Fizična zaščita

Uvod

- Zaščita, ki se izvede izven računalniškega sistema za "obrambo" pred:
  - naravnimi nesrečami
  - vsiljivci
  - nepooblaščenimi dostopi

Naravne nesreče

- ni jih možno napovedati
  - voda
    - poplave
    - deževje
  - potresi
  - ogenj

Naravne nesreče: voda

- *"naraščajoča voda"* - blato, ostanki, ruševine, odpadna voda
- *"padajoča voda"* - uničenje naprav, izpad razsvetljave, uničenje (zrušitev) stropov, prekomerna vlaga
- nasveti za zaščito:
  - poplave lahko povzroči dež, sneg, ki se topi, počena cev, voda za gašenje
  - namestitev senzorjev za vodo je pričakovana
  - namestitev računalniških centrov v višja nadstropja
  - ob začetku "poplavljanja" zaključitev dela na sistemu in umik opreme (če je možno) oz. zaščita opreme
  - umik magnetnih trakov in podatkov
  - mokre računalnike je potrebno posušiti

Naravne nesreče: potresi

- nasveti za zaščito:
  - namestitev računalnikov daleč od oken
  - v "ogroženih" področjih namestitev računalniške opreme (centra) v nižja nadstropja
  - postavitev "lahko" gibljivih objektov na oddaljeno mesto

Naravne nesreče: ogenj

- praviloma nevarnejši kot voda
- nasveti za zaščito:
  - namestitev detektorjev dima
  - prostori računalniških centrov naj bodo ognjevarni:
    - prostori brez oken
    - protipožarna vrata
  - gasilski aparati na prah (voda lahko povzroči še več škode) morajo biti v prostorih računalniškega centra ali v neposredni bližini
  - za primer požara mora biti izdelan varnostni načrt, ki ga je potrebno večkrat preveriti
  - ljudi je potrebno naučiti za uporabo omenjenega načrta
  - kajenje na področju računalniškega centra ni dovoljeno
  - ob požaru po možnosti zaključiti delo na sistemu in odstraniti opremo oz. podatke

Naravne nesreče: ogenj

- zaščitna oprema
  - izguba 25 milijonov delovnih dni za ponovno vzpostavitev sistema
  - 50% “požganih” podjetij gre v stečaj
  - stroški za ponovno vzpostavitev sistema so izredno visoki (osebni računalnik: $2000-$8000 za megabajt podatkov)
  - mediji za shranjevanje podatkov vzdržijo okoli 45°C
  - v notranjosti varnostnih sefov je po eni uri požara okoli 55°C
  - priporočljiva uporaba ognjevarnih posod (podatkovni sef) za prenos medijev (po eni uri požara, ki razvije temperaturo 930°C, so podatki še vedno varni)

Naravne nesreče: ogenj

- požarna zaščita v računalniških centrih:
  - 60% pregledanih centrov je popolnoma nezaščitenih
  - 90% preostalih se ni zavedalo, da lahko magnetni mediji zgorijo

Naravne nesreče: pogoste napake

UGOTOVLJENE SLABOSTI RAČUNALNIŠKIH CENTROV	% POGOSTOSTI
RC se nahaja ob zunanji steni z velikimi okni	62
RC je prepoznaven od zunaj, včasih celo označen	54
RC oz. PB nista požarno zaščitena	49
blizu RC (prostor zgoraj, spodaj, levo, desno) se skladiščijo lahko vnetljivi materiali	57
notranja oprema RC je iz lesa ali plastike	79
kabelska napeljava (razdelilne doze v stenah) in prezračevalni jaški niso zaščiteni pred zunanjim ognjem	58
odpadni papir in ostali nevarni materiali se shranjujejo v RC blizu podatkovnih shramb	51

Naravne nesreče: pogoste napake

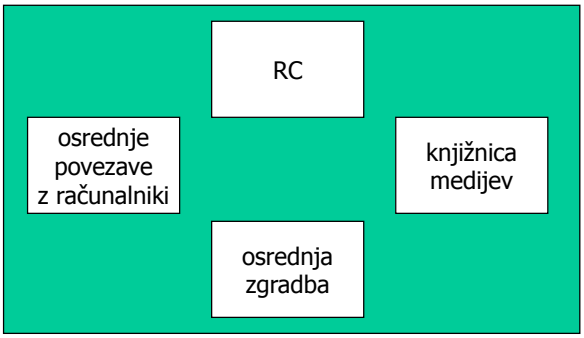
UGOTOVLJENE SLABOSTI RAČUNALNIŠKIH CENTROV	% POGOSTOSTI
napačno postavljeni detektorji ognja	38
alarm za ogenj se v RC ne sliši	54
avtomatični gasilni aparati so prestavljeni iz "avtomatično" na "ročno"	43
prezračevalni sistem se v primeru požara izključi prepozno ali pa se sploh ne	59
PB se nahaja v sobi brez posebne (dodatne) požarne zaščite	81
v primeru požara ni dodatne zaščite pred vlago, ki jo povzroča požar; ni dodatne zaščite pred kislimi dimi	76
v prostoru za arhiv podatkov se nahajajo neprimerne električne ali celo vodovodne napeljave	53

Izgradnja fizično primerno zaščitenega računalniškega centra

- nekoč:
  - računalniški center je bil en prostor, ki ga je bilo enostavno nadzorovati
- danes:
  - ob računalniškem centru, ki se nahaja v podjetju, obstaja še ogromno dodatne opreme, ki jo je potrebno zaščititi
- izbor fizične lokacije:
  - računalniški center naj bo nameščen izven "prometnih" poti v osrednji zgradbi
  - prostori RC naj ne bodo ob zunanjih stenah in oknih
  - zagotoviti je potrebno varovanje prostora (varnostno zaklepanje) in nadzorovati dostop do prostora
  - električna in prezračevalne (klimatske) napeljave naj bodo za RC ločene

Izgradnja fizično primerno zaščitenega računalniškega centra

- priporočljive lokacije različnih delov računalniškega centra



Priporočila lokacijo (prostore) RC

- RC naj ne bo v bližini plinskih postaj, letališč, garaž, kemičnih skladišč in energetskih sistemov
- RC naj ne bo v bližini industrije, ki “proizvaja” prašne delce
- RC naj bo na lokaciji, kjer ga iz različnih vzrokov ali v kateremkoli obdobju ne more poplaviti
- RC naj ne bo ob glavnih “prometnih” poteh in zunanjih zidovih
- dostop do in v RC naj bo omejen samo na ljudi, ki takšen dostop potrebujejo
- prostor z računalniki naj bo zaščiten pred vdori vode; za morebitne vdore naj ima primeren hiter iztok

Temperatura

- problemi
  - računalniški sistemi so temperaturno občutljivi
  - z naraščanjem temperature postajajo nekatere komponente nepredvidljive
- rešitve
  - ob izpadu hlajenja računalniški sistem izklopimo (neželena rešitev)
  - RC naj uporablja lastno klimatsko napravo
  - ob naraščanju temperature naj bodo klimatske naprave sposobne vzdrževati primerno delovno temperaturo
  - klimatski sistem centra naj bo povezan s požarnimi detektorji

Električna energija

- problemi
  - izpad električne energije negativno vpliva na delovanje računalniškega sistema
  - neželeni so nihanje napetosti in sunki napetosti
- rešitve
  - uporaba stalnega vira energije (generatorja), ki loči računalniški sistem in/ali center od ostalega napajanja v primeru izpada
  - uporaba dodatnega vira energije za minimalno osvetlitev delovnih področij, klimatskih naprav, vodnih črpalk in vsaj enega dvigala
  - računalniški sistemi naj bodo opremljeni z učinkovitimi filtri in/ali zaščitami za prestrezanje in ublažitev sunkov oz. nihanj napetosti

Električna energija

- rešitve
  - na razpolago naj bodo posebne baterije za razsvetljavo za primer popolnega izpada in izvajanje nujnih operacij
  - v primeru strele izklopimo vse računalniške sisteme in ostale naprave pod električno napetostjo
  - za zaščito pred strelo instaliramo ustrezno zaščito
  - V RC uporabimo antistatični pod (tla)

Vsiljivci

- nepooblaščeni obiskovalci lahko povzročijo:
  - krajo opreme ali podatkov
  - poškodbo opreme
  - kršitev tajnosti (vpogled v občutljive podatke)

