AGENCIJA ZA INFORMACIONO DRUŠTVO REPUBLIKE SRPSKE

Odjeljenje za informacionu bezbjednost

oib.aidrs.org

Terminologija informacione bezbjednosti

Stojan Radanović

Oznaka dokumenta	OIBRS-PUB-E1-02
Urednik izdanja	mr Srđan Rajčević [srdjan.rajcevic@aidrs.org]
Autor	Stojan Radanović [stojan.radanovic@aidrs.org]
Datum izdavanja	3.6.2015.
Lokacija objave	https://oib.aidrs.org

SADRŽAJ

1. Uvod

Činjenica je da informacione tehnologije danas predstavljaju sastavni dio gotovo svake ljudske aktivnosti. U mnogome nam olakšavaju i ubrzavaju posao, pristup sadržajima koji nas interesuju i obezbjeđuju komunikaciju sa okruženejm bez obzira na udaljenost. Može se reći da danas mnoge stvari, koje su nam omogućile informacione tehnologije, uzimamo zdravo za gotovo. Jednostavno, one se podrazumjevaju.

Jedna od pretpostavki za potpuno prihvatanje informacionih tehnologija kako u privatnom tako i u poslovnom životu, a koja se podrazumijeva, jeste informaciona bezbjednost. Možda najbolji pokazatelj koliko je bezbjednost u smislu informacionih tehnologija značajna, jeste i postojanje zakonske i podzakonske regulative. U Republici Srpskoj to je Zakon o informacionoj bezbjednosti Republike Srpske kao i Pravilnik o standardima informacione bezbjednosti i Uredba o mjerama informacione bezbjednosti

Prema Zakonu o informacionoj bezbjednosti Republike Srpske (Službeni glasnik Republike Srpske", br. 70/11), termin **informaciona bezbjednost** odnosi se na stanje povjerljivosti, cjelovitosti i dostupnosti podataka.

Kako u teoriji, tako i u praksi, termin informaciona bezbjednost je jako širok pojam koji između ostalog obuhvata programe, opremu, procedure i naravno obučen kadar koji je zadužen za ispravno funkcionisanje samog sistema.

2. Poznavanje tematike

Brošura koju čitate je nastala prije svega iz potrebe da se korisnici upoznaju sa tematikom informacione bezbjednosti, te da kroz upoznavanje sa terminologijom koja se koristi u ovoj oblasti i njenim pojašnjenjem, steknu širu sliku o problemima koji se mogu javiti.

Svakodnevno se mogu čuti razni termini koji su u manjoj ili većoj mjeri poznati građanima. U pitanju su termini poput Backdoor-a, Bug-a, Firewall-a, Malware-a, Trojnaca ili Virusa, koji se najčešće pominju u kontekstu nastale štete, kako po fizička tako i pravna lica.

Šteta se najčešće ogleda u korumpiranim ili izgubljenim podacima kao i u nemogućnosti korištenja servisa. Jedna od posljedica može biti i „curenje" podataka kako iz malih ali i velikih sistema koji bar u jednom momentu nemaju adekvatnu zaštitu podataka.

Kao primjer pomenućemo multimedijalni gigant Sony, koji je imao velikih problema na polju zaštite svojih sistema i servisa što je rezultovalo objelodanjivanjem osjetljivih informacija i kao i nemogućnosti korištenja Sony-jevih servisa.

Shodno prethodno rečenom u daljem tekstu pojasnićemo neke pojmove i termine koji se tiču **informacione bezbjednosti**.

3. Predmetna terminologija

U ovom dijelu nastojaćemo da Vam predstavimo većinu termina i fraza koje su karakteristične za informacione tehnologije, a koje se koriste i na polju informacione bezbjednosti. Istina jeste i da se sa pojavom neke nove tehnologije vezane za ovu tematiku pojavljuju i novi termini, a samim tim i skraćenice tj. akronimi koji uglavnom, nedovoljno upućenima, prouzrokuju zabunu.

U ovom dijelu ćemo pojasniti neke od pojmova koji bi trebali da rezultuju boljom upućenosti u problematiku informacione bezbjednosti.

3.1.Termini i pojmovi

Zbog jednostavnijeg pronalaženja termini i pojmovi koji slijede su poredani abecedno radi lakšeg pronalaženja.

