Zaštita informacionih sistema i bezbednost

Održavanje IS

Preporuke danas su da cijena ulaganja u zaštitu informacionih sistema treba da bude od 7% do 15% cijene hardvera i softvera samog IS.

Najčešći uzroci postajanja žrtve

-Požuda
-Pohlepa
-Lakovjernost
-Lenjost
-Saosjećanje
-Brzopletost

Požuda:

Prevaranti na internetu računaju na vaše emocije pa se često, naročito na društvenim mrežama, pretvaraju da su (atraktivni) muškarci ili žene.

Trebalo bi da znate da flert na internetu, naročito sa osobama koje ne poznajete, najčešće ima manje romantične motive nego što bi vi to želeli.

Pohlepa:

Ako je nešto suviše dobro da bi bilo istinito, najmanje što možete da uradite je da posumnjate u to.

Besplatni računar, telefon, dobitak na lutriji ili procenat od novčane transakcije koja je ima veze sa ozloglašenom internet destinacijom Nigerijom su dovoljno sumnjiva ponuda da bi ultimativan savjet bio - uzdržite se i ignorišite ponudu.

Lakovjernost:

Neki prevaranti pokušavaju da pridobiju poverenje korisnika koristeći u tu svrhu poznate brendove ili se pak, predstavljaju kao prijatelji vaših prijatelja računajući da im je to dovoljna preporuka.

Lenjost:

Kriminalci računaju na vašu lenjost i na to da se nećete potruditi da provjerite da li je link u pristigloj email poruci koju vam navodno šalje banka pravi, posetom web sajtu direktnim ukucavanjem internet adrese vaše banke u adres-baru browser-a ili jednostavnim pozivanjem banke telefonom.

Saosjećanje

Iako je u ovom društvu ljudskih slabosti saosjećanje jedina vrlina, ipak je višak samilosti nepoželjan dok boravite na internetu.

Preotimanje Facebook naloga i objavljivanje statusnih poruka sa takvih naloga u kojima vlasnici pozivaju svoje prijatelje u pomoć jer su negdje u nevolji, bio je jedan od najuspešnijih modela internet prevara tokom 2009. godine, a mnogi dobroćudni ljudi su nasjeli na ovakve zahtjeve za pomoći.

Slično je i sa zahtjevima za donacijama lažnim neprofitnim organizacijama koje traže novac za račun pomoći ugroženom stanovništvu neke oblasti koja je pogođena prirodnom katastrofom (zemljotres u Japanu, na primjer).

Brzopletost:

Ruku pod ruku sa molbama koje apeluju na vaše osjećanje samilosti ide i insistiranje da se “djeluje brzo” jer “vrijeme ističe”.

Šta god neko na internetu zahteva od vas, vi zahtjevajte vrijeme potrebno da dobro razmislite.

Održavanje IS

Djelovanje ljudi ili prirode može da prouzrokuje odstupanje u funkcionisanju IS. Važno je, stoga, znati kako obezbjediti neprekidan rad IS i znati šta preduzeti ako sistem doživi slom.
Upravljanje Informacionim Resursima (eng. Information Resources Managment - IRM) obuhvata sve aktivnosti u vezi sa:

- planiranjem,
- organizovanjem,
- sticanjem,
- održavanjem,
- obezbjeđivanjem i
- kontrolisanjem resursa IT.

Resursi IT su veoma raznovrsni i tu spadaju:

- tehnološka sredstva
- kadrovska sredstva
- sredstva veza IT.

Rukovodilac IS i krajnji korisnici

- Organizacija IS može da usvoji jedan od sljedeća četiri pristupa korišćenju računara krajnjih korisnika:
  - Da ih pusti da potonu ili isplivaju
  - Da koristi štap
  - Da koristi šargarepu
  - Da ponudi podršku.

