**Nacionalni CERT**
**Republike Srbije**

# SRB-CERT

REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA
ELEKTRONSKE KOMUNIKACIJE
I POŠTANSKE USLUGE

# 01 Uvod

Pojam informaciona bezbednost je sve prisutniji u celokupnom društvu, kako u svetu, tako i kod nas. Svedoci smo činjenice da je doskorašnji način korišćenja Interneta, pretežno u cilju zabave, prestao da postoji. Danas je Internet sastavni deo svakodnevnog života, bilo da ga koristimo u privatne ili poslovne svrhe. Samim tim, već više od dve decenije, Internet sa sobom nosi i određene opasnosti, ne samo na nivou pojedinca, već i na nivou društva. Sve su učestaliji primeri napada na informacionu infrastrukturu državnih institucija, finansijskih grupacija, kompanija različitih profila, akademskih udruženja, ali i računara koje koristimo u svojim domovima.

U tekstu koji sledi, Nacionalni CERT Republike Srbije će pokušati da približi korisnicima računara i mobilnih uređaja svoja iskustva i znanja u vezi sa sigurnijim i bezbednijim korišćenjem Interneta

Veoma je važno na koji način se koriste računari i mobilni uređaji, jer je sve prisutnija opasnost od gubitka podataka, onemogućavanja pristupa podacima, krađe kredencijala ili identiteta, ali sve češće dolazi i do zloupotrebe računara za pristup drugim računarima. Ovakve zloupotrebe najčešće imaju za cilj sticanje protivpravne finansijske koristi.

Cilj Nacionalnog CERT-a Republike Srbije je da svakom korisniku predstavi osnovne principe bezbednog i sigurnog korišćenja Interneta, odnosno svih pogodnosti koje Internet pruža.

Opšte je poznato da milioni ljudi širom sveta u svakom trenutku koriste Internet mrežu. Većina njih spada u kategoriju savesnih i odgovornih korisnika. Ipak, postoje i oni koji Internet mrežu ne koriste na takav način, već, sakriveni iza virtuelne zavese, pokušavaju na različite načine da naruše funkcionisanje vašeg, ili sistema drugih korisnika koji su na mreži.

Načini zlonamernih pristupanja računarskim sistemima mogu biti različiti. Glavna podela je na aktivne i pasivne pristupe. Aktivni pristup pretpostavlja izmenu nekih podataka, što se naknadno može utvrditi forenzičkim analizama, dok se pasivni pristup teže otkriva, jer on ne vrši nikakvu izmenu podataka u informacionom sistemu, već najpre ima ulogu takozvanog 'osluškivanja' mreže i najčešće se primenjuje u slučajevima špijunaže.

Neki od načina koje zlonamerni korisnici Interneta primenjuju za pristup računarima ili mobilnim uređajima su 'Phishing', zatim upad u neadekvatno zaštićeni privatni ili javni bežični pristup Internet mreži (Wi-Fi) ili bežični prenos podataka (Bluetooth), kao i zloupotreba sigurnosnih propusta instaliranog softverskog rešenja na računaru, odnosno informacionom sistemu.

Za najveći broj napada se koriste jednostavne metode, kao što su 'Phishing', 'Spam' i slično.

02

# Phishing

*'Phishing'* je jedna od metoda kojom zlonamerni korisnici Interneta prosleđuju imejl poruke na što veći broj adresa, u očekivanju da će neko od korisnika koji dobiju ovakvu poruku postupiti po navedenim instrukcijama. Najčešće to bude poruka na lažnom linku, koja često sadrži i lažni formular, a koju vam, navodno, prosleđuje vaša banka ili Internet provajder, i u kojoj se od vas zahteva da unesete svoje lične podatke. Na ovakav način, zlonamerni korisnici Interneta pokušavaju da dobiju vaše lične podatke, odnosno vaše kredencijale - korisničko ime i lozinku, pomoću kojih dalje pristupaju vašim nalozima, kao što su 'Facebook', 'e-mail' i slično.