Access control – Kontrola pristupa, je vrsta mehanizma koja određuje ko ima pravo pristupa nekom sistemu, a ko ne. Postoje dvije osnovne vrste kotrole pristupa, fizička i logička. Fizička se odnosi na pravo pristupa nekoj zgradi, prostoriji ili samoj IT opremi, dok se logička odnosi na pravo pristupa informacijama kao i servisima koji se mogu koristiti za bilo koji vid manipulacije istim.

Access Point (AP) – Pristupna tačka, je pojam koji se uglavnom koristi u bežičnim kmunikacijama. Obično predstavlja uređaj bilo da je zaseban ili kao dio drugog uređaja (npr. računara) koji omogućava klijentu (korisniku) da se poveže na lokalnu mrežu ili internet. Komunikacija s bežičnim pristupnim tačkama odvija se prema IEEE 802.11 standardima.

Anti-virus – Anti-virus, je sigurnosni program koji se pokreće na računaru ili mobilnom uređaju koji štiti uređaj tj. podatke identifikujući i sprečavajući širenje malicioznih programa na sistemu. Anti-virus ne može da identifikuje baš sve maliciozne programe, tako da je moguće, iako je anti-virus aktivan, da postoji neki malware unutar sistema. Anti-virus može da se koristi na nekom od organizacionih nivoa, kao što su e-mail serveri gdje pregledaju prijemnu i odlaznu poštu. Ponekad se anti-virus naziva i antimalware jer je dizajniran da štiti od različitih oblika malicioznih programa.

Backdoor – Tajni ulaz, predstavlja metod prikrivenog pristupa kompjuterskim sistemima. Može biti riječ o sistemskoj grešci koju je moguće eksploatisati, bez obzira da li su namjere maliciozne ili ne. Moguće je da se radi i o programu koji je postavljen sa ciljem neautorizovanog pristupa. Čak i standardne lozinke koje se uobičajeno daju korisnicimna, a koje se ne promijene blagovremeno mogu prestavljati vid **Backdoor**-a.

Backup – Sigurnosna kopija, predstavlja periodičnu izradu kopija dokumenata i programa zatečenih u momentu izrade kopije. Postoje dvije vrste backup-a. Full backup (kompletna kopija) koji obuhvata cjelokupan sadržaj izvora koji se kopira ili Incremental backup (parcijlana kopija) koji obuhvata samo izmjene koje su nastale od momenta kreiranja zadnje kopije.

Botnet – Mreža robota, ovaj termin se odnosi na veći broj računara koji su, bez znanja vlasnika ili korisnika računara, pod kontrolom drugih lica u svrhu ispunjavanja zadataka određenih od tih istih lica. Obično se koriste u svrhu spamovanja ili za DoS napade na sisteme ustanova ili servise kako bi se onemogućio njihov normalan rad tj. pružanje određene usluge. Računar korisnika dospijeva u botnet najčešće zbog sigurnosnih propusta u programima koji se koriste na računaru (web browser-i ili neki drugi programi). Maliciozni program najčešće ostaje prikriven kao regularan servis do momenta aktiviranja od strane vlasnika programa. Postoje legalni i ilegalni botnet-i.

Bug – greška, u IT terminologiji odnosi se na manju grešku u kodu programa koja se manifestuje nelogičnim ponašanjem datog programa ili jednog njegovog dijela. Iako obično bezezleni, mogu da dovedu do problema u smislu nemogućnosti izvršenja neke od funkcija programa ali i slabljenja sigurnosnih karakteristika samih programa čiji su sastavni dio, te njihove zloupotrebe.

Computer Emergency Response Team (CERT) - Odjeljenje za informacionu bezbjednost, vrši koordinaciju prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih pravnih i fizičkih lica. Obično je zaduženo za:

- rad na spriječavanju prijetnji po bezbjednost informacija u elektronskom obliku,
- razvoj kriterijuma, procedura i alata za testiranje i evaluaciju bezbjednosti informacionih sistema i njegovih komponenti i testiranje informacionih sistema.
- pružanje podrške i saradnja sa relevantnim organima i institucijama u oblasti suzbijanja sajber kriminala i
- davanje, tj izdavanje upozorenja za ciljnu grupu ili javnost o ranjivostima IT proizvoda i usluga kao i pojavi malicioznog softvera te preporučenim mjerama zaštite pri korišćenju određenih proizvoda a sve u cilju edukacije najšire javnosti i unapređenju svijesti o značaju informacione bezbjednosti

Cryptography – Kriptografija, predstavlja naučnu disciplinu koja proučava metode sigurne komunikacije u slučaju kad posotoji mogućnost presretanja poruke od strane mogućih protivnika. Uopšteno rečeno, radi se o kreiranju i analiziranju protokola koji onemogućavaju protivnika da se domogne sadržaja poruke.

DoS (Denial-of-service) – onemogućenost pristupa ili usluge, predstavlja vrstu napada koji ima za cilj, kako mu i samo ime govori, da se oneogući pristup odgovarajućim servisima i uslugama ili da se prolongiraju vremenski kritične operacije i na taj način nanese šteta licu ili organizaciji.

Debuging – otklanjanje greške, riješavanje problema koji su nastali kao posljedica greške u kodu programa.

Encryption – Enkripcija, proces šifrovanja poruka na način da samo određena osoba (ili oosbe) može da je pročita. Enkripcija sama po sebi ne gatrantuje, da poruka neće biti presretnuta, ali enkripcija ne dozvoljava, u ovom slučaju presretaču, pristup sadržaju poruke. Za potrebe enkripcije se koriste određeni algoritmi koji poruku pretvaraju u nečitljiv oblik, čime postaje neupotrebljivaza za lica koaj nemaju pristup algoritmima koji su korišteni za njeno šifriranje.

Firewall – Zaštitni zid, predstavlja logički ili fizički prekid u mreži kako bi se onemogućio pristup računarima ili mreži od strane potencijalnih napadača. Zadatak mu je da na osnovu unaprijed zadatih pravila kontroliše mrežni saobraćaj između sigurne mreže (obično vlastita) i potencijalno nesigurne mreže. Lični računari mogu da imaju u okviru operativnog sistema implementiran firewall kako bi zaštili korisnika, tj sadržaj računara.

Flooding – plavljenje, vrsta napada koja ima za cilj da izazove prestanak rada računara ili nekog drugog sistema za obradu podataka na način da ga „zatrpa“ sa prevelikom količinom ulaznih podataka nego što sistem može da primi ili obradi.

Hacker – haker, osoba koja ima adekvatan nivo poznavanja programskih jezika i funkcionisanja računara i računarskih sistema, koje koristi za neovlašten pristup računarima i njihovom sadržaju. Najčešće koriste svoje znanje za pisanje i implementiranje malicioznog koda u računarske sisteme sa ciljem zloupotrebe sadržaja. Najčešće su u pitanju prodaja podataka trećoj strani, ali i ucjena. Često se dešava da kompanije angažuju osobe sličnim kvalifikacijama sa ciljem procjene sigurnosti sistema unutar same kompanije.

Hoax – Prevara, najčešće se radi o lažnim upozorenjima koja uimaju za cilj da ubijede korisnika da preuzme neki program kako bi zaštitio svoj računar od virusa ili nekog drugog oblika

malicioznog programa. Ukoliko korisnik povjeruje, lako se može desiti da baš taj program bude maliciozan.

Malware – Maliciozni program, predstavlja bilo koji oblik programa koji ima za cilj da dovede do poremećaju u radu računara i računarskih sistema, prikupi osjetljive ili lične infofrmacije ili da omogući nedozvoljen pristup računarima. Ovdje se radi isključivo o programima koji imaju namjeru da nanaesu štetu, a ne o programina koji usljed određenih nedostataka mogu da prouzrokuju problem. Malware-i su najčešće „nevidljivi“, a cilj je obično špijunaža korisnika, krađa podataka, sabotaža ili čak i ucjena zarad iznuđivanja novca. U malware se ubrajaju: virusi, crvi, trojanci i spajveri.

