Sigurnosna zaštita korisnika

Mr. sc. Branimir Radić

Rujan, 2013.

SADRŽAJ

- *UVOD*
- *OSOBNO RAČUNALO*
- *E-MAIL*
- *INTERNET*
- *ZAŠTITA, EDUKACIJA I OGRANIČENJA*
- *ZAKLJUČAK*

UVOD

- Za pomoć korisnicima potrebno je razumijeti prijetnje:
  - http://sistemac.srce.unizg.hr/fileadmin/user_root/seminari/Srce-Sys-Seminari-Sigurnosne_racunalne_prijetnje.pdf
- Prevencija i detekcija je tema ovog predavanja
- U idealnom svijetu – svaki korisnik razumije što koristi i koji su rizici, to nije svijet u kojem živimo
  - Nedostatak obrazovanja
  - EULA – 30-40 strana samo-zaštite
  - Neprestani napredak tehnologije – veći složeniji sustavi -> više mogućnosti zloupotrebe
  - 50% uređaja umreženo?

UVOD

- Zaštita korisnika je i zaštita sustava i obrnuto
- Neinformatičke ustanove – (obrazovne, znanstvene i drugo) nerijetko imaju značajni broj ne-tehnički educiranog kadra
- U predavanju neće biti obrađeno kako sustavom štititi sustav, već samo kako korisnike i korisničke uređaje

UVOD

- Osnovna i prva zaštita korisnika – EDUKACIJA
- Drugi pristup je restrikcija
- Ovi pristupi nisu međusobno isključivi, ali onemogućava ih samo jedna stvar – arogancija
  - Korisnika – Ja sam MR. dtr. Dr.sc. Miss Universe…
  - Administratora – „What's the worst that can happen?!"
  - Uprave– „What's the worst that can happen?!"
  - Sokrat: " I appear to be wiser than he, because I do not fancy I know what I do not know."

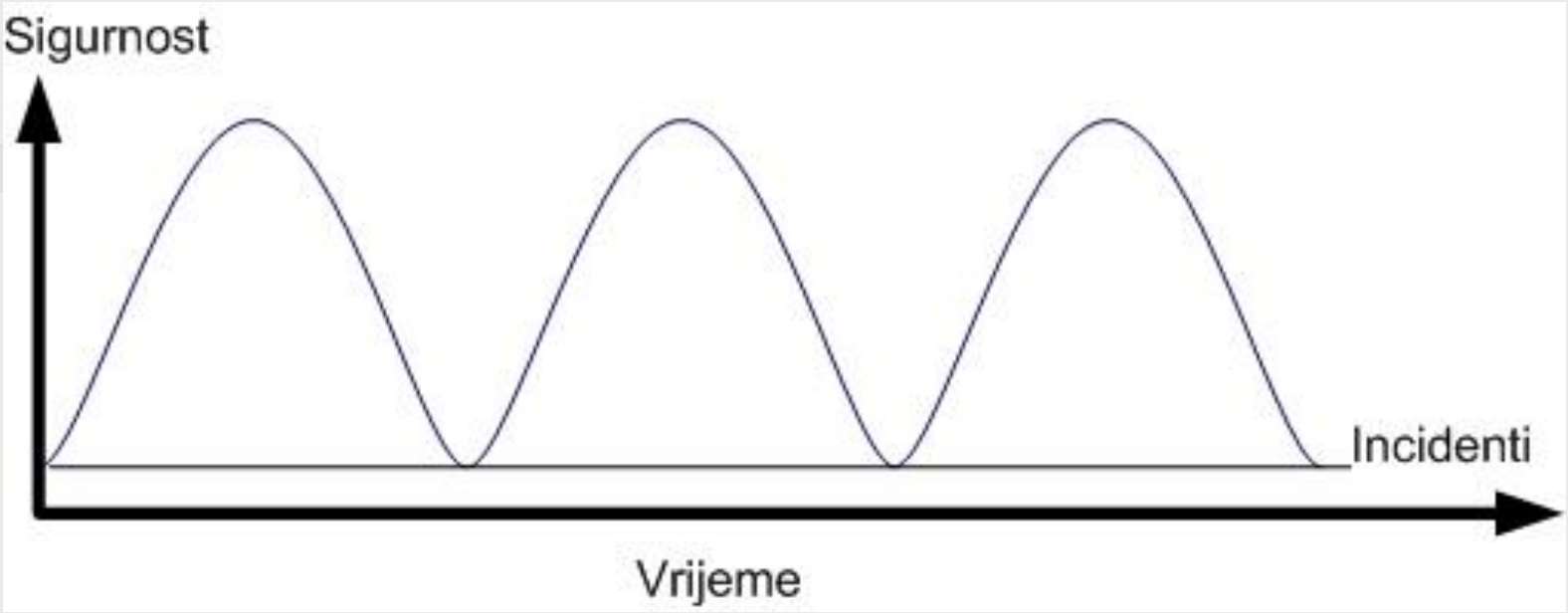
UVOD

- Korisnici uglavnom na MS tehnologijama – „ranjivije” (odnosno napadanije) od drugih.
- Eskalacija rizika kako se napreduje po zapovjednom lancu i eskalacija broja sustava za kompromitaciju
- „Gadgets” – danas sve veći broj uređaja izmjenjuje podatke

UVOD

- Važno je znati najgori mogući scenarij
- Primjera radi windows ključevi
- Kada se zna što je najgore što se može dogoditi **ponekada** je moguće dobiti razumijevanje
- Problem – koliko sredstava se uloži toliko se sigurnosti ostvari, ako se uloži više sredstava ne dogodi se incident, čini se da su sredstva protraćena…

UVOD



OSOBNO RAČUNALO

- Osobna računala
  - Zaštita korisničkih podataka
  - Kontrola pristupa
  - Zaštita od eskalacije incidenta
  - Edukacija (formalna + neformalna)

OSOBNO RAČUNALO

- Zaštita korisničkih podataka – centraliziranje upravljanja:
  +
  - Pojednostavljenje modela
  - Efikasnost
  - Unifikacija alata
  - Globalna sigurnosna pravila
  - Automatska implementacija novih pravila
  - Udaljeno upravljanje i ispravke
  - Upravljanje slikama
  - Mobilnost korisnika
  - Politika izmjena lozinki ili složenost lozinki

OSOBNO RAČUNALO

- Zaštita korisničkih podataka – centraliziranje upravljanja:
  -
    - Udaljeno upravljanje i ispravke – tendencija pristupa zovi za svaku sitnicu
    - Pretjerano oslanjanje na sustav
    - Zloupotreba centralizacije
    - Specifični korisnici i zahtjevi
    - Cijena
    - Single Point of Failure

OSOBNO RAČUNALO

- Zaštita korisničkih podataka – centraliziranje upravljanja: Implementacije
  - AD
  - samba 4 (+ Ubuntu server + openldap)
  - Freeipa
  - GOsa²
- Korisnici, računala i grupe + group policy

OSOBNO RAČUNALO

- Zaštita korisničkih podataka – backup :
  - Postoje brojna rješenja, komercijalna i besplatna:
    - Komercijalana – Asigra Cloud Backup, Comodo Backup, Druva InSync, Norton Ghost, Windows Backup and Restore…
    - Freeware – Bacula, rdiff backup, rsync, AOMEI Backupper, Redo Backup and Recovery…
- http://en.wikipedia.org/wiki/List_of_backup_software

OSOBNO RAČUNALO

- Zaštita osobnih podataka – backup
  - Što štititi?
  - Kako štititi?
  - Privatnost?
- Odvajanje diskova
- Odvajanje direktorija
- Odvajanje korisničkog prostora
- Nužno uvođenje pravila da se ne dođe u situaciju da se (skupi) backup koristi za multimedijske sadržaje

OSOBNO RAČUNALO

- Zaštita osobnih podataka – backup
  - Treba razlikovati backup i arhiviranje
  - Desktop Vs „Posao mapa”
  - Tko kada i kako upravlja backupom + restoreom

OSOBNO RAČUNALO

- Antivirusna zaštita
  - Trenutno „System Center Endpoint Protection”
  - Problem ako se često mijenja
  - Otvorena vrata!!!
  - Treba biti upravljan samo od strane administratora
  - Svaka netipična akcija može biti problem

OSOBNO RAČUNALO

- Odgovoran rad:
  - Ne raditi pod administratorom – mač sa dvije oštrice
  - Raditi pod povišenim privilegijama – mač sa dvije oštrice
  - Redovite obavijesti o mogućim rizicima

OSOBNO RAČUNALO

- Kontrola pristupa
  - Fizička
    - Pristup do samog ureda odnosno računala
    - Pristup do poslužitelja sa pristupom korisničkim računalima
    - Automatsko zaključavanje
    - Biometrijske metode – Jednostavnost, pouzdanost i neinvezivnost

OSOBNO RAČUNALO

- Kontrola pristupa
  - Logička
    - Podjela adresnog prostora
    - Firewall
    - Korisničke ovlasti
    - Segmentacija

OSOBNO RAČUNALO

- Firewall
  - Ulazni – važniji
  - Izlazni – Nije bezznačajan
- Dvostruka implementacija otežava pronalaženje bugova, ali sprečava samovolju
- Trostruka implementacija je suvišna i treba je izbjegavati (računala+Vlan+Vanjski FW)
- Jedan dio treba biti statički

OSOBNO RAČUNALO

- Zaštita od eskalacije incidenta
  - Pristup minimalnih ovlasti – više posla kada nema problema
  - Klasifikacija resursa/dokumenata + implementacija modela:
    - *Lattice* model
    - *Bella-LaPadula* („no read up, no write down”) – pristup po razinama
    - *Biba* model („no write up, no read down”) - integritet za objekte i subjekte
    - Take-Grant model – rizičan vrlo u akademskoj zajednici, prednost je manja aktivnost vrha piramide

OSOBNO RAČUNALO

- Stvari koje korisnici trebaju znati:
  - Osobna sigurnost na računalnom sustavu
  - Sigurnost i važnost sigurnosti lozinke
  - Fizička sigurnost
  - „Nesigurnost” podataka
  - Netrajnost podataka
  - Doseg nesigurnosti
  - Enkripcija – kada je ima a kada nema
  - Razlika i važnost razlika wireless i wired konekcija

OSOBNO RAČUNALO

- Stvari koje korisnici trebaju znati (idealno):
  - Krađa identiteta
  - Zaštita podataka
  - Antivirusna zaštita
  - Oporavak u slučaju incidenta/kvara
  - On-line poslovanje

Pauza

E-MAIL

- Elektronska pošta - prijetnje
  - Virusi
  - SPAM
  - Phising
  - Razne prijevare elektroničke pošte – vrlo prilagođene korisnicima

E-MAIL

- Virusi
  - U attach datoteci (često komprimiranoj – privatnost)
  - Download nakon pristupa lažnim web stranicama
  - Zaštita
    - Web klijenti neka razina integrirane zaštite
    - Pravila na poslužitelju ograničavaju prenosive extenzije
  - Posljedice
    - Preuzimanje e-mail adresara
    - Zlorabljenje kompromitiranog računa elektronske pošte + vidi gore
    - Zlorabljenje kompromitiranog računala

E-MAIL

- Virusi
  - Šteta
    - Blaklisting klijenta ili domene
    - Gubitak podataka
    - Gubitak privatnosti podataka
    - Eskalacija – poznati pošiljatelj

E-MAIL


ROYAL BANK
of
NIGERIA
I have emailed everyone I can possibly find, my Prince, but no-one wants to help you move your money.
AGENT-X COMICS
WWW.AGENT-X.COM.AU

E-MAIL

- SPAM
  - Q1 2013 - The percentage of spam in total mail traffic was up by 0.5 percentage points in the first quarter, averaging 66.5%.
  - 4 osnovna tipa – Reklame za web stranice, reklame za proizvode, “419 scams”, Phishing (zbog specifičnosti izdvojeno objašnjen)
- Zaštita
  - SPAM filteri (oba nivoa)
  - Odgovorno ponašanje
  - Ignoriranje (nije uvijek moguće)

E-MAIL

- SPAM – Posljedice
  - Financijska prevara
  - Povečanje količine samog SPAM-a (prema korisniku i domeni)
  - Krađa identiteta (i šire od email-a)
  - Prestanak rada poslužitelja (preopterećenje)
- SPAM – Šteta
  - Blaklisting klijenta ili domene
  - Gubitak povjerenja
  - Eskalacija – poznati pošiljatelj
  - Gubitak željene elektronske pošte

