UDC 519.6:004.42.056 INFO M: str. 41-46

PRIMENA HEŠ FUNKCIJA U CHAP AUTENTIFIKACIJI
A HASH FUNCTIONS APPLICATION IN CHAP AUTHENTICATION PROTOCOL

Slaviša Popravak, Velimir Dedić

REZIME: Ova rad daje pregled primene funkcija sažimanja (heš funkcija) u domenu primenjene kriptografije. Poseban naglasak dat je na primenu heš funkcija u očuvanju autentičnosti poruka, a konkretan primer mogućeg scenarija napada na heš dat je u slučaju korišćenja CHAP autentifikacije. Simulirano je presretanje komunikacije tokom CHAP sesije i metodom napada rečnkom prikazan je uspešan napad. U zaključku je data preporuka za zaštitu od ovakve vrste napada.
KLJUČNE REČI: heš funkcije, CHAP, sigurnost lozinke
ABSTRACT: This paper deals with hash functions application in practical criptography. CHAP protocol was analyzed as an example of using hash. An dictionary-style attack on CHAP authentification session was succesfully simulated. In the conclusion, policy recommendation was given.
KEY WORDS: hash function, CHAP, password security

1. FUNKCIJE SAŽIMANJA (HEŠ FUNKCIJE)

Funkcije sažimanja, ili kako se još nazivaju heš funkcije, su jednosmerne funkcije koje ulazni podatak promenjive dužine pretvaraju u izlazni podatak fiksne dužine. Taj izlazni podatak se naziva „heš" (engl. *hash*). Smatra se da je veoma teško iz datog izlaznog heša dobiti ulazni podatak od koga je nastao dati heš. Najznačajnije heš funkcije koje se koriste ili su se koristile ranije su: MD2, MD4, MD5 koje proizvode heš dužine 128 bita i SHA, RIPEMD koje proizvode heš dužine 160 bita [1].

Postoje brojni neuspešni pokušaji da se pronađu ulazni podaci za neke od najčešće korišćenih heš funkcija, kao što su SHA-1, MD5.

Jednosmernost heš funkcija ogleda se u sledećem:

1) za dati ulazni podatak (p) proizvoljne dužine, heš (h) fiksne dužine lako se određuje;
2) međutim, od heša h fiksne dužine, ulazni podatak p je nemoguće odrediti ili je određivnje neprihvatljivo teško i sporo.

Takođe, neprihvatljivo teško je naći malu izmenu poruke p, a koja ne bi uticala na promenu vrednosti heša h. Isto tako, neprihvatljivo teško je naći dve poruke koje bi dale isti heš. Heš funcija MD5 upravo iz ova dva razloga više nije preporučljiva za digitalne sertifikate [6].

Pored jednosmernosti heš funkcija, druga osobina njihove primene koju treba razmotriti je postojanje kolizije. Kolizija, u primeru heš funkcija, nastaje kada dva različita ulazna podatka proizvedu isti heš, naravno ukoliko se nad njima primenila ista heš funkcija. S obzirom da je svaki heš ograničen i fiksne je dužine, onda je nemoguće da svaki mogući ulazni podatak proizvede jedinstveni heš.

Primera radi, pretpostavimo da postoji heš funkcija koja proizvodi izlazni heš dužine L=3 bita, ovo znači da postoji ukupno 8 različitih heševa. Takođe, pretpostavimo da postoji samo jedan skup ulaznih podataka sačinjan od 5 bitova - ovo znači da postoji 32 različite ulazne datoteke. Ako bi se nad svakim od ulaznih fajlova primenila pomenuta hipotetička heš funkcija, onda bi se dobilo 32 heša, ali bar 4 različite datoteke proizvele bi isti heš. Pokazali smo da bi na taj način došlo do kolizije.

U slučaju praktično primenjenih heš funkcija, npr. MD5 proizvodi heš dužine 128 bita, a SHA-1 proizvodi heš dužine 160 bita, verovatnoća nastanka kolizije je zanemarljivo mala.

Savršena heš funkcija mogla bi da bude ona funkcija koja bi za svaki mogući ulazni podatak proizvela jedinstveni izlazni heš. Međutim, ovo je u praksi nemoguće, osim ako je skup svih mogućih ulaznih podatak unapred poznat i fiksan. U praksi, kada se govori o MD5 i SHA-1 heš funkcijama, ne postoji fiksan broj ulaznih podataka, tako da je postojanje kolizije neizbežno.

Jedna od važnijih podela heš funkcija je na:

1) jednoparametarske - postoji samo jedan ulazni argument za heš funkciju, a to je sama poruka, ulazni podatak
2) dvoparametarske - postoje dva ulazna argumenta za heš funkciju, a to su ulazni podatak i ključ

Jednoparametarske heš funkcije ne obezbeđuju proveru integriteta poruke, jer napadač koji je presreo poruku, izmenio njen sadržaj i prosledio je dalje ka njenom ciljnom primaocu, može da, bez ikakvih problema, izmeni i heš koji putuje sa porukom. Novi heš bi odgovarao izmenjenoj poruci i primalac ne bi mogao da zna da je poruka promenjena na putu od pošiljaoca do njega (osim u slučaju ako je korišćen neki drugi mehanizam za proveru integriteta).

Ako se koriste dvoparametarske heš funkcije, ovakvo nešto bilo bi moguće samo ako napadač zna koji ključ koriste pošiljalac i primalac.

2. NAJČEŠĆE PRIMENE HEŠ FUNKCIJA

Široka je primena heš funkcija u domenu informacionih tehnologija. Neke od tih primena su sledeće: provera autentičnosi poruka (*Messages Authentication Code – MAC*), digitalni sertifikati, čuvanje lozinki na disku, autentifikacija korisnika mrežnih reursa (*Challenge-Handshake Authentication Protocol, CHAP*) i drugo. Ukratko će biti pomenuta svaka od njih,

a detaljnija pažnja će biti posvećenja primeni heš funkcije MD5 u CHAP autentifikaciji. Takođe će biti prikazan i jedan od mogućih napada na CHAP.

2.1. *Messages Authentication Code - MAC*

Messages Authentication Code čini relativno mala količina informacije koja se pridružuje poruci, a služi da se autentifikuje poruka i proveri integritet poruke. Sama primena jednoparametarskih heš funkcija, bez dodatnih mera zaštite, ne može da obezbedi ni autentifikaciju poruke niti proveru integriteta poruke. Ako nije korišćen ključ prilikom kreiranja heša poslate poruke, napadač može da presretne poruku, izmeni njen sadržaj i takođe izmeni originalni heš poruke u heš koji će odgovarati izmenjenoj poruci. Ovo bi se takođe moglo izbeći šifrovanjem i tada napadač ne bi bio u prilici da neopaženo izmeni poruku.

Izraz koji se koristi kada se jednoparametarske (engl. *keyless*) heš funkcije koriste zajedno sa kriptografskim ključem (engl. *keyed*) je HMAC (engl. *Hash-based Authentication Code*). Za izračunavanje HMAC-a mogu se koristiti npr. heš funkcije MD5, SHA-1. Dati MAC algoritmi se nazivaju HMAC-MD5 i HMAC-SHA1. Snaga datog HMAC-a zavisi od više faktora: dužina heša u bitima koji proizvodi korišćenja heš funkcija, jačine date heš funkcije, kao i od dužine i kvaliteta korišćenog kriptografskog ključa.

2.2. *Primena heš funkcija kod digitalnih sertifikata*

Još jedna značajna primena heš funkcija vezana je za digitalne sertifikate. Digitalni sertifikat je dokument koji sadrži podatke o vlasniku sertifikata i njegov pripadajući javni ključ, takođe ih međusobno povezuje digitalnim potpisom. Digitalnim potpisom se overava i potvrđuje veza između identiteta korisnika i javnog ključa. Digitalni sertifikat se sastoji od:

a) javnog ključa
b) informacije o identitetu (ime, identifikator korisnika - UID)
c) podacima o izdavaocu sertifikata, datumu izdavanja i roku važenja
d) serijskog broja sertifikata, algoritma korišćenog za potpisivanje
e) jedinstveno imena izdavaoca i vlasnika sertifikata
f) digitalnog potpisa izdavaoca sertifikata

Međutim, treba znati: ono što se zaista potpisuje jeste heš koji je nastao primenom neke od heš funkcija nad podacima koji se potpisuju. U tu svrhu se, u današnje vreme, koriste MD5 i SHA-1 heš funkcije. U skorije vreme, pošto se MD5 već pokazao kao nedovoljno bezbedan, preporuka je da se koristi SHA-1 ili neki drugi algoritam.