Password – Lozinka, riječ ili kombinacija znakova kreirana sa ciljem omogućavanja pristupa računarima, dokumentima, ili određenim servisima. Predstavlja vid identifikacije korisnika kojem omogućava prava pristupa pomenutim kategorijama. Treba da bude poznata samo osobi kojoj se dozvoljava pristup. U pojedinim slučajevima, mada se to posebno definiše, postoje lozinke koje se čuvaju na sigurnim lokacijama i koje se mogu koristiti u posebnim situacijama (koje su strikno definisane) kada osoba koja je vlasnik te lozinke nije prisutna.

Patch – zakrpa, jeste nadogradnja ranjivog programa ili sistema. Uobičajena je praksa da se računari i računarski sistemi drže zaštićenim putem pravovremene nadogradnje problematičnih programa. Mnogi proizvođači programa objavljuju nadogradnje svojih proizvoda polugodišnje,kvartalnopa čak i mjesečno. Stoga je u cilju zaštite, potrebno konstantno nadograđivati programe, ali i koristiti nove verzije tih programa jer sa svakom novom iteracijom ti programi postaju sve sigurniji i sposobniji u smilsu mogućnosti primjene i količine i kvaliteta opcija koje su implementirane.

Phising - Phishing (izgovara se kao riječ fishing), predstavlja način prevare korisnika računara u cilju otkrivanja ličnih ili finansijskih informacija putem lažne e-poruke ili Web lokacije. Uobičajena phishing prevara na mreži počinje e-porukom koja izgleda kao zvanično obavještenje iz pouzdanog izvora, kao što je banka, preduzeće koje se bavi kreditnim karticama ili ugledni prodavac na mreži. Primaoce e-poruka upućuje na lažnu Web lokaciju gdje se od njih zahtjeva da unesu lične podatke, kao što su broj računa ili lozinka. Ove informacije se nakon toga obično koriste za krađu identiteta.

Spear Phishing – sličan prethodno pomenutom. U odnosu na obični razlikuje se u taktici. Dok se kod običnog phishinga poruke šalju na veliki broj adresa, u ovom slučaju poruke se šalju tačno određenoj ciljnoj grupi. Obično unutar jedne organizacije. Zbog same prirode napada teže ga je otkriti, a i vjerovatnoća da će primaoc poruke biti prevaren je veća.

RAT (Remote Access Trojans) – Trojanci sa daljinskim pristupom, su maliciozni programi koji u sebi sadrže **Backdoor** za adminstrativnu kontrolu nad ciljanim računarom. Obično ih sam korisnik preuzme bilo kao dio nekog drugog programa (npr. igrica) ili budu primljeni kao prilog elektronskoj pošti. Jednom kad se pokrene i dozvoli pristup napadaču može se koristiti za slanje istog programa na druge nezaštićene računare kreirajući **Botnet**.

Sniffing – njuškanje, predstavlja jedan od naječešće korištenih načina krađe podataka. Radi se o praćenju i snimanju sadržaja koji putujuju između dvije tačke u komunikacionom sistemu. Može da bude lokalni kad se presreću podaci upućeni valstitom računaru ili daljinski kad se presreću podaci upućeni nekom drugom računaru na mreži. Često se koristi od strane samih administratora mreže u smislu praćenja iskorištenosti i upotrebe mrežnih resursa, ali i od potencijalih napadača kao uvod i pripema za napad koji obično rezultuje negativnim posljedicama.

Spam – Spam (junk email, smeće), je termin koji se koristi za neželjene ili korisniku nebitne poruke elektronske pošte. Šalju se na pojedinačne adrese korisnika, najčeće sa linkovima na sajtove sa reklamama ili u gorem slučaju **Phishing** sajtove ili sajtove sa **Malware**-om. Problem spam-ova je moguće riješti putem filtriranja elektronske pošte na mail serverima.

Spyware - je program koji će od vas pokupiti lične informacije, a da pri tome ne znate šta on radi i da vam nije postavljeno pitanje da li se slažete sa time. Informacije se mogu kretati od podataka o sajtovima koje posećujete do osetljivih informacija kao što su korisničko ime i lozinka. Spyware se najlakše širi preuzimanjem (*download*-om) programa koji su predstavljeni kao besplatni.

Spoofing – lažno predstavljanje, je pokušaj lažnog predstavljanja jednog korisnika kao nekog drugog. U tom slučaju, ako je pokušaj spoofing-a uspiješan mogu nastati veliki problemi jer prevareni korisnik ima utisak da komunicira sa osobom od povjerenja, te može dozvoliti pristup osjetljivim informacijama ili ih proslijediti, čija zloupotreba može dovesti do velike štete, kako po samog korisnika tako i po organizaciju ili kompaniju. Najčešće vrste spoofing-a su e-mail spoofing, IP spoofing (internet protocol spoofing) i URL spoofing.

Trojan – Trojanac, predstavlja tip malware-a koji je na prvi pogled legitiman, u smislu da se na uređaju nalazi iz opravdanih razloga i obavlja korisnu funkciju. Za razliku od virusa nema potrebu da se dalje širi i umnožava. U suštini on maskira malicioznu funkciju koja se obično odnosi na umanjenje sigurnosti sistema uređaja na kome je instaliran. Najčešće se to postiže postojanjem bacdoor-a. Shodno tome, trojanac omogućava neovlašten pristup računaru i njegovu zloupotrebu ili zloupotrebu podataka pa čak i brisanje istih.

Virus - Virus, je vrsta malicoznog programa koji može sam da se umnožava i da pri tom čini štetne radnje (korumpira podatke ili ih briše), ali i ne mora. Najčešće se distribuiše putem interneta, lokalnih mreža ili preko medija za prenos podataka kao što su USB prenosna memorija ili CD-ovi. Nepostojanje antivirusnih programa kao i nemar korisnika u velikoj mjeri povećava mogućnost da se računar bude zaražen sa virusom.

VPN (Virtual Private Network) – Virtuelna privatna mreža, predstavlja virtuelnu mrežu koja se bazira na već postojećoj mreži, i predstavlja proširenje privatne mreže putem iste ili neke druge javne ili dijeljene mreže. U pitanju je point-to-point konekcija koja omogućava sigurnu razmjenu podataka koristeći protokole kao što je IPSec.

Vulnerability – ranjivost (slabost), predstavlja bilo koju slabost koju napadači ili njihovi malware-i mogu biti u stanju da iskoriste. Primjera radi, to može biti bug u programu ili nepravilno konfigurisan web server. Napadač ili malware može da iskoristi tu slabost sa ciljem neovlaštenog pristupa sistemu. Mada je ponekad slabost i u samim procedurama unutar sistema ili u samim ljudima, najčešće u smislu neadekvatne obučenosti.

Worm – Crv, je vrsta malware-a koji je programiran za širenje od računara do računara preko interneta ili bilo koje druge mreže. Dizajniran je kao samostalan program i kao takav nema potrebu da se kači za odgovarajuće programe. Ukoliko računari, koji su povezani na mrežu, nemaju odgovarajuću zaštitu, worm može da dospije do njih. Generalno, ovaj tip malwera nije dizajniran da oštećuje ili modifikuje podatke na računaru za razliku od virusa kojima je to najčešće namjena.

4. Zaključak

U prethodnom poglavlju su pobrojani i opisani samo neki od termina koji se odnose na tematiku informacione bezbjednosti. Mahom radi se treminologiji koja se odnosi na same probleme koji mogu da se pojave kao i na intrumente koji ih prouzrokuju.

Problemi su brojni počev od usporavanja rada računara i zagušenja mreže pa do potpunog gubitka podataka koji se nalaze na računaru. Moguće je i činjenje radnji koje predstavljau krivično djelo. Varijante su zaista brojne i ni u kom slučaju nisu dobrodošle.

Što se tiče instrumenata koji uzrokuju pomenute probleme. Oni se najčešće svode na jedan pojam. A to je malware. Bilo da su u pitanju crvi, virusi, trojanci ili spajveri, posljedice uvijek postoje. Pitanje procedura kao i ljudskog faktora je podjednako značajno.

Bitno je razumjeti sljedeće. Primjenom odgovarajućih sigurnosnih alata, prije svega programa za detekciju i sprečavanje bilo kojeg vida malware-a, kako i obukom korisnika i

uspostavljenjem odgovarajućih procedura, rizik od kompromitovanja je minimalan. Samim tim i moguće štete su svedene na minimum.

5. Reference

- www.sans.org/security-resources/glossary-of-terms/,
- www.nist.gov ; Glossary of Key Information Security Terms,
- http://www.securingthehuman.org/resources/security-terms,
- www.wikipedia.org