Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Bezbednost internet pregledača

Uvod

Internet pregledači (eng. *browser*) kao što su Google Chrome, Microsoft Edge, Apple Safari, ili Mozilla Firefox predstavljaju jedan od najčešćih načina putem kojih ljudi koriste internet. Koristimo ih kad čitamo vesti, proveravamo elektronsku poštu, za onlajn kupovinu, gledanje video zapisa i igranje igrica. Kao rezultat toga, pregledači su česta meta sajber kriminalaca.
Mnogi ljudi pretpostavljaju da je pretraživanje interneta dovoljno bezbedno ako se drže toga da posećuju samo dobro poznate veb lokacije kojima veruju. Međutim, prilično je jednostavno slučajno kliknuti ili posetiti nebezbednu veb stranicu, ponekad čak i ne znajući da se to dogodilo. Pored toga, veb lokacije koje poznajete i kojima verujete itekako mogu biti hakovane, a sajber kriminalci na njih mogu instalirati zlonamerni softver. Na kraju, današnji pregledači nude mnogo novih funkcionalnosti, koje često mogu biti zbunjujuće i koje vas mogu izložiti dodatnim opasnostima ako nisu dobro konfigurisane.

Bezbedno korišćenje vašeg pregledača

U nastavku su predstavljeni najvažniji koraci koji vam mogu pomoći da se zaštitite:

Ažuriranje: Uvek koristite najnoviju verziju pregledača. Ažurirani pregledači sadrže najnovije bezbednosne ispravke i mnogo su bezbedniji. Sa današnjim računarima ovo je prilično jednostavno postići jer je dovoljno samo da na svom sistemu omogućite automatsko ažuriranje. Drugi način je da neke pregledače jednostavno restartujete (zatvorite i ponovo pokrenete) nakon što vam se prikaže obaveštenje da je dostupna nova verzija. Nakon ažuriranja, proverite da li vaš pregledač nudi i neke nove bezbednosne funkcionalnosti od kojih možete imati koristi.

Upozorenja: Današnji pregledači često mogu da prepoznaju određene zlonamerne veb lokacije koje su dizajnirane da vam nanesu štetu. Ako vas pregledač upozori da je veb sajt koji nameravate da posetite opasan, zatvorite karticu pregledača i potražite ono što vam je potrebno na nekom drugom veb sajtu.

Sinhronizacija: Nemojte sinhronizovati svoj službeni pregledač sa privatnim pregledačem niti sa bilo kojim privatnim nalozima. Sinhronizacija podrazumeva omogućavanje pregledačima na različitim uređajima da razmenjuju informacije jedni sa drugima i tako dele vaše informacije o pregledanju, kao što su istorija pregledanja, obeleživači (eng. *bookmarks*) i sačuvani sadržaj.

Lozinke: Mnogi pregledači podržavaju opciju čuvanja vaših lozinki za različite sajtove. Umesto da svoje lozinke čuvate u pregledaču, preporučujemo vam da koristite poseban menadžer lozinki. Menadžeri lozinki su zasebne aplikacije koje poseduju mnogo više bezbednosnih opcija i funkcionalnosti.

Dodaci: Dodaci (eng. *plug-ins*) ili ekstenzije su mali delovi softvera koji se dodaju pregledačima da bi se omogućila određena dodatna funkcionalnost. Međutim, svaki novi dodatak pregledaču može dodati i nove ranjivosti. Zbog toga na svom službenom računaru instalirate jedino one dodatke koji su odobreni od strane vaše kompanije, i dodatke, kao i pregledač, redovno ažurirate. Uklonite sve dodatke koji vam više nisu potrebni ili ih ne koristite.

Režim privatnosti: Većina pregledača nudi i opciju uključivanja režima privatnosti, poznatog i kao inkognito mod. Kada otvorite karticu pregledača u ovom režimu vi zapravo ograničavate informacije koje pregledač prikuplja o vama. Na primer, vaš pregledač tada neće prikupljati kolačiće, čuvati istoriju pregledanja i neće čuvati niti deliti osetljive informacije o vama.

Ćaskanje uživo: Neke veb lokacije nude funkciju ćaskanja uživo putem koje možete postavljati pitanja. Učestvujte u ovim onlajn ćaskanjima samo na poznatim, pouzdanim veb sajtovima. Pored toga, vodite računa i ograničite informacije o vama koje delite tokom sesije ćaskanja, jer ne znate ko sve prikuplja vaše podatke, šta sa njima radi i kome ih možda prodaje ili sa kim deli.

Čuvajte se udaljenog pristupa: Putem prevarne veb lokacije kriminalci mogu pokušati da hakuju vaš računar postavljanjem lažnog bezbednosnog iskačućeg prozora u vaš pregledač koji vas upozorava da je vaš računar zaražen i požuruje da uspostavite sesiju onlajn ćaskanja da bi vam pomogli da popravite računar. Potom će verovatno tražiti da im hitno dozvolite da instaliraju agenta za udaljeni pristup kako bi izvršili popravku. Zapravo je vaš računar sasvim u redu. Radi se o pokušaju prevare da instalirate zlonamerni softver kako bi mogli da ukradu vaše lozinke i druge podatke i da prate sve vaše aktivnosti na internetu.

Odjava: Kada završite sa posetom veb sajtu, obavezno se odjavite kako biste uklonili osetljive informacije za prijavu i lozinku pre nego što zatvorite pregledač.

Gost urednik

Din Parsons je izvršni direktor kompanije ICS Defense Force, sa preko 20 godina iskustva u odbrani od sajber napada. On je, takođe, i sertifikovani instruktor SANS obuke ICS515 i koautor/instruktor obuke ICS418, na kojima predaje o aktivnoj odbrani od sajber napada, reagovanju na incidente, liderstvu i upravljanju rizikom za industrijske kontrolne sisteme. www.linkedin.com/in/dean-parsons-cybersecurity.

Dodatni materijal

Menadžeri lozinki: https://www.sans.org/newsletters/ouch/password-managers/
Ažuriranje: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Socijalni inženjering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Privatnost - zaštitite vaše digitalne tragove: https://www.sans.org/newsletters/ouch/privacy/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović