Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- **Kako se pripremiti**
- **Izgubljeni / ukradeni uređaji**
- **Pristup bežičnim mrežama**
- **Javno dostupni računari**

Kako putovati bezbedno

Uvod

U ovom izdanju objasnićemo kako da bezbedno pristupite Internetu i koristite vaše uređaje dok ste na putovanju.

Gost urednik

Steve Armstrong je tehnički direktor za CyberCPR u Logically Secure-u, sertifikovani SANS instruktor i nekadašnji autor kurseva pri SANS-u. Aktivan je na Twitter-u kao **@Nebulator** i na Google plus-u: **+SteveArmstrongSecurity**.

Kako se pripremiti

Ako možemo da smatramo da je vaša mreža kod kuće ili na poslu bezbedna, onda uvek kada ste na putovanju svaku mrežu smatrajte nepouzdanom. Nikada ne znate ko je još priključen i kakvu pretnju može da prestavlja. Jednostavne mere koje možete da preduzmete pre samog putovanja mogu biti od velike pomoći da vaši uređaji i informacije ostanu bezbedni. Jednu ili dve nedelje pre putovanja:

- Identifikujte podatke koji vam neće biti potrebni dok ste na putovanju i uklonite ih sa uređaja. Na takav način će te značajno smanjiti negativne posledice ukoliko je vaš uređaj izgubljen, ukraden ili privremeno zaplenjen od carine ili službe bezbednosti. Ako se radi o službenom putovanju, raspitajte se kod vaših nadređenih, da li vaša organizacija obezbeđuje alternativne uređaje, specijalno konfigurisane za službena putovanja.
- Ako se radi o putovanju u inostranstvo, proverite kakav se tip priključka za struju koristi u državi u koju putujete. Možda će te morati da nabavite odgovarajući adapter. Takođe, proverite paket usluga provajdera vašeg mobilnog uređaja. Cene usluga prenosa podataka u romingu mogu da budu izuzetno visoke, tako da će te verovatno imati u planu da isključite opciju prenosa podataka dok ste u inostranstvu, sem ako vaš paket usluga ne uključuje i tu opciju. Ako vaš mobilni provajder ima takvu uslugu u ponudi, možda se odlučite da, na određen broj dana, aktivirate dodatni paket usluga koji podrazumeva i usluge u romingu.
- Instalirajte softver za daljinsko praćenje uređaja i opcijom daljinskog brisanja podataka, u slučaju da je vaš uređaj izgubljen ili ukraden. Mnogi noviji mobilni uređaji već imaju ugrađenu takvu opciju, samo je treba aktivirati (imajte na umu da je za takvu funkcionalnost potreban pristup Internetu).

Jedan ili dva dana pre putovanja:

Kako putovati bezbedno

- Ažurirajte na najnovije verzije operativni sistem uređaja, aplikacije i anti-virus softver.
- Aktivirajte odgovarajuća bezbednosna podešavanja, na primer „firewall“.
- Ako već nije podešeno, aktivirajte zaključavanje uređaja osigurano jakom lozinkom. Takvim podešavanjem, u slučaju da je uređaj izgubljen ili ukraden, pristup podacima će biti onemogućen.
- Izvršite enkripciju svih uređaja tako da u slučaju da su izgubljeni ili ukradeni onemogućite pristup uskladištenim podacima. Neki uređaji, na primer iPhone, to rade automatski, ako postavite lozinku ili pristupni kod.
- Napravite rezervnu kopiju svih uređaja. Ako se nešto nepredviđeno desi vašim uređajima dok ste na putovanju ili ostanete bez podataka, imaćete vaše podatke na sigurnoj lokaciji.

Bezbednost vaših uređaja dok ste na putovanju leži u pripremi uređaja pre nego krenete na put, fizičkoj sigurnosti uređaja u toku putovanju i korišćenju enkripcije prilikom svake “on-line” aktivnosti.

