SAVJETI ZA ZAŠTITU OD ZLOUPORABA I PRIJEVARA

Međunarodni pozivi

Budite oprezni kada uzvraćate pozive s brojeva koji imaju međunarodni predbroj, u Cjeniku Metroneta (www.metronet.hr) ili pozivom na broj 0800 8228 možete provjeriti međunarodni predbroj i prema tome odrediti odakle je poziv upućen.

Sigurnost na internetu

Redovito održavajte računalo zaštićenim – instalirajte anti-malware i antispam programe, te ih redovito nadograđujte sigurnosnim zakrpama i novim definicijama. Obratite pozornost na programe koje instalirate na računalo. Neki programi zahtijevaju stalnu vezu s internetom (stalno skidanje i slanje podataka), čime se može stvoriti znatna količina podatkovnog prometa (npr. online videoigre i servisi za komunikaciju u realnom vremenu).

Ukratko:

- Uvijek imajte uključen vatrozid i antivirusni alat te pripazite na njihova upozorenja.
- Redovno ažurirajte operativni sustav računala.
- Prilikom korištenja kućne bežične mreže koristite enkripciju kako bi se zaštitili od neovlaštenih upada.
- Izbjegavajte spajanje na nepoznate WiFi mreže ili mreže koje ne koriste enkripciju podatkovnog prometa
- Za pristup javnim servisima poput društvenih mreža, elektroničkoj pošti i sličnom koristite kompleksne zaporke koje sadržavaju više od 6 znakova, te se sastoje od slova, brojeva i specijalnih znakova.

Detaljnije:

1. Zaštitite svoje računalo:
   - koristite anti-malware programe
   - redovito obnavljajte definicije anti-malware programa (update)
   - pretplatite se na neku antivirus mailing listu
   - redovito instalirajte zakrpe (patch, update) i sigurnosne dodatke za vaš operativni sustav
   - korisnici MS Windows operativnih sustava mogu koristiti Windows Update servis (http://windowsupdate.microsoft.com)
   - koristite vatrozid (firewall)
   - provjerite da li su Internet stranice kojima pristupate na tzv. "crnim listama" proizvođača anti-malware programa
   - budite oprezni pri skidanju (download) datoteka s interneta, kao i pri otvaranju privitaka (attachment) elektroničke pošte

- datoteke uglavnom imaju samo jednu ekstenziju (.txt, .doc, .exe itd.). Datoteke sa dvije ili više ekstenzija (npr. .exe.scr) u pravilu su virusi ili drugi oblici programa koji mogu ugroziti sigurnost i/ili funkcionalnost Vašeg računala ili podatka
- očistite računalo od adwarea/spywarea (reklamnih i špijunskih "računalnih nametnika")

2. Zaštitite se od primanja neželjenih poruka (spam):
   - pazite kome dajete i gdje upisujte svoju pravu e-mail adresu. Za registracije na raznim web stranicama i web forumima koristite neku drugu adresu otvorenu na nekom besplatnom e-mail servisu
   - ako koristite newse , u polje "E-mail address" svog news programa nemojte upisati svoju aktivnu mail adresu ili ju zamaskirajte - npr. ivan.horvat@UKLONI-OVOinet.hr
3. Zaštitite svoju privatnost:
   - pazite kome dajete osobne podatke (ime, adresu, broj telefona)
   - nikada i ni na koji način nikome nemojte davati podatke za spajanje na internet (korisničko ime, lozinku) - osim ako zovete Službu za korisnike svog operatora koji se koriste za provjeru Vašeg identiteta
   - pazite kome dajete svoju e-mail adresu
   - budite oprezni u on-line konverzacijama (chat, IRC, ICQ itd.)

Virusi i ostali malware programi

Računalni virus je program koji ima sposobnost kopiranja samog sebe i aktiviranja u računalu bez dopuštenja i znanja vlasnika. Osim virusa postoje i drugi štetni programi (trojan, worm itd). Pojam *malware* upotrebljava se kao zajednički naziv za sav štetan softver (računalni virusi, trojanski konji, crvi, spyware i dr.). Malware ima za cilj izazvati neočekivane, neugodne i često nepoželjne situacije, a može izazvati i manju ili veću štetu na vašem računalu, kao što je npr. gubitak podataka s tvrdog diska, iskorištenje Vašega računala za napade na druge sustave ili otuđenje Vaših podataka. Često je napisan na način koji mu omogućuje samostalno "razmnožavanje" i širenje s jednog računala na drugo.

Kako se virusi i ostali malware-i prenose?