E-MAIL

- Phishing
  - Specifični oblike neženjene pošte usmjeren na krađu privatnih podataka lažnim predstavljanjem
  - Izuzetno napredovao u zadnje vrijeme
  - Usredotočen na činjenicu da većina korisnika preolako dijeli korisničko ime i zaporku. Istraživanje “dajte mi svoju lozinku”, izvor RSA, 2007.:
    - 70% za čokoladicu (London)
    - 34% ni za što (London)
    - 67% za kavu u Starbucku (Italija)

E-MAIL

- Phishing – zaštita
  - Isto kao kod SPAM-a + edukacija
  - Kada bi se u sve glave moglo simultano unijeti “Noone but you may ever know your password” phishing bi nestao ☺
  - Dvostruko usmjeren na neznanje – Zastrašivanje + neznanje o procedurama

E-MAIL

- Elektronska pošta zaštita sustava – ovisi o administratoru dodijeljenim ovlastima:
  - SPAM filter – rizik HAM-a u ovisnosti o strogoći – moguće blokiranje ili samo obilježavanje
  - Upravljanje zaporkama
  - Integracija sa manje ili više štićenim sustavima – AAI.

E-MAIL

- Elektronska pošta savjeti:
  - Zdrav razum – Što je sumnjivo u mračnoj ulici…
  - Ne odgovarati na SPAM i uvredljive poruke – primjer rasizam
  - Ne otvarati datoteke ili linkove od nepoznatih izvora
  - Zaporke – odgovorno upravljanje; izmjena i zaštita
  - Odgovorno ponašanje na javnim terminalima

INTERNET

- Nema štete do štete koju neodgovorni/neuki korisnik može napraviti vlastitom računalu
- Socijalne mreže i štetni likovi sa njih
- Unos lozinki na krivim (lažnim) web stranicama
- Pregledavanje Internet sadržaja sa nesigurnim preglednikom:
- Nepoznavanje rizika on-line financijskog poslovanja
- Pristup nesigurnim i nepotvrđenim sadržajima (https sa neispravnim/nepotpisanim certifikatom)
- Pristup tajnim (zaštićenim) sadržajima putem nesigurne mreže

INTERNET

- Pristup tajnim (zaštićenim) sadržajima putem javnih terminala
- Zaštita
  - Odgovorno pretraživanje Internet sadržaja (nužna edukacija)
  - Redovna nadogradnja preglednika – poželjno središnje upravljanje (IE pogodniji)
  - Filtriranje sadržaja – Idealno „Open on demand”
  - Korištenje integriranih ekstenzija za preglednike problem je više prevelik izbor nego nedostatak: https://chrome.google.com/webstore/search/security

INTERNET

- Posljedice:
  - Zaraza virusom uz sve posljedice koje to donosi
  - Materijalna šteta pri prijevarama
  - Kompromitacija korisničkog računa na legitimnim sustavima
  - Trojanac u pregledniku koji
    - Prenosi informacije o ponašanju za kasniju zloupotrebu
    - Snima ponašanje i podatke – kasnija krađa identiteta
  - Modifikacije preglednika (vrlo često, ali više iritantno nego išta ozbiljnije)

Edukacija

- Razina edukacije koja bi trebala biti obvezna ovisi o:
  - Kritičnosti podataka kojima korisnik upravlja
  - Kritičnosti sustava kojima korisnik pristupa
  - Vremenu koje korisnik radi na računalnom sustavu
  - Složenosti operacija koje na računalnom sustavu korisnik izvodi (čistačica VS. Recezent)

Edukacija

- Neformalno:
  - Phishing test uvjet za odobravanje korisničkog računa:
    - http://www.sonicwall.com/furl/phishing/
    - http://www.opendns.com/phishing-quiz/
    - **http://survey.mailfrontier.com/survey/quiztest.cgi?themailfrontierphishingiqtest**
    - https://www.paypal.com/webapps/mpp/security/antiphishing-canyouspotphishing
  - Phishing test, IQ test, Quiz
  - http://www.emailspamtest.com/

Edukacija

- Neformalno:
  - Uvjet za korisnički račun je neki oblik EULA – napraviti vlastiti, pravna valjanost i vrijednost nije toliko važna
    - Nabrojati rizike
    - Potencijalne štete
    - Kraj sa „razumijem i prihvaćam”
  - Moguće pri nadogradnji sustava