Ranjivost IS i računarski kriminal

Ključni termini u ovoj oblasti:

- **Kopija** - kopija podataka ili programa koji se čuvaju na obezbjeđenom mjestu
- **Dešifrovanje** - transformacija šifrovanog koda u čitljivu informaciju
- **Šifrovanje** - transformacija podatka u šifrovani kod prije slanja
- **Izloženost** - šteta, gubitak ili oštećenje koje može nastati ako nešto pođe kako netreba u IS
- **Tolerancija na greške** - sposobnost IS da nastavi da funkcioniše kada dođe do greške
- **Mjere za zaštitu IS** - procedure, uređaji ili softver koji pokušavaju da obezbjede da sistem funkcioniše kako treba.

Ranjivost IS i računarski kriminal

Ključni termini u ovoj oblasti:

- **Tačnost i pristupačnost podataka** - garancija tačnosti, potpunosti i pouzdanosti podataka uvijek u toku rada IS
- **Rizik** - vjerovatnoća da će se ostvariti pretnja napada na IS
- **Pretnje (ili opasnosti)** - razne opsnosti kojima je IS izložen
- **Ranjivost** - pod uslovom da postoji opasnost, osjetljivost sistema na oštećenja koja pretnja izaziva.

Ranjivost IS i računarski kriminal

Sve veći problem i ograničavajući faktor razvoja i primjena računarskih sistema postaje bezbjednost informacionih sistema.

U poslovnim informacionim sistemima računarske konfiguracije su veoma različite, te se u jednom poslovnom sistemu mogu koristiti:

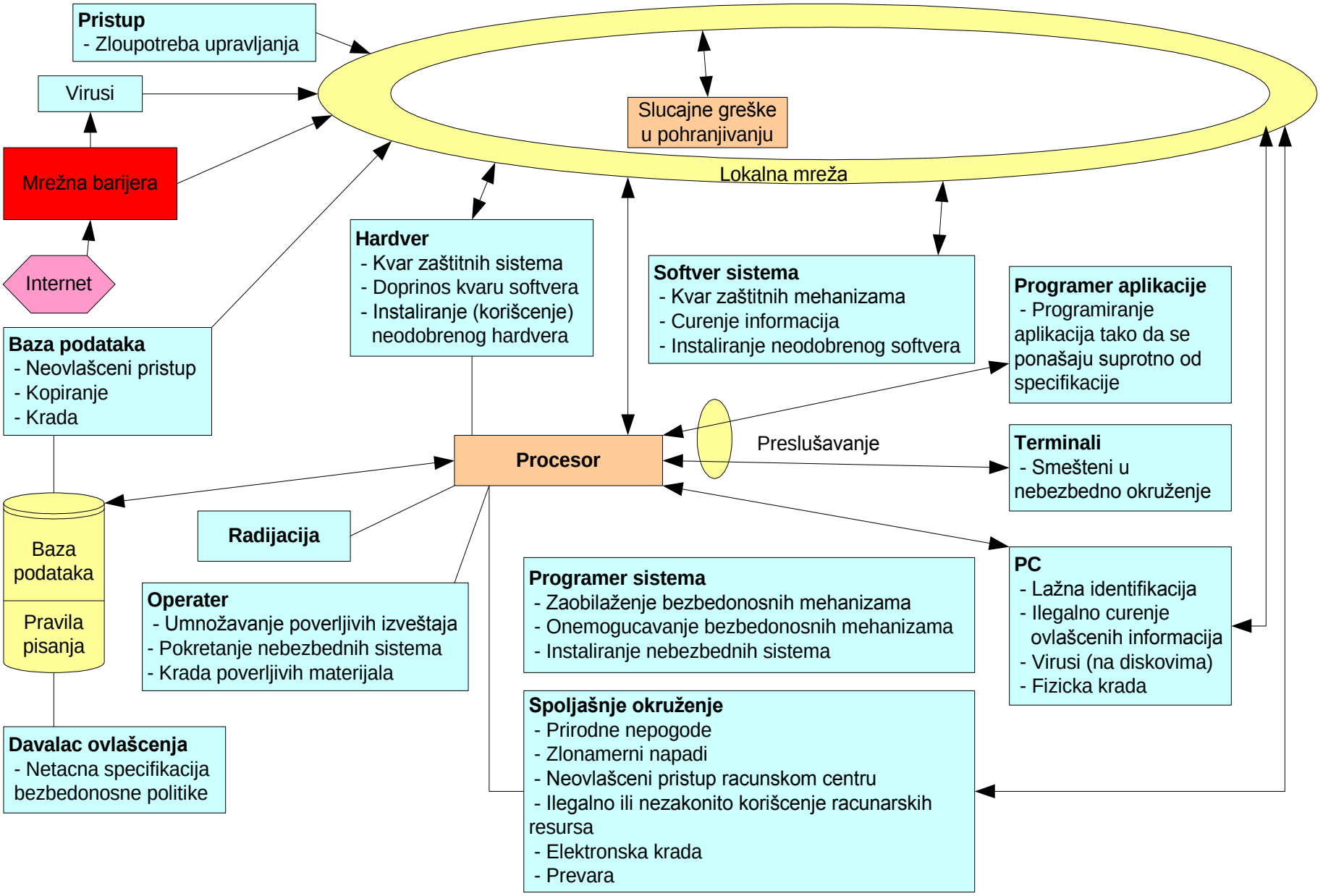
- Veliki računari za centralnu obradu
- Manji računari za decentralizovano prikupljanje i obradu podataka
- Personalni računari za automatizaciju kancelarijskog poslovanja