Sledeći primer će još više da ilustruje potrebu za heš funkcijama kod digitalnog potpisivanja poruka. Ako bi neko hteo digitalno da potpiše poruku koja je veličine 10 MB, on bi za to koristio svoj privatni ključ i time obezbedio proveru integriteta poruke i identiteta pošiljaoca. Međutim, problem je što bi digitalni potpis bio veličine kao i sama poruka, odnosno 10 MB, te bi pošiljaoc morao da pošalje 20 MB primaocu, što nije zanemarljivo.

Ovaj problem se rešava korišćenjem heš funkcija i to na sledeći način. Od same poruke, koja je u pomenutom primeru veličine 10 MB formira se heš. Heš će biti dužine 128 bita ili 160 bita, u zavisnosti da li je korišćena MD5 ili SHA-1 funkcija. Zatim će se samo dati heš poruke digitalno potpisati privatnim ključem pošiljaoca. Sama poruka i njen heš će se poslati primaocu (na neki siguran način, što za ovaj primer nije od značaja). Na ovaj način se umesto 10 MB dodatne informacije načinilo nešto više od 128, odnosno 160 bita, a postigla se ista funkcionalnost.

2.3. *Primena heš funkcija za čuvanje lozinki na disku*

Takođe, još jedna od važnijih i čestih primena heš funkcija je za čuvanje lozinki na disku. Korisničke lozinke na diskovima računara ili servera ne čuvaju se u neenkriptovanom, originalnom obliku, jer bi u tom slučaju bilo relativno lako za napadača da dođe do datoteke u kojoj se čuvaju lozinke i na taj način stekne prava bilo kog korisnika datog sistema. Kada korisnik kreira lozinku prvi put ili kada je promeni po svojoj želji ili zato što ga je organizaciona politika na to primorala, kreira se odgovarajući heš date lozinke. Dati heš se čuva na disku zajedno sa korisničkim imenom kojem data lozinka pripada.

Kada korisnik pokuša da se prijavi na dati sistem, on unosi svoje korisničko ime i lozinku. Server od unesene lozinke kreira heš korišćenjem heš funkcije koja se koristila i prilikom čuvanja lozinke na disku. Za uneseno korisničko ime se u bazi korisnika traži odgovarajući heš i dati heš se poredi sa hešom koji je kreiran od stringa koji je korisnik uneo u polje za lozinku. Ako se dva podudaraju onda je korisnik uspešno autentifikovan, odnosno unešena lozinka odgovara korisničkoj lozinci.

Jedan od mogućih napada na korisničke lozinke sačuvane na disku na pomenuti način je da se dati server ponovo pokrene, a sistem podigne sa sistemskog diska. Zatim su moguće dve opcije. Prva je da se baza korisničkih naloga (SAM baza - ako je reč o operativnom sistemu Windows) prekopira na neki prenosivi disk i odnese, pa se onda lozinke dešifruju. Tehnički, radi se o sledećem: korisiti se napad rečnikom (*dictionary attack*) ili napad grubom silom (*brute force attack*) nad ukradenom SAM bazom. Nad rečima iz rečnika ili pseudoslučajno kreiranim stringovima (od dozvoljenih vrsta karaktera u lozinci) primenjuje se heš funkcija, koja je korišćenja prilikom čuvanja lozinki na disk. Dobijeni heševi se porede sa heševima u SAM bazi. Kada dođe do podudaranja, korišćeni string je korisnička lozinka.

Osnovni vid zaštite od ovog tipa napada je fizičko obezbeđenje servera uz korišćenje striktnih organizacionih politika. Drugi vid zaštite je politika korisničkih lozinki (engl. *password policy*). Adekvatna politika korisničkih lozinki će povećati vreme neophodno za dešifrovanje korisničke lozinke, što će usloviti da je data lozinka u momentu kada je napadač otkrio već postala nevažeća, jer sistem primorava korisnika da lozinku menja u redovnim vremenskim intervalima.