Vsiljivci: kraja

- predmeti, primerni za krajo:
  - računalniki - predvsem prenosniki
  - prenosni mediji - enostavno odtujljivi
  - poročila
- zaščita:
  - omejitev in nadzor dostopa
  - omejena prenosljivost
  - detekcija izhoda

Vsiljivci: kraja

- OMEJITEV IN NADZOR DOSTOPA
  - čuvaj (vratar, receptor) - najstarejši način varovanja - 24 ur na dan, 7 dni na teden
    - oprema: kamere, monitorji, direktna povezava s policijo in gasilci
    - uspešnost: NE VEDNO (preverjanje ljudi)
  - ključavnica - drugi najstarejši način varovanja.
    - oprema: enostavna in poceni
    - uspešnost: NE VEDNO (dvojniki, izgubljeni ključi)

Vsiljivci: kraja

- OMEJENA PRENOSLJIVOST
  - zaklepanje prostorov (omejena učinkovitost)
  - teža predmeta (omejena učinkovitost)
  - lepljenje, priklepanje (omejena učinkovitost)
  - dodatne ključavnice
  - verige in kabli
  - kletke
- DETEKCIJA IZHODA
  - zaščita prenosnih komponent kot pri knjigah, prenosnih medijih

Vsiljivci: kraja

- na tržišču obstaja široka paleta produktov




Vsiljivci: poškodba opreme

- najrazličnejše možnosti na najrazličnejših nivojih in opremi
- tipi poškodb:
  - namerna - vsiljivci, zaposleni
  - nenamerna - zaposleni

Vsiljivci: kršitev zaupnosti

- vpogled v občutljive podatke
- učinkovit nadzor dostopa
- uničenje podatkov na različnih medijih

Vsiljivci: kršitev zaupnosti

- uničenje podatkov na različnih medijih
  - stroji za uničenje podatkov na različnih medijih (razrez v različne oblike, sprememba agregatnega stanja, sežig medijev - standardi okolja)
  - prepis magnetnih prenosnih medijev z različnimi vzorci
    - ERASE ali DELETE nista dovolj učinkovita
  - uničenje zapisov na magnetnih medijih in priprava za ponovno uporabo
  - naprave, ki ne oddajajo informacij
    - Tempest - certificiranje orodij

Pooblaščen in nepooblaščen dostop

- Pooblaščen dostop do računalniškega centra, opreme in podatkov je eden najučinkovitejših in najzahtevnejših načinov fizičnega varovanja
- priporočila za načrt nadzorovanja dostopa :
  - vstop v RC je dovoljen le zaposlenim, ki ta dostop potrebujejo za opravljanje svojega dela
  - uprava naj vodi formalno politiko dostopa do centra:
    - vstop za zaposlene ni avtomatizem (prva točka)
    - nadzor vstopa s kamero in vrati, ki se odpirajo le v eno smer ob uporabi ustreznega "ključa"

Pooblaščen in nepooblaščen dostop

- Priporočila za načrt nadzorovanja dostopa:
  - predstavniki podjetij, obiskovalci in drugi zaposleni naj se:
    - pred vstopom identificirajo
    - nosijo ustrezen znak
    - vpišejo v knjigo gostov dan, uro in namen obiska
    - v RC gibljejo v spremstvu zaposlenega iz RC
  - pošta in oprema se ne dostavljajo direktno v RC
  - identifikacijske kartice so obvezne za vse zaposlene

Pooblaščen in nepooblaščen dostop

- možni ključi za vstop v RC
  - magnetna kartica ali magnetni ključ
    - problem kraje -> dodatno geslo
  - pametna kartica oz. žeton (npr. “kalkulator”)
    - kartica z vgrajenim mikročipom in pomnilnikom
    - natančno definirana pooblastila in prepovedi
    - nadomestilo za čuvaja (vratarja - receptorja)
    - dodatna zaščita

Pooblaščen in nepooblaščen dostop

- možni ključi za vstop v RC
  - biometrične naprave
    - zagotavljajo večjo varnost
    - fiziološke - analizirajo karakteristike posameznika
      - pregled oči (identifikacijska koda temelji na preverbi celotnega očesa. Zahtevana je vsaj 70% pokritost s shranjenim vzorcem)
      - prstni odtis (identifikacijska koda je povezana z obliko prstnega odtisa - problemi z umazanijo, vrezninami, porezanimi-neