

Kako zaštititi kućni računar – besplatna rešenja



Ponekad imamo potrebu da određene eksterne uređaje (mobilni telefon, USB fleš...) povežemo na naš računar. Ali oni mogu biti inficirani raznim malware-vima koji u određenim situacijama mogu da ugroze bezbednost računara i pored antivirusne zaštite koju primenjujete.

Kako je malware dospelo na moj eksterni uređaj?



Svi mi posedujemo mnoštvo prenosnih eksternih memorijskih uređaja na koje smeštamo razne podatke. Iste te uređaje povezujemo na razne računare (kod prijatelja, kod kuće, na poslu...). Ako je neki od računara na koje povezujemo naše prenosne uređaje zaražen nekim malware-om, velika je verovatnoća da će on zaraziti i naš prenosni uređaj, a mi ćemo pomoću njega nesvesno proširiti zarazu na druge računare na kojima ih koristimo, a koji nisu adekvatno zaštićeni.

Kako to sprečiti? Kako se zaštititi?



Da bismo umanjili rizik da nesvesno donesemo zaraženi uređaj, potrebno je da pazimo kako i gde koristimo naš uređaj, da ga povremeno proverimo od eventualne infekcije malicioznim programima i da pre svega zaštitimo naš kućni računar.

Šta je potrebno za zaštitu kućnog računara?



Da bismo efikasno zaštitili kućni računar, ne moramo trošiti novac da kupujemo razne programe za zaštitu jer danas postoji veliki izbor besplatnih programa za kućnu/privatnu upotrebu. Da bismo se zaštitili od velikog broja malware-a potrebno nam je nekoliko programa:

1. Antivirusni program
2. Firewall
3. Antimalware skener
4. Program za sprečavanje infekcije sa eksternih portabilnih USB uređaja

Pored ovih programa, potrebno je i podesiti prava pristupa na računaru. Većina korisnika se loguje na svoj računar sa nalogom koji ima administratorska prava. Da li nam je to zaista stalno potrebno? Iz bezbednosne perspektive, to je veliki rizik, jer za pokretanje određenih malware programa potrebna su administratorska prava. Niko od nas nema realnu potrebu da za vreme rada na svom kućnom računaru bude konstantno logovan sa administratorskim pravima. Administratorska prava su nam potrebna samo kada želimo da instaliramo neki program, promenimo neka podešavanja, eventualno pokrenemo neki program koji zahteva administratorska prava. Preporučljivo je da se za svakodnevnu upotrebu koristi običan korisnički nalog, a da se samo u slučaju potrebe logujete na administratorski nalog kako biste izvršili određena podešavanja. Naravno, svaki nalog koji koristite na kućnom računaru treba da ima lozinku. Za potrebe pokretanja programa koji traži administratorska prava ne morate se izlogovati iz vašeg korisničkog naloga pa logovati na nalog sa administratorskim pravima već za takve slučajeve imate opciju Run as (ili Run as administrator), koja vam omogućava da pokrenete određeni program sa administratorskim pravima pristupa (do ove opcije se dolazi desnim klikom na ikonicu pa se iz menija odabere). Preporuka je i da za svakog korisnika svog kućnog računara imate napravljen poseban korisnički nalog.

Još neki saveti kako povećati bezbednost na internetu

- Redovna provera i instalacija nadogradnji operativnog sistema
- Redovna provera i instalacija poslednje verzije programa koje koristimo
- Instaliranje proverenih programa i iz proverenih izvora (sa oficijalnog sajta proizvođača, sa proverenog repozitorijuma).
- Oprez pri pristupanju raznim sadržajima na internetu! Neke reklame mogu biti link do malware, pa je potrebno da pazimo na šta klikćemo. Zarad zaštite od takvih reklama možemo koristiti dodatak za pretraživač ABP (Adblock Plus), koji blokira većinu reklama koje nam se prikazuju na internetu. Možete ga preuzeti sa <https://adblockplus.org/> .
- Provera reputacije sajta koji posećujemo. Preporuka je da koristimo neki od dodataka za internet pretraživač koji bi nam mogao dati informaciju o sajtu koji posećujemo. Postoji plugin WOT (Web of Trust), koji nam daje ocenu drugih korisnika određenog sajta. Možete ga preuzeti sa linka <https://www.mywot.com/> .
- Neki od zlonamernih sajtova sami izvršavaju određene akcije po otvaranju stranice, odnosno po učitavanju stranice. Da bismo to sprečili, potrebno je da koristimo neki od dodataka za browser koji sprečava izvršavanje takvih akcija. No Script je dobar plugin za Firefox koji nam pruža zaštitu od takvih napada. Za Google Chrome i Opera pretraživač plugin koji nam pruža zaštitu od tih napada zove se Not Scripts
- Budite oprezni i pri upotrebi društvenih mreža i komunikacije putem elektronske pošte. Ako dobijete poruku sa neobičnim linkom čak i od poznate osobe, budite obazrivi. Neki malware programi koji su zarazili računar šalju poruke u ime korisnika računara preko maila, društvenih mreža i tako pokušavaju da se prošire po mreži.
- Posebno budite obazrivi sa priložima u elektronskoj pošti i pre otvaranja ih proverite antivirusom.
- Pazite šta gde objavljujete na internetu. Često preko društvenih mreža, blogova ili nekih foruma delimo svoje privatne informacije bez razmišljanja ko to sve može da vidi i šta može sa tim informacijama da uradi. Pre nego što nešto objavimo, trebalo bi da razmislimo kome sve to dajemo na uvid.
- Posebno budite obazrivi pri bilo kom vidu komunikacije sa nepoznatom osobom.
- Korišćenje bezbednih lozinki za sve internet servise. Za svaki servis korišćenje posebne lozinke. Radi jednostavnijeg čuvanja lozinki može se koristiti neki program za upravljanje lozinkama, kao na primer KeePass, koji čuva lozinke kriptovane i zaštićene na vašem računaru. Možete ga preuzeti sa <http://keepass.info/> .