (engl. spyware) je odeljen širokoj grupi tehnika koje se koriste da na skriven način dobiju informacije sa računara. Špijunski softver najčešće uzima oblik računarskog koda koji je instaliran na računar korisnika bez njegovog znanja i pristanka, koji sakuplja određene informacije i šalje ih nekom centralnom izvoru. Ovakav softver može izmeniti ponašanje korisnikovog računara.
5. Pecanje (phising - igra reči sa reči fishing - pecanje) je napada na korisnike računara u pokušaju da ih prevari da učine radnju koja je predviđena da ih ošteti. Ta šteta može, na primer, imati oblik bilo koje vrste prevare ili instalacije malvera ili špijunskog softvera na računar korisniika.
6. Synchronization poplava je napad na ciljani IKT sistem, konkretno napad na ključne projektne karakteristike TCP/IP mrežnog protokola. U SYN poplavi, napadač šalje hiljade SYN paketa ciljanom IKT sistemu. SYN paket je obično poruka poslata sa drugog računara koji želi da ustanovi mrežnu konekciju sa metom. Nakon prijema SYN paketa, ciljani IKT sistem odgovara sa SYN/ACK (engl. acknowledgement - potvrda) i u tom trenutku počinje komunikacija.
7. Napad za odbijanje usluge (engl. Denial of Service attacks - DoS napad) je napad na ciljani IKT sistem pri čemu je cilj da se isti delimično ili potpuno onesposobi. Svrha DoS napada jeste da predstavi ciljani sistem beskorisnim za legitimne namene. Radi efikasnije prikrivenosti napada napadači koriste razne tehnike za izbegavanje detekcije. U malver ekonomiji, autori malvera smatraju da su njihovi proizvodi uspešni ukoliko su u stanju da izbegnu detekciju.
8. „Napad nultog dana“ je ime novih napada na prethodno nepoznatoj ranjivosti napadnutog IKT sistema, ili potpuno nova vrsta napada na postojeće slabosti IKT sistema. Izraz „nulti dan“ potiče od broja dana upozorenja od vremena kada je ranjivost objavljena i kada je zloupotrebljena. Drugim rečima, ovo su ranjivosti za koje ne postoje zakrpe.
   Napredne istrajne pretnje (engl. Advanced Permanent Threat - APT) su podigle dosta buke i uzrok su mnogim dezinformacija u stručnim krugovima. Od ove vrste napada trenutno ne postoji adekvatna odbrana.
9. Brutal-force attack je vrsta napada koja za cilj ima razbijanje lozinki za pristup IKT sistemu. Napad se izvodi od strane zlonamernog

korisnika ili softvera na računar (server) ili operativni sistem da bi se došlo do tajne lozinke ili simetričnog ključa za enkripciju. Najčešće se vrši pogađanjem lozinke ili ključa dok se ne otkriju.

10. SQL injection predstavlja napad na bilo koju vrstu baze podataka, uključujući i Oracle baze podataka.
11. Cross-site scripting (XSS) predstavlja tip ranjivosti računarskih mreža u IKT sistemu i tipično se javlja u veb aplikacijama. U ovoj vrsti napada napadač ubacuje client-side skript u veb strane koje su pregledali drugi korisnici. XSS ranjivosti mogu se korisiti od strane napadača radi zaobilaženja kontrole pristupa određene politikom sajta. Ovi napadi čine oko 80% napada koji su izvršeni na veb sajtovima. Uticaj ovakvog napada može biti u rasponu od male smetnje do ozbiljnog bezbednosnog rizika.
12. Root.kit napadi se izvode infiltriranjem zlonamernog softvera u ciljani IKT sistem. Dizajniran je tako da skriva sebe u okviru ostalih resursa (direktorijuma, fajlova, procesa i sl.). Pri tome svoje delovanje sve vreme zadržava u napadnutom IKT sistemu.



Slika 1: Maliciozne aktivnosti na hostovanim Internet prezentacijama po godinama (CKISIP)
Izvor: Statistički podaci preuzeti iz periodičnog izveštaja CKISIP



Slika 2: Maliciozne aktivnosti prema servisima MO i VS na internetu (KISIP)
Izvor: Statistički podaci preuzeti iz periodičnog izveštaja CKISIP

Iz svega navedenog može se zaključiti da je IKT sistem stalno izložen raznim rizicima koji prete da degradiraju njegovu funkciju i učine ga osetljivim na gubitak poverljivih informacija. Njegov značaj za sistem odbrane Republike Srbije i Republiku Srbiju u celini nameće potrebu sveobuhvatne procene rizika. Procena rizika u području informacione bezbednosti IKT sistema podrazumeva sistematičan proces organizovanja informacija i znanja u cilju donošenja odluka u

okviru šireg procesa upravljanja rizikom u kome se na sveobuhvatan način i na svim nivoima moraju identifikovati pretnje i analizirati i proceniti rizici asocirani sa izloženostima delovanju tih pretnji. Zbog toga se proces procene rizika mora sprovesti na svim nivoima komandovanja i rada i u svim sistemima od značaja za operativne i funkcionalne sposobnosti.

Pregled malicioznih aktivnosti na hostovanim internet prezentacijama prikazan je na slici 1.

U pogledu napada na servise MO i VS na Internetu, zastupljenost pojedinih malicioznih aktivnosti je data na slici 2.

Prikazani podaci pokazuju da je IKT sistem MO i VS konstantno pod napadima različitog tipa, a takođe može se uočiti trend povećanja ispoljavanja zlonamernih aktivnosti u 2017. godini u odnosu na 2016. godinu, prema svim Internet sajtovima.

3 ZAKLJUČAK

Sagledavanjem izazova, rizika i pretnji odbrani Republike Srbije, složenosti i kompleksnosti sistema odbrane, kao i aktivnosti na planiranju i pripremama odbrane Republike Srbije, uviđa se ogroman značaj pravovremenih, sigurnih, proverenih, zaštićenih, odnosno bezbednih informacija. Složenost i kompleksnost sistema odbrane, kako njegove strukture, tako i sistema upravljanja, rukovođenja i komandovanja sistemom, prouzrokuje i niz mera i aktivnosti koje treba preduzeti u pogledu informacione bezbednosti.

Planiranje priprema civilnog društva za odbranu treba da bude stalan, planski, organizovan, sveobuhvatan, racionalan i efikasan proces, zasnovan na realnim mogućnostima i usklađen sa postojećim i potencijalnim izazovima, rizicima i pretnjama po bezbednost i odbranu Republike Srbije. Jedinstvenom metodologijom pripremanja, izrade, usvajanja, usklađivanja i ažuriranja planova obezbediće se maksimalan stepen povezivanja subjekata sistema odbrane u ostvarivanju i iznalaženju optimalnih rešenja za planirane ciljeve i stvaranje preduslova za efikasno izvršavanje postavljenih zadataka i preuzetih obaveza iz Plana odbrane u ratnom i vanrednom stanju.

Zbog mnogih ranjivosti, direktno i stalno su ugrožena informaciona dobra i primenjene savremene tehnologije, a posredno se pretnja ispoljava i prema korisnicima i čitavom društvu. Iako se pretnja, ostvarivanjem ispoljava kao sajber napad u virtuelnom prostoru, može imati dalekosežne posledice u materijalnom svetu i može ugroziti tradicionalne društvene aktivnosti, u koje spadaju i aktivnosti odbrambenog sistema. Većina savremenih armija, bez obzira na stepen društvenog i ekonomskog razvoja matične zemlje, vojni savezi i organizacije intenzivno su prisutni i svoje aktivnosti u sajber prostoru i dalje povećavaju.

CITIRANA DELA

Pleskonjić, D., Maček, N., Đoršević, B. i Carić, M. (2007). *Sigurnost računarskih sistema i mreža*. Beograd: Mikro knjiga.

Rodić, B, G. Đorđević, Da li ste sigurni da ste bezbedni, monografska publikacija, Produktivnost AD, Beograd, 2004. godina, strana 35-37.

Slavković, R., Kršljanin, D. (2015). Uticaj operativnog okruženja na sajber pretnje. *Vojno delo*, (5). Beograd: Medija centar „Odbrana“.

Stajić, Lj. (2003). *Osnovi bezbednosti*. Beograd: Policijska akademija, str.16.