Jedna politika korisničkih lozinki mogla bi da definiše sledeća pravila i na taj način poveća bezbednost računarskih sistema u tom aspektu i time spreči pomenuti napad:

a) važnost lozinke 42 dana (administratori 30 dana)
b) minimalna važnost 2 dana
c) sistem pamti poslednje korisnikove 24 lozinke i ne dozvoljava mu da ih ponovo koristi
d) složenost lozinke - da bude sačinjena od sledećih skupova karaktera:
e) velika slova (A - Z)
f) mala slova (a - z)
g) brojevi (1 - 9)
h) specijalni znaci (!, #, $, %)

Drugi tip napada podrazumeva korišćenje nekog od alata koji će nasilno da promeni korisničku lozinku i pripadajući heš (Linux live cd - Knoppix, L.A.S i drugi sadrže ovakve alate). Jedan od alata koji može da se koristi u ove svrhe je program poznat kao *chntpw.* Pomenuti program „prebriše" postojeću loziku i postavi novu. Međutim, problem kod ovog tipa napada na korisničke lozinke (problem za napadača) je taj što je korisničku lozinku promenio, pa će to dati korisnik pre ili kasnije da primeti. Ovo nije slučaj sa prvim tipom napada, jer u tom napadu napadač otkriva korisničku lozinku i može da je koristi kao što je koristi i dati korisnik, a da ovaj to ne primeti.

2.4. *Primena heš funkcija kod CHAP autentifikacije*

Još jedna od primena heš funkcija je u CHAP protokolu za autentifikaciju na PPP vezama (*point-to-point protocol*). Autentifikacija na PPP vezama nije obavezna, već opciona. Ukoliko se implementira, jedna od alternativa je korišćenje CHAP-a. Naravno, niti je CHAP autentifikacija jedina opcija za autentifikaciju na PPP vezama, niti je ovo jedina primena CHAP-a. CHAP se još može korisiti i za PPTP, PPPoE, dot.1x i dr.

3. PRIMENA MD5 HEŠ FUNKCIJE U CHAP AUTENTIFIKACIJI

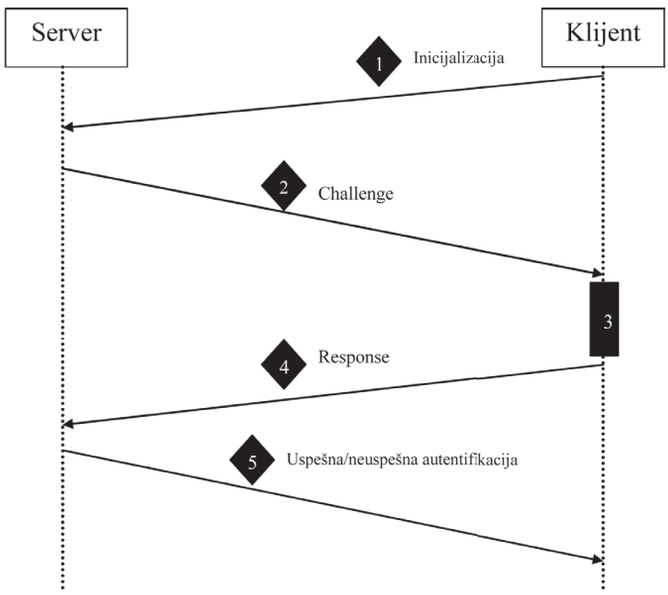
CHAP autentifikuje korisnika ili uređaj metodom *Three-Way Handshake*. Koraci u autentifikaciji su sledeći:

1. Autentifikator šalje signal *challenge* klijentu
2. Klijent, na osnovu signala *challenge*, ID-a i lozinke računa MD5 heš i šalje ga autentifikatoru
3. Autentifikator na osnovu istih parametara računa svoj MD5 heš i poredi ga sa MD5 hešom koji je dobio od klijenta. Ukoliko su heševi identični, autentifikacija je uspešna i klijent je dokazao svoj identitet.

Autentifikacija je zasnovana na lozinci koju znaju obe strane koje učestvuju u autentifikaciji, i kao što će biti kasnije pokazano, od odabira lozinke zavisi i nivo bezbednosti ovakve autentifikacije.

3.1. *Napad na CHAP*

Na Slici 1 ilustrovana je CHAP autentifikacija. Koraci u procesu autentifikacije, prikazani između klijenta (koji želi da bude autentifikovan) i servera (koji vrši autentifikaciju) naznačeni su rednim brojevima sekvenci.