Na ovakav način, zlonamerni korisnici Interneta dobijaju mogućnost da izmene sadržaj na vašim nalozima, šalju poruke ili fotografije, odnosno video zapise vašim prijateljima, ili drugim korisnicima. Zloupotrebe ovakvog karaktera mogu naneti štetu ne samo vama, već i članovima vaše porodice, prijateljima, pa čak i onim ljudima do kojih stigne takva jedna poruka, a koje vi zapravo i ne poznajete.

# 03 Bezbedno bežični

Opšte je poznato da se današnji računari i drugi mobilni uređaji u standardnom paketu opreme nude sa opcijom Wi-Fi (bežičnog povezivanja na privatne ili javne mreže), i Bluetooth (bežični prenos podataka). Ovakav pristup Internetu nam omogućava jednostavniju i lakšu upotrebu i dostupnost svih željenih sadržaja, kako kod kuće, tako i na javnim mestima kao što su hoteli, restorani, obrazovne ili kulturne ustanove i slično.

Ono što je važno napomenuti, ta dostupnost nije omogućena samo vama, već i svim drugim korisnicima Interneta koji se nalaze u vašoj blizini i koriste tu tačku pristupa. Ukoliko neki od njih pripadaju grupi zlonamernih korisnika, pružena im je mogućnost da iskoriste sve nedostatke ovakvog načina prenosa podataka i da pristupe vašim nalozima koje će zloupotrebiti na način koji im se, u datom trenutku, učini najpogodnijim. To može biti deljenje vaših fotografija, ili video zapisa sa vašeg naloga, ali isto tako mogu slati i fotografije, odnosno video zapise, ili neki drugi sadržaj koji nije vaš, a čijom distribucijom vam može biti naneta velika šteta. Ono što Nacionalni CERT Republike Srbije posebno preporučuje, jeste izbegavanje korišćenja javnih bežičnih tačaka za pristup Internetu prilikom izvršavanja finansijskih transakcija, ili provere stanja bankovnih računa, ukoliko navedena tačka pristupa nije adekvatno zaštićena. Sugestija je da bežične tačke za pristup Internetu na računarima obavezno budu osigurane lozinkom koja ne sadrži informacije vezane za vaš datum rođenja, imena kućnih ljubimaca i slično, jer se takve lozinke lako mogu otkriti.

04

# Malware

## Maliciozni softver

Većina korisnika računara je imala prilike da se upozna sa pojmovima kao što su: trojanac, crv ili virus. Neki korisnici su čak bili prinuđeni da otklanjaju posledice koje ovakvi maliciozni softveri izazivaju na računarima, odnosno informacionim sistemima. Za razliku od drugih vidova zloupotrebe računara, maliciozni softveri mogu pričiniti najveću štetu krajnjim korisnicima, ali i informacionim sistemima uopšte.

Ovde posebnu pažnju treba skrenuti na one tipove malicioznih softvera koji se instaliraju na računar putem propusta otkrivenih na operativnim sistemima. Time je omogućeno da osoba koja je postavila takav maliciozni softver može u potpunosti preuzeti kontrolu nad tim računarom, bez znanja vlasnika, i time omogući ostvarivanje svih željenih ciljeva. Pored propusta koji se odnose na operativne sisteme (npr. Microsoft Windows, MAC OS) koji su instalirani na računarima, postoje i propusti koji se tiču instaliranih Internet pretraživača (npr. Internet Explorer, Opera, Google Chrome), ili alata koji omogućavaju čitanje multimedijalnih datoteka (npr. Windows Media Player), ili dokumenata (npr. Adobe Acrobat Reader).

Nacionalni CERT Republike Srbije bi skrenuo posebnu pažnju na tip malicioznog softvera koji je poznat pod nazivom 'Ransomware'. Ovaj tip malicioznog softvera nesavesni korisnici Interneta postavljaju u računare, odnosno informacione sisteme kako bi kriptovali podatke i time onemogućili njihovu upotrebu, a pričinjena šteta može biti nemerljiva. Znajući da posledice ovako pričinjene štete mogu biti izuzetno velike, zlonamerni korisnici zahtevaju isplatu određene sume novca, kako bi zauzvrat dostavili ključeve za enkripciju, odnosno omogućili da ponovo pristupite i koristite inficirane datoteke. Najveći problem u ovakvoj situaciji je taj što korisnik nije siguran da će zaista dobiti ključeve za enkripciju oštećenih podataka, ili ako ih i dobije, njihovom primenom možda neće biti moguće pristupiti svim podacima koji su bili inficirani ovakvim malicioznim softverom. Dodatni problem je to što plaćanjem otkupnine, korisnici finansiraju kriminalne organizacije i zato je preporuka Nacionalnog CERT-a Republike Srbije, ali i drugih organizacija koje se bave informacionom bezbednošću, da se otkupnina ne plaća.