Virusi i ostali malware- imaju različite načine širenja i prenošenja. Moguće je prenijeti ih u obliku e-mail poruke odnosno priloga (attachment) u poruci, zaražene datoteke na vanjskim memorijskim jedinicama (USB stickovi, CD-i, memorijske kartice itd.), putem komunikacijskih programa kao što su IRC i ICQ, itd. Neki virusi se aktiviraju odmah po dolasku na novo računalo, drugi su pak podešeni da se aktiviraju u određeno vrijeme, pokretanjem određenog programa ili određenom korisničkom aktivnosti.

Vrste virusa

- virusi (malware-i) dijele se prema različitim kategorijama od kojih su najčešće podjele na:
  - zlonamjerni kod koji inficira datoteke - neki od takvih programa zaraze programske datoteke, obično određene *.com* i *.exe* datoteke. Kada se program

pokrene, pokrene se i virus. Drugi pak dolaze samostalno i njihovo pokretanje je neovisno o ostalim programima

- virusi koji inficiraju sistemske ili pogonske datoteke - smještaju se u određena sistemska područja na disku, odnosno ukoliko zaraze pogonske datoteke (boot sector) - u pogonska područja na disku ili se zapisuju nakon aktivacije u dio radne memorije namijenjene operativnom sustavu ili drugom dijelu za sistemske programe.
- makro virusi - donedavno najčešći oblik virusa, koji inficira npr. MS Office aplikacije. Ova vrsta čini uglavnom najmanje štete od svih vrsta virusa

U posljednje vrijeme najrašireniji su virusi koji se šire putem interneta, odnosno privitaka (attachment-a) u e-mail porukama. Takvi virusi se sami, bez znanja vlasnika zaraženog računala, šalju na e-mail adrese koje pronađu na računalu, u adresaru programa za upravljanje mailovima (npr. Outlook) ili na samom internetu.

Zaštita od virusa

Najbolji način za zaštitu od zlonamjernih programa jest korištenje redovito ažuriranog antivirusnog programa, te pažljivo praćenje izvora dokumenata ili programa koji se snimaju ili pokreću na računalu. Obzirom da ovo postaje dosta teško u uvjetima sve većeg širenja e-mail virusa, korištenje antivirusnog programa postaje apsolutna nužnost. Uz njih ćete od vašeg distributera ili proizvođača antivirusnog programa redovno dobivati i upozorenja i obavijesti o novim virusima. Ukoliko pak to upozorenje ne dolazi od vjerodostojnog izvora, šanse su da se radi o tzv. virus hoax-u , odnosno lažnom upozorenju.

Jedan od najčešćih načina širenja zlonamjernih programa je preko e-mail poruka, zato je nužan oprez pri otvaranju privitaka sumnjivih e-mail poruka. Pritom nije važno je li pošiljatelj netko koga poznajete ili nije (polje "From" u e-mail poruci) jer se noviji zlonamjerni programi distribuiraju sa zaraženog računala bez znanja njegovog vlasnika te je moguće da dobijete zaraženu e-mail poruku i s adrese nekoga koga poznajete i za koga znate da ne bi poslao virus.

Za zaštitu od virusa koriste se programi raznih proizvođača od kojih su neki i besplatni za privatne korisnike. Većina besplatnih programa ne dozvoljava upotrebu u poslovnim okruženjima.

Metronet ima strateški partnerski status (Managed Service Partner) s najvećim svjetskim sigurnosnim brandovima, te stoga svojim korisnicima može ponuditi paletu antimalware-a.

Firewall

Firewall (vatrozid) je zaštita računala koja obavlja kontrolu, i provjeru paketa podataka koji nose informacije sa i na Internet ili unutar korisnikove lokalne mreže. Firewall je napravljen da bi zaštitio povjerljive korisničke podatke od neautoriziranih korisnika blokiranjem i zabranom prometa prema pravilima koje korisnik sam određuje.

Firewall može biti softverski ili hardverski. Softverski firewall instalira se na jedno računalo, a ovisno o namjeni može štititi jedno računalo ili cjelokupnu mrežu korisnika. Hardverski firewall je fizička komponenta koja omogućuje zaštitu čitave mreže ili određenog broja računala. Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koja određuju kakav promet je dopušten, a kakav zabranjen.

Firewall programi za osobna računala

Firewall koji se nalazi na osobnom računalu korisnika ima zadatak kontrole i ograničavanja pristupa računalu s Interneta ili lokalne mreže. Njegova je uloga da na osobnom računalu omogućava pristup samo onima kojima smo to i dopustili, a svi ostali su onemogućeni i njihovi pokušaji pristupa zabilježeni.

Za razumijevanje rada firewall-a potrebno je poznavati dva stručna pojma, a to su IP adrese i portovi.

TCP i UDP portovi

Korisnik putem različitih programa (ftp, mail, http, chat, msn) koristi razne sadržaje na Internetu koji se prenose u obliku TCP ili UDP paketa. Da bi se razlikovali paketi različitih programa, svaki program ima svoj port (vrata, prolaz, kanal) po kojem šalje i prima pakete; tako npr. FTP koristi portove 20 i 21, HTTP port 80, itd. Što je manje portova ostavljeno otvoreno i što je manje adresa kojima ste dozvolili pristup, to je mogućnost zlonamjernog pristupa računalu manja.