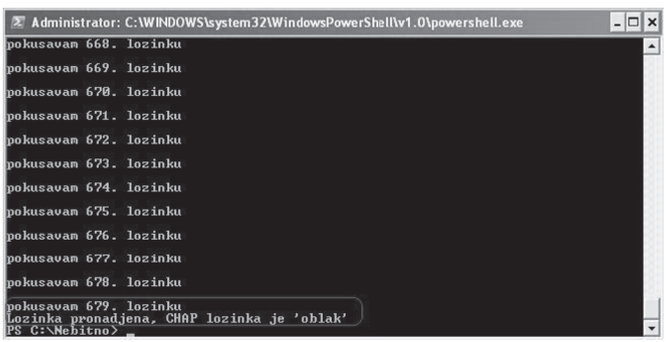
Slika 1. – *CHAP autentifikacija*

Sa Slike 1 vidimo korake u procesu autentifikacije, koji se mogu sistematizovati kao sledeće vremenski poređane sekvence (1 do 5):

1. Klijent inicira autentifikaciju
2. Server šalje klijentu signal CHAP *challenge*, koji sadrži sledeće parametre:
   a) Identifikator tipa paketa – ovde je to "*challenge*"
   b) ID - identifikator *challengea*
   c) Slučajni broj
   d) Ime autentifikatora (ID i slučajni broj autentifikator čuva i lokalno)
3. Klijent kada dobije Challenge čini sledeće korake:
   1. Sažima u jedan string: ID, lozinku i slučajni broj - navedenim redosledom
   2. Nad time računa MD5
4. Zatim klijent serveru šalje CHAP odgovor koji sadrži sledeće:
   a) Identifikator tipa paketa – ovde je "*response*"
   b) ID - prekopiran iz challenge paketa
   c) MD5 heš (izračunat u prethodnom koraku)
5. Server, nakon što dobije CHAP odgovor od klijenta, čini sledeće:
   1. Na osnovu ID - a, pronalazi slučajni broj koji je poslao datom klijentu
   2. Sažima u jedan string: ID, lozinku i slučajan broj
   3. Nad time računa MD5
   4. Izračunati MD5 poredi sa MD5 hešom koji je dobio od klijenta i ukoliko su identični autentifikacija je uspešna

Ono što se, iz prethodnog opisa, može primetiti je da lozinka nije poslata mrežom prilikom autentifikacije. Ono što je mrežom prolazilo je CHAP *challenge*, slučajni broj , ID i CHAP *response*. To je saobraćaj koji neko, prisluškivanjem mreže, može da uhvati.

Iz demonstracionih razloga podešeni su Microsoftov PPTP server i klijent za CHAP autentifikaciju između njih. Na ovaj način omogućena je simulacija prisluškivanja saobraćaja između servera i klijenta tokom autentifikacije. Ostalo je da se pokuša sa napadom na lozinku. Za tu potrebu kreirana je skriptu u Powershellu, koja metodom napada na rečnik otkriva lozinku. Izvorni kod skripte svojim obimom ne dozvoljava da bude prikazan u celini u ovom radu. Slika 2 ilustruje uspešan završetak napada i pronađenu lozinku u 679. pokušaju.



Slika 2. – *CHAP lozinka pronađena*

Da bismo potvrdili ispravnost rada pomenute skripte, pretvorena je dobijena lozinka "oblak" u heksadecimalni oblik. Zatim su sažeti ID, lozinka(oblak) i slučajni broj nad stringom je izračunat MD5 heš

Dati rezultat se u potpunosti podudaraju sa parametrima koji su presretnuti

4. ZAKLJUČAK

Cilj ovog rada je bio da se opišu funkcije sažimanja, pomenu i opišu neke od njihovih primena u praksi. Veća pažnja u radu je posvećena primeni MD5 funkcije u CHAP autentifikaciji. Prikazan je mogući scenaro napada na CHAP.

Pomenuta powershell skripta izvodi napad rečnikom i biće uspešan samo ukoliko je za lozinku uzeta reč iz rečnika. Ukoliko, za lozinku, nije korišćena reč iz rečnika, napad e biti neuspešan. Međutim, skripta bi se mogla koristiti i za napad grubom silom. Tada bi se umesto rečnika, prethodno napravila datoteka koja bi sadržala sve moguće kombinacije karaktera, koji su dozvoljeni za lozinku, definisane minimalne i maksimalne dužine. Ta datoteka bi se onda ponudila kao izvor potencijalnih lozinki.

Kada je reč o zaštiti od pomenutog tipa napada, onda bi odabir složene lozinke znatno otežalao napad. Ako je reč o CHAP autentifikacija između dva rutera, onda se lozinka unosi samo jednom (prilikom konfiguracije). U tom slučaju ne bi bilo komplikovano uneti veoma složenu i dugačku lozinku, zato što ona ne mora da se zapamti i unosi svaki put kada se želi ostvariti konekcija.