# 05
# Preporuke

Postoji više preporuka kako zaštititi računar od napada zlonamernih korisnika. Osnovna preporuka je obavezno instaliranje nekog od antivirusnih softvera na računare ili mobilne uređaje. Time ćete onemogućiti jednostavan pristup bilo kom zlonamernom korisniku. Dodatni vidovi zaštite su: postavljanje određenog 'Firewalla' na računar, zatim blagovremeno ažuriranje operativnog sistema i aplikacija koje se nalaze na računaru, odnosno mobilnom uređaju, primena automatskog ažuriranja operativnog sistema i aplikacija ukoliko postoji takva opcija, zatim postavljanje odgovarajuće lozinke čijim unosom se omogućava prijava korisnika na računar. Lozinka bi trebalo da sadrži svaki od preporučenih slovnih ili znakovnih karaktera, kako bi složenost lozinke bila što veća i time otežala neovlašćeni pristup računaru. Savet je da lozinka ne bude kreirana od informacija koji su ličnog karaktera. Tu pre svega mislimo na datume rođenja, imena roditelja, dece ili kućnih ljubimaca i slično, jer su to informacije koje zlonamerni korisnici najpre unose kao opciju prilikom pokušaja upada u računar.

Dodatni vidovi zaštite računara se svode na savesno rukovanje i korišćenje računara, odnosno svih pogodnosti koje nudi Internet. Ovde najpre mislimo na redovno kreiranje rezervnih kopija (eng.'Backup') svih važnih dokumenata, zatim bezbedno otvaranje elektronske pošte, odnosno imejla, koji u sebi mogu sadržati određene priloge (eng. 'attachment') putem kojih se distribuiraju računarski virusi. Poruke koje stignu od nepoznatih korisnika ne treba otvarati bez prethodne provere. Sugestija je da se posećuju isključivo zaštićene Internet stranice, koje u svojoj adresnoj liniji obavezno sadrže oznaku 'http://', ili 'https://', odnosno 'HTTPS protokol' (eng. 'Hypertext Transfer Protocol Secure').

Nacionalni CERT Republike Srbije skreće pažnju svim roditeljima čija deca aktivno koriste različite tipove socijalnih mreža na Internetu, da na adekvatan način objasne svojoj deci koji podaci, odnosno sadržaji mogu, ili treba da budu dostupni na Internet nalogu, a koje ne bi trebalo objavljivati. Posledice koje mogu da se jave zbog neadekvatno objavljenog sadržaja na Inetrnetu ne moraju uvek biti materijalne prirode, već se mogu odraziti i na psihu deteta, jer smo svedoci sve prisutnijeg vršnjačkog nasilja, a jedan vid takvog nasilja upravo može biti objavljivanje nekog neadekvatnog sadržaja na Internetu.

# 06
# Zaključak

Internet je sastavni deo svakodnevnog života i, kao takav, stalno se unapređuje u kvalitativnom i kvantitativnom smislu, a krajnji cilj je da svim korisnicima olakša obaveze, ali i život učini zabavnijim. Sve ove olakšice ostavljaju prostor za zloupotrebu i samim tim korisnike čine izloženijim i ranjivijim i u tom smislu Nacionalni CERT Republike Srbije, u saradnji sa drugim CERT timovima, čini sve kako bi pružio maksimalnu zaštitu korisnicima Interneta.

Budite odgovorni prema sebi i drugima dok radite i uživate na Internetu!

REPUBLIKA SRBIJA

RATEL

REGULATORNA AGENCIJA ZA
ELEKTRONSKE KOMUNIKACIJE
I POŠTANSKE USLUGE

**ADRESA**
Palmotićeva 2
11103 Beograd
Republika Srbija

www.cert.rs