Ranjivost IS

Rizici koji prijete jednom računskom sistemu su:

- **Kompjuterski kriminal**
- **Sabotaža**
- **Špijunaža**
- **Nedovoljna čistoća u prostorijama u kojima su smješteni računari**
- **Slučajno ili namjerno kvarenje računarskih sistema**
- **Razne vremenske nepogode**

Pretnje bezbednosti



Ranjivost IS

Ranjivost IS se povećava prelaskom na umrežene računarske sisteme.

Opasnosti se mogu podjeliti na dvije grupe:

- **Nenamjerne opasnosti**
- **Namjerne opasnosti**

Ranjivost IS nastavak

Nenamjerne opasnosti:

- **ljudske greške**
- **opasnosti okruženja/sredine**
- **kvarovi računarskih sistema**

Ranjivost IS

Namjerne opasnosti :

- krađa podataka
- neodgovarajuća upotreba podataka
- krađa opreme ili programa
- namjerna manipulacija u rukovanju, unosu, obradi, prenosu ili programiranju podataka
- štrajkovi radnika
- nemiri ili sabotaža
- zlonamjerno oštećenje računarskih resursa
- uništavanje virusima
- razne računarske zloupotrebe i kriminal

S obzirom na svoju prirodu kompjuterski kriminal vrlo brzo nakon svoje pojave dobija karakter međunarodnog kriminala što zahtjeva i organizovanje međunarodne saradnje na planu njegovog suzbijanja. U tom smislu od značaja je i donošenje međunarodnih akta među kojima su:

- **Preporuka Saveta Evrope o kriminalitetu vezanom za kompjutere (1989.)**
- **Rezolucija UN o kompjuterskom kriminalu (1990.)**
- **Rezolucija Međunarodnog udruzenja za krivično pravo (1992.)**
- **Preporuka Saveta Evrope vezana za informacionu tehnologiju (1995.)**

U dopunama ***Krivičnog zakona Srbije*** početkom 2003. godine uvedeno je niz potpuno novih inkriminacija posebno u oblasti zaštite

kompjuterskih programa,

Internet mreže i protokola podataka,

bezbjednosti podataka na Mreži,

hakerskih upada i

raznih zloupotreba...

Izvodi iz Krivičnog zakona Srbije

Kompjuterski kriminal i autorska prava

U ovu oblast spadaju slijedeća krivična djela:

- neovlašćeno korišćenje računara i računarske mreže (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)
- računarska sabotaža (minimalna kazna – **1 godina,** maksimalna – **8 godina zatvora**)
- pravljenje i unošenje virusa (minimalna kazna – **novčana**, maksimalna – **3 godine zatvora**)
- računarska prevara (minimalna kazna – **6 meseci**, maksimalna – **12 godina zatvora**)

- ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)
- neovlašćen pristup zaštićenom računaru ili računarskoj mreži (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)
- sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (minimalna kazna – **novčana**, maksimalna – **3 godine zatvora**)
- neovlašćeno korišćenje autorskog i drugo srodnog prava (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)

Podvale u programiranju
Metode napada na računarske sisteme

- Virus
- Crv
- Trojanski konj
- Sečenje salame
- Superubijanje
- Tajna vrata
- Logička bomba
- Odbijanje usluga
- Njuškavac
- Podvala
- Drobilica lozinki
- Ratni pozivi
- Pomoćna vrata

Virusi – najčuvenija metoda napada

Virus je najčuvenija metoda napada, a dobila je ime po sposobnosti programa da se prikači "inficira" za druge računarske programe navodeći ih da i sami stvaraju viruse. Virus može da se širi kroz računarski sistem veoma brzo.

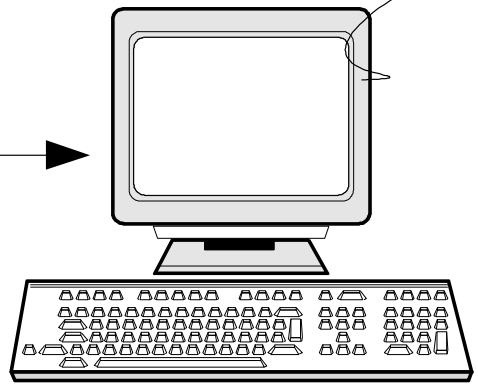
Kada se virus učvrsti u legitimni softverski program, program postaje inficiran, a da vlsnik programa nije svjestan infekcije. Kada se softver koristi, virus se širi oštećujući taj program, a možda i druge. Tako legitimni softver djeluje kao ***trojanski konj***.

Struktura virusa

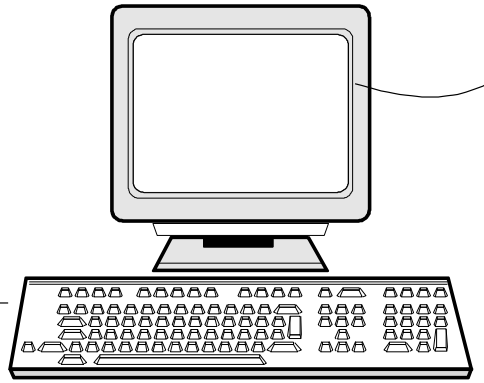
1. Obavezna komponenta
2. Nosiva komponenta (*payload*)
3. Funkcija za okidanje

Kako se širi računarski virus

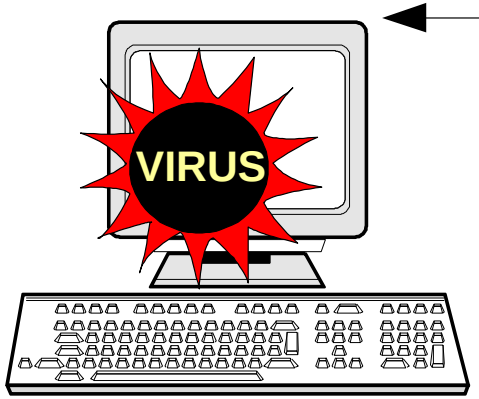
Baš kao što biološki virus remeti žive celije I tako prouzrokuje bolest, racunarski virus - zlonamerno unesen - ulazi u unutrašnjost racunara i remeti normalan rad mašine.



2) Virus se ucvršcuje I putuje gde god putuje program-domacin ili podatak, bilo na disketu, u lokalne mreže ili na elektronske oglasne table



1) Virus nastaje kada programer napiše program koji se smešta u program domacina



3) Virus se aktivira nakon nekog vremenskog perioda ili odredenim okolnostima, npr. Kao posledica nekih racunarskih operacija koje izvrši korisnik. Zatim obavi ono što je programer virusa nameravao - npr. odštampa neku poruku ili izbriše neke podatke.