TCP portovi funkcioniraju na način da rade provjeru isporuke sadržaja uz mogućnost ponovnog slanja paketa mrežnog prometa ili njihove korekcije, dok UDP portovi samo šalju pakete mrežnog prometa bez provjere isporuke poslanih paketa.

Prilikom podešavanja firewall-a potrebno je pažljivo razmotriti koji promet smatramo poželjnim, a koji ne pa će dobro konfiguriran firewall automatski dopuštati Vašim aplikacijama pristup Internetu ili pristup pojedinim poslužiteljima preko definiranih protokola i portova i obrnuto.

IP adresa

IP adresa predstavlja jedinstvenu oznaku svakog računala, a služi za komunikaciju, odnosno isporuku mrežnog prometa među računalima i drugim elektronskim uređajima.

IP adresa može biti privatna ili javna. Privatne IP adrese su adrese unutar korisnikove mreže, dok su javne IP adrese one IP adrese koje se koriste za razmjenu podataka putem interneta.

Nadogradnje operativnog sustava i programa koje koristite

Proizvođači programa, operativnog sustava i paketa nadogradnje (service pack) uočavaju propuste na operativnim sustavima i aplikacijama, te izdaju odgovarajuće sigurnosne zakrpe dostupne uobičajeno na stranicama proizvođača. Nadogradnju operativnih sustava Windows možete pokrenuti na stranici http://windowsupdate.microsoft.com/ ili odabirom izbornika *Start* na vašem računalu → All Programs → Windows Update.

Nadogradnju MAC OS-a možete provjeriti putem App Store aplikacije, pod stavkom Update.

Savjeti za korištenje i zaštitu WLAN-a

Nezaštićena WLAN veza omogućava drugim računalima pristup vašem hot-spotu i zloporabu vašeg računa

- Pri konfiguraciji bežične mreže potrebno je koristiti odgovarajuću razinu enkripcije podataka kako bi izbjegli krađu podataka ili identiteta, te spriječili napade koji mogu biti izvedeni putem Vaše bežične mreže
- Preimenujte svoju WLAN mrežu i promijenite zadanu lozinku navedenu na uređaju.
- Isključivanje SSID prijenosa (naziv WLAN mreže) pruža dodatnu sigurnost jer druga računala moraju znati SSID kako bi se spojila.

Phishing

Što je phishing?

Phishing je vrsta prijevare putem koje zlonamjerni pojedinac ili organizacija (lažno se predstavljajući) pokušava doći do osjetljivih, povjerljivih ili tajnih podataka. Podaci koji se takvim putem prikupljaju mogu biti osobni podaci (poput imena, prezimena, lozinke, PIN-ova, pristupnih podataka raznim servisima), a u poslovnim okruženjima phishing napadi gotovo uvijek se provode kako bi se došlo do poslovnih podataka ili kako bi se identitet žrtve iskoristio za pristup poslovnom okruženju.

Najčešći oblici phishing napada provode se putem maila ili lažnih web stranica na kojima se traži unos podataka.

Sofisticiranost phishing napada varira. Npr. masovni i manje stručni napadi provode se slanjem e-mail poruke u kojoj se od korisnika traži da odgovori s pristupnim podacima, a u svrhu poboljšavanja usluge ili sprečavanja brisanja korisničkog računa. Takve poruke gotovo redovito prati slaba pismenost, gramatičke i pravopisne greške.

Napredniji napadi često se provode na nekoliko razina i traju dulji vremenski period. Ovakvi napadi karakteristični su za poslovna okruženja.

Ovakav napad provodi se pažljivim odabirom potencijalne žrtve. Nakon pronalaženja žrtve osobi se šalje e-mail poruka ili se upućuje telefonski poziv, te se lažnim predstavljanjem traže podaci ili posjeta zaraženoj web stranici koja sadrži maliciozni kod kojim se vrše daljnje faze napada. Ovakvi napadi uvijek su personalizirani, a često napadač detaljno proučava poziciju osobe, njene poslovne i privatne navike. Ovakvim napadom, u slučaju uspješnosti mogu se nanijeti velike poslovne štete ako je žrtva visoko pozicionirana u svojoj organizaciji.

Obrana od phishing napada

Najbolji način obrane od phishing napada sastoji se od dvije razine:

1) Antimalware zaštita web filteringom koji će prepoznati gotovo sve postojeće napadače.

2) Provjerom osobe ili organizacije koja vas kontaktira. Na primjer, banka nikada telefonskim putem neće tražiti osobne podatke radi evidencije osobnih podataka, broja kartice ili PIN-a.