LITERATURA

[1] Bishop M.: „Computer Security: Art and Science", Addison Wesley, 2003
[2] Pleskonjić D., Maček N., Đorđević B., Carić M.:„Sigurnost računarskih sistema i mreža"; Mikro knjiga, Beograd, 2007.
[3] „RFC1994 - PPP Challenge Handshake Authentication Protocol (CHAP)" W.Simpson, 1996
[4] Sotirov A., Stevens M., Appelbaum J., Lenstra A., Molnar D.: „MD5 considered harmfull today - creating a rogue CA certificate", veb izvor http://www.win.tue.nl/hashclash/rogue-ca/, aktuelno 1.2.2010.
[5] Wang X., Yu H.: "How to Break MD5 and Other Hash Functions" In: Ronald Cramer (editor), "Advances in Cryptology - EUROCRYPT 2005", volume 3494 of Lecture Notes in Computer Science, pages 19-35,Springer Verlag, Berlin, 2005.
[6] http://www.win.tue.nl/hashclash/rogue-ca/. aktuelno 1.2.2010.

Slaviša Popravak, dipl. ing, Mercator-s doo, Novi Sad
Kontakt: slavisa.popravak@mercator.rs
Oblasti interesovanja: zaštita računarskih mreža i sistema, mrežna infrastruktura, računarske mreže

Doc. dr Velimir Dedić, Visoka škola za informacione tehnologije, Zemun, Tehnički fakultet Čačak
Kontakt: velimir.dedic@its.edu.rs
Oblasti interesovanja: informacioni sistemi, adaptivno e-učenje, medicinska informatika i statistika

ZITEH 10 – ZAKLJUČCI SA SAVETOVANJA
održanog 5. i 6. marta 2010. godine u Beogradu

Treće naučno-stručno Savetovanje o Zloupotrebi informacionih tehnologija i zaštiti – ZITEH, pod pokroviteljstvom Ministarstva za telekomunikacije i informaciono društvo, u organizaciji Udruženja IT Veštak i Instituta za poslovna istraživanja, Univerziteta Singidunum, i u suorganizaciji sa Privrednom komorom Beograda i Privrednom komorom Srbije, održano je u Beogradu 5. i 6. marta 2010. godine.

Cilj Savetovanja je da ukaže na rapidno širenje i upotrebu savremenih informaciono - komunikacionih tehnologija (IKT) u svim sferama života i njihovu masovnu zloupotrebu na lokalnom, regionalnom, nacionalnom i globalnom nivou. Ta činjenica nameće imperativnu i urgentnu potrebu adekvatnog odgovora na ovaj izazov, jer pasivnost i zakasnelo reagovanje za posledicu može imati vrlo ozbiljne problema sa dalekosežnim posledicama.

Skupu su prisustvovali i prezentovali radove predstavnici vojske, policije, tužilaštva, pravosuđa, Srpske Pravoslavne crkve, akademskih institucija, privrednih komora Srbije i Beograda, informatičkog sektora i privrede iz Srbije i Republike Srpske. Na Savetovanju su prezentovana 34 naučno-stručna rada, koji pokrivaju sve aspekte tematike skupa, a koji su publikovani u CD zborniku "ZITEH 10", registrovanom u Narodnoj biblioteci Srbije (ISBN 978-86-90951111-6 COBISS.SR-ID 173688076). Zlatni sponzori Savetovanja su MFC Mikrokomerc i Kompanija Dunav osiguranje, a prijatelji ZITEH-a: Informatika AD, Microsoft, 3D Caddit d.o.o. i Division multimedia.

Polazeći od potrebe pravovremenog i sveobuhvatnog sagledavanja prepoznatih problema, učesnici skupa, u cilju iniciranja neophodnih mera i akcija u institucijama sistema, jednoglasno su usvojili sledeće zaključke:

1. U informacionom društvu kritični resurs postaje znanje, a ključne funkcije postaju produkcija i distribucija znanja. Da bi borba protiv zloupotrebe IKT bila uspešna moraju se permanentno razvijati bezbednosna kultura, podizati svest o potrebi zaštite informacionog prostora i generisati, objedinjavati i širiti znanja i veštine koji bi bili u funkciji sprečavanja, otkrivanja, dokazivanja i sankcionisanja svih vidova zloupotreba.

2. Za uspešno suzbijanje transnacionalnog fenomena zloupotrebe IKT učesnici smatraju da prvi korak mora da bude pokretanje inicijative za HITNU izradu NACIONALNE STRATEGIJE ZAŠTITE KIBER-PROSTORA, kao najvažnijeg i najsnažnijeg pokretačkog i usmeravačkog instrumenta za sve ostale aktivnosti i akcije. Nosilac ove ključne inicijative bi morala da bude VLADA Republike Srbije, kao državni entitet najodgovorniji za opšte stanje u naciji, koja istovremeno predstavlja najviši autoritet i ima najveći kapacitet neophodan za realizaciju takvog značajnog projekta. Donosioci odluka i odgovorni za stanje u ovoj oblasti treba da shvate da se informaciona bezbednost bez Nacionalne strategije svodi na običnu improvizaciju, koja samo prikriva postojeće probleme.

3. Paralelno sa inicijativom za izradu Strategije treba pokrenuti široku akciju bezbednosnog obrazovanja u školama, posebno osnovnim, na fakultetima i akademijama u cilju podizanja na znatno viši nivo opšte INFORMATIČKE BEZBEDNOSNE KULTURE mladih i SVESTI o potrebi ZAŠTITE informacionog prostora. Permanentno, sistemtično informatčko obrazovanje je jedini pravi način da se u društvu generišu kritična masa SVESTI i ZNANJA, koja bi garantovala da će se preventivnim i proaktivnim delovanjem zloupotreba IKT dugoročno držati pod kontrolom. Učesnici Savetovanja su duboko ubeđeni da bi ovo, dugoročno gledano, bila jedna od najkorisnijih i najisplativijih NACIONALNIH INVESTICIJA u razvoj informacionog društva.

4. Neophodna je institucionalna podrška u donošenju zakonske regulative, čijim bi odredbama ova kompleksna oblast bila pravno uređena.

5. Učesnici Savetovanja posebno insistiraju na izradi, donošenju i primeni nedostajućih nacionalnih standarda važnih za ovu oblast, harmonizovanih sa evropskim i međunarodnim standardima.

6. Poznavanje problematike sve šire zloupotrebe IKT, u sve većoj meri postaje DEO OPŠTE KULTURE našeg društva, a za državnu upravu, vojsku, policiju, sudstvo i tužilaštvo, i deo PROFESIONALNIH OBAVEZA. Zbog toga je za ove kategorije veoma bitno obezbediti ROBUSNU edukaciju iz ove oblasti, kako bi svoje funkcije i u novom ambijentu mogli uspešno i profesionalno obavljati.

7. Učesnici Savetovanja predlažu da:

a. Udruženje IT Veštak identifikuje sva potencijalna znanja i veštine sa kojima raspolažu njegovi članovi, kvantifikuje vrednost gubitaka koje organizacije i pojedinci mogu imati od zloupotreba IKT i podatke dostave svim institucijama i organizacijama, pozvanim na Savetovanje.

b. Svi učesnici Savetovanja, preko Udruženja IT Veštak, svojim kritičkim primedbama i sugestijama uzmu učešće u procesu javne rasprave na Predlog zakona o zaštiti informacija u IKT sistemima.

c. Udruženje IT Veštak u saradnji sa PK Beograda i PK Srbije organizuje okrugli sto za stručnu raspravu o terminologiji u oblasti zloupotreba IKT i zaštite.

d. Udruženje pripremi i ponudi Ministarstvu prosvete material (prezentaciju) za predavanja u trajanju od 2 školska časa za osnovne škole na temu opasnosti od zloupotreba IKT i zaštite.

e. Udruženje, kroz različite forme, preko medija, foruma i okruglih stolova neprekidno vrši pritisak i insistira na pro-aktivnim merama državnih i nevladinih organizacija u oblasti zaštite i borbe protiv zloupotreba IKT.

Beograd, 6.03.2010. god

CIP - Katalogizacija u publikaciji Народна библиотека Србије, Београд 659.25
INFO M: časopis za informacionu tehnologiju i multimedijalne sisteme = journal of information technology and multimedia systems
glavni i odgovorni urednik Dragana Bečejski Vujaklija. . - . –
Beograd : Fakultet organizacionih nauka,
2002- (Stara Pazova : SAVPO). - 30 cm
- Tromesečno ISSN 1451-4397 COBISS.SR-ID 105690636