Virusi –

Danas postoji veliki broj raznih virusa. Ovaj broj se kreće do 70.000, a mjesečno se u prosjeku pojavi oko 100-150 novih virusa.

Pritom nijedan antivirusni program neće detektovati apsolutno sve viruse.

Metode napada na računarske sisteme

Crvi za razliku od virusa nemaju prvu obaveznu komponentu , tj. ne inficiraju druge programe, već se šire mrežom i to najčešće preko elektronske poste.

Trojanski konj se za razliku od crva i virusa ne širi sam već je za to potrebno da korisnik vrši kopiranje na drugi računar. Oni su često destruktivni i mogu ukrasti informacije sa računara.

Virusna infekcija bankomata

Bankomati dve američke banke, koji su bili temeljeni na operativnom sistemu Windows-a, pogođeni su crvom Nachi. To je prva do sada poznata virusna infekcija, koja je pogodila bankomate.

Da li ima virusa za štampače?

Zaštita IS

Odbrambene strategije. Kako se zaštititi?

- Sprečavanje i odvraćanje
- Otkrivanje
- Ograničavanje
- Obnova
- Ispravka

Zaštita IS

Tehničke mjere obuhvataju zaštitu hardvera, softvera, prenosa i obrade podataka.

Mogu se podjeliti na:

- Fizičke
- Mjere zaštite u računarskom sistemu

Fizička zaštita treba da obezbjedi zaštitu

- Neispravnih instalacija
- Požara
- Poplava
- Zagađene okoline
- Štetnih zračenja
- Neurednog napajanja električnom energijom
- Nepovoljnih klimatskih i temperaturnih uslova
- Elementarnih nepogoda
- Fizička krađa opreme

Sredstva za kontrolu pristupa

Kontrola pristupa je onemogućavanje neovlašćenog pristupa korisnika djelu računarskog sistema ili čak čitavom sistemu.

Pristup računarskom sistemu se sastoji od 3 koraka:

- Fizičkog pristupa terminalu
- pristupa sistemu
- Pristupa konkretnim komandama, transakcijama, privilegijama, programima i podacima u okviru sistema

Autentifikacija i lozinke

Autentifikacija može biti zasnovana:

- Na nečemu što znate
  - Npr., lozinke
- Na nečemu što imate
  - Npr., smart kartica
- Na osnovu nečega što **jeste**
  - Npr., otisak prsta, mrežnjača oka ...

Nešto što znate

- Šta može da bude lozinka!
  - PIN
  - Matični broj
  - Majčino djevojačko prezime
  - Datum rođenja
  - Ime vašeg kućnog ljubimca, itd.

Zašto lozinke?

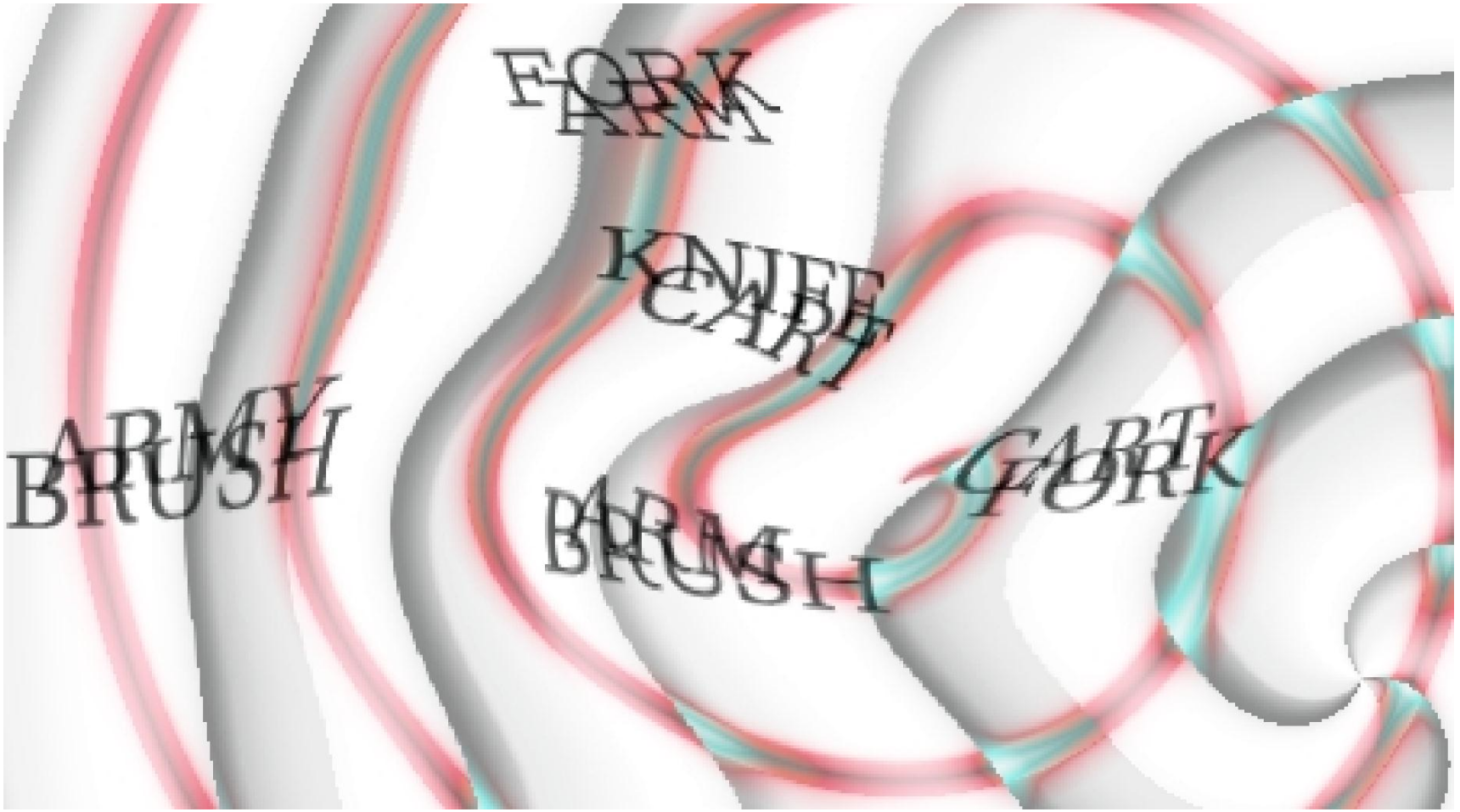
- Zašto je “nešto što znam” popularnije od “nečeg što imam” i “nečeg što jesam”?
- **Cjena**: lozinke su besplatne
- **Pogodnost**: jednostavnije je resetovati lozinke nego izdati korisniku novi otisak prsta

CAPTCHA

Completely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part -
Potpuno automatizivani javni Tjuringov test za razlikovanje čoveka od računara

Da li CAPTCHAs postoji?

Test: Naći 2 iste riječi u ponuđenoj slici



- Lako za većinu ljudi
- Teško za računare (OCR problem)

Biometrijska kontrolna sredstava

- Fotografija lica
- Otisci prstiju
- Geometrija šake
- Skeniranje dužice oka
- Šara krvnih sudova u mrežnjači oka
- Glas
- Potpis
- Dinamika udara na tastaturu
- Termografija lica

- Ekstr
  mem
- Radi

ANTIVIRUS PROGRAMI

Srećom, infekcije računarskim virusima, crvima ili trojancima mogu se spriječiti, a posljedice njihovog dejstva ublažiti ili potpuno sanirati primjenom kvalitetnog **antivirus programa**.

ANTIVIRUS PROGRAMI

Postoje dva smjera razvoja pretraživanja antivirusnih programa:

1. Generički
2. Specifičan za pojedine viruse

Danasnji antivirus programi koriste obadvije metode u cilju prepoznavanja malicioznih programa.

ANTIVIRUS PROGRAMI

Generičko pretraživanje se vrši traženjem određenih "osobina" virusa. Ovako se ne može identifikovati virus već samo generička maliciozna aktivnost.

ANTIVIRUS PROGRAMI

Pretraživanje specifično za pojedine viruse

se vrši tako što se u datoteci koja se pregleda traži određeni potpis koji ukazuje na virus. Ali ovako se ne može detektovati novi virus, već samo oni čiji se potpisi nalaze u internoj bazi.

ANTIVIRUS PROGRAMI

Pretraživanje virusa antivirus programom se može vršiti na dva načina:

-U stvarnom vremenu-vrši se provjera svake datoteke prije njenog izvršavanja

- Na zahtjev korisnika-pregleda hard disk

ANTIVIRUS PROGRAMI

Kvalitet antivirusnog programa se ocenjuje na osnovu:

- Brzine skeniranja
- Sposobnosti da otkrije viruse
- Lakoća instalacije
- Konfigurisanja i azuriranja liste potpisa poznatih virusa

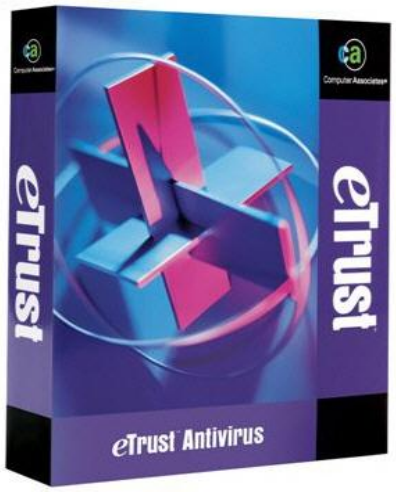
Antivirusni programi sprečavaju zarazu tako što skeniraju fajlove koji su pokrenuti u potrazi za kodom koji bi odao prisustvo virusa.

Ukoliko ga nađu zabrane pokretanje zaraženog programa.

Već zaražene fajlove čiste tako što unutar zarazenog fajla brišu kod za koji su sigrurni da je virus.

Ako ste zaraženi nekim novim virusom o kome ne postoji podatak u internoj bazi vašeg antivirusnog programa on neće otkriti ništa ili će ga otkriti kao “mogući virus” koji neće uspjeti da očisti jer ne razlikuje ostatak koda od pravog programa u koji se ugnjezdio virus.

ANTIVIRUS PROGRAMI

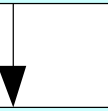


Obezbjeđenje Weba i interneta

-Bezbjedonosne mjere
-Mrežna barijera (Firewall)

Upravljanje rizikom

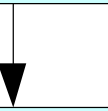
Korak 1. Procena imovine (sredstava)
Utvrđivanje vrednosti I značaja imovine kao što su podaci, hardver, softver I mreže.



Korak 2. Ranjivost imovine (sredstava)
Registrovanje slabosti u postojećem zaštitnom sistemu u pogledu potencijalnih opasnosti.

Korak 3. Analiza gubitaka
Provena verovatnoće nastanka štete i specifikacija opipljivih i neopipljivih gubitaka.

Korak 4. Analiza zaštite
Opis postojećih kontrolnih sredstava koje treba razmotriti, verovatnoće uspešne odbrane uz njihovu pomoć i troškova.



Korak 5. Analiza odnosa troškova i koristi
Upoređivanje troškova i koristi. Razmatranje verovatnoće da dođe do štete i uspešne zaštite od štete. I na kraju, donošenje odluke koje zaštitne mere instalirati.

Pitanja upravljanja

- **Programi za jačanje svijesti o bezbjednosti sistema su važni za svaku organizaciju, posebno ako je jako zavisna od IT.** Ovakvi programi trebalo bi da postoje na nivou korporacije i to uz podršku višeg rukovodstva. Pored toga, praćenje bezbjedonosnih mjera i obezbjeđenje pridržavanja administarativnih kontrolnih sredstava su bitni za uspješnost plana obezbjeđenja.

- **Kontrola IS treba da bude institucionalizovana i ugrađena u organizacionu kulturu.** Potrebno je da organizacije kontrolišu IS ne zato što to zahtjeva osiguravajuća kompanija, već time što mogu da uštede znatne sume novca i sačuvaju kompaniju od propadanja.