Edukacija

- Formalna
  - ECDL tečajevi na srcu http://www.srce.unizg.hr/proizvodi-i-usluge/obrazovanje/tecajevi/osnovni-tecajevi/ecdl-tecajevi/
    - Certificiranje
  - Školovanje – FER, FOI, ETFOS, FESB, PMF …
  - CSCU http://www.eccouncil.org/Training/cscu-assessment

Edukacija

- Neformalna
  - Predavanja i seminari (poput ovog)
  - On-line literatura; primjerice:
  - http://www.net-security.org/secworld.php?id=10036
  - http://lifehacker.com/5916551/browse-like-bond-use-any-computer-without-leaving-a-trace-with-tails

Edukacija

- Literatura
  - „Za neznalice” edicija – ohrabrujuća za početnike
  - „A beginner’s guide” – malo naprednije, ali i dalje adekvatno za početnike
  - Za naprednije korisnike: „**Quick Reference Guide**”
  - Za administratore – službena Microsoft literatura – tipa „A Comprehensive Guide”
  - I naravno google ☺

Ograničenja

- Ironično, ali istinito tehničkim mjerama zaštite korisnika najviše se protive sami korisnici jer:
  - Ograničavaju neke aspekte rada na računalu
  - Rijetko sputavaju produktivan rad (puno češće „dangubljenje”)
  - Korisnici smatraju (neopravdano) da su uvedene tehničke mjere nepotrebne
  - Nisu svjesni potencijalnih šteta
  - Precjenjuju vlastito znanje i sigurnost
  - Precjenjuju pouzdanost samih računalnih sustava

Ograničenja

- Tehničke mjere:
  - Automatska instalacija zakrpa na računalima
  - Automatska i središnje upravljana antivirusna zaštita
  - Ograničenje rada poslužitelja elektroničke pošte – veličina poruka, veličina attachment datoteka, dopuštene extenzije, ne prihvaćanje naprednih mailova (koji zahtijevaju post procesiranje)
  - Ograničenje ovlasti u slučaju incidenta

Ograničenja

- Tehničke mjere (nastavak):
  - Firewall ograničenja
    - Zatvoreni portovi
    - Zatvoren adresni prostor
    - Filtriranje Internet sadržaja

Zaštita

- Za implementaciju kvalitetnih pravila potrebno je imati:
  - Adekvatnu potporu uprave institucije
  - Kvalitetnu sigurnosnu politiku
- Sigurnosna politika je dokument koji:
  - Mora podržati uprava
  - Daje smjernice za upravljanje informacijskom sigurnošću u skladu sa poslovnim zahtjevima organizacije i relevantnim zakonima i propisima
  - Skup dokumenata – da bi zadržala jednostavnost
  - Podložna redovitim izmjenama kako bi pratila tehnologije

Zaštita

- Sigurnosna politika treba sadržavati:
  - Definiciju informacijske sigurnosti, glavne ciljeve i važnost sigurnosti
  - Izjavu uprave o podupiranju sigurnosne politike odnosno ciljeva politike
  - Okvir za uvođenje kontrola te strukturu za procjenu i upravljanje rizikom
  - Objašnjenje sigurnosne politike, principe, norme i zahtjeve specifične za organizaciju
  - Definiciju odgovornosti u upravljanju sigurnošću, uključujući i proceduru i odgovornost za prijavu incidenata

Zaštita

- Za sigurnosnu politiku preporuča se PDCA model
  - **P**lan - Planiranje
  - **D**o - Provođenje
  - **C**heck - Provjera
  - **A**ct - Djelovanje

Zaključak

- Najveća prijetnja sigurnosti je?:
  - Nesiguran software
  - Nesigurna mreža
  - Nesiguran OS
  - Pogreške u konfiguraciji
  - Ili...

Zaključak

- Za zaštititi korisnika (od samog sebe) :
  - Uvesti kontrole
  - Uvesti upravljanje
  - Brojne zaštite
  - Pravila za korisnike
- Osnova je podrška nadređenih

An Aside

- Rizik i upravljanje rizikom je dio posla, budući da je teško producirati točne brojeve osobni savjet je :

  ALWAYS OPEN WITH THE WORST CASE SCENARIO!!!

  (NO MATTER HOW IMPROBABLE)

Hvala!
Pitanja?