Izgubljeni / ukradeni uređaji

Kada krenete na putovanje vodite računa o fizičkoj bezbednost vaših uređaja. Na primer, nikada ne ostavljajte svoje uređaje u automobili tako da budi lako uočljivi, pošto kriminalci lako mogu da vam razbiju staklo i ukradu sve što ima neku vrednosti. Jedan od načina zaštite je da sa sobom ponesete sajlu/kabl na zaključavanje, tako da svoje uređaje možete fizički da zaključate, na primer laptop, kada nisu u vašem direktnom posedu. Kriminal svakako predstavlja veliki rizik, međutim imajte na umu da je daleko veća verovatnoća da ćete uređaj izgubiti nego da vam ga ukradu. Prema studiji koju je objavio „Verizon“, verovatnoća da će uređaj biti izgubljen je 15 puta veća nego da će biti uraden. Prema tome, uvek kada ste na putovanju proveravajte prisustvo vaših uređaja češće nego što to uobičajeno radite, na primer kada prođete aerodromsko obezbeđenje, napustite taksi ili restoran, kada se odjavite iz hotelske sobe ili iskrcate iz aviona.

Pristup bežičnim mrežama

Dok ste na putovanju, pristup Internetu često podrazumeva korišćenje javnih bežičnih mreža, na primer u hotelu, lokalnom kafiću ili na aerodromu. Problem sa javnim bežičnim mrežama nije samo u činjenici da nikada ne možete da budete sigurni ko ih je postavio, nego i što ne znate koje je osim vas na njih povezan. Usled toga, treba ih tretirati kao nepouzdane, u stvari to i jeste razlog zbog koga je potrebno pripremiti, osigurati svoj uređaj pre putovanja. Pored toga, kod bežičnog pristupa za komunikaciju između vašeg uređaja i bežičnog pristupnog uređaja koriste se radio talasi. To znači da svako koje je fizički blizu vas potencijalno može da presretne i nadgleda vašu komunikaciju.

Kako putovati bezbedno

Zbog svega navedenog ako koristite javnu bežičnu mrežu, potrebno je da obezbedite vašu „on-line“ komunikaciju korišćenjem enkripcije (šifrovanja). Na primer, prilikom korišćenja Internet pretraživača vodite računa da Internet strane koje posećujete omogućavaju enkripciju komunikacije (u okviru Internet adrese imaće ’https://’ prefiks i ikonu zatvorenog katanca). Osim toga, možda imate mogućnost korišćenja Virtuelne Privatne Mreže (VPN – „Virtual Private Network“) koja takođe omogućava enkripciju komunikacije. Korišćenje VPN-a vam je možda omogućeno od strane poslodavca, a postoji i mogućnost da za privatne potrebe sami nabavite takvo rešenje. Ako niste sigurni ni u jednu ponuđenu bežičnu mrežu na raspolaganju, razmislite o povezivanju preko vašeg „pametnog telefona“. (Upozorenje: Kao što smo ranije napomenuli, ovakvo rešenje može da bude veoma skupo kada se koristi u inostranstvu, prvo proverite sa vašim provajderom).

Javno dostupni računari:

Nemojte nikada koristiti javno dostupne računare, kao što su na primer računari u hotelskim holovima, bibliotekama ili Internet kafeima. Ne možete da znate ko je pre vas koristio računar i da li je neko namerno ili nenamerno inficirao računar. Kada god je to moguće, koristite samo uređaje koji su u vašem posedu i pod vašom kontrolom. Ako ipak morate da koristite javni računar, nemojte koristiti servise koji zahtevaju prijavljivanje ili kucanje lozinke.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org/

Dodatne informacije

Lozinke:	http://www.securingthehuman.org/ouch/2013#may2013
Verifikacija iz dva koraka:	http://www.securingthehuman.org/ouch/2013#august2013
Enkripcija:	http://www.securingthehuman.org/ouch/2014#august2014
Bezbednost tvog novog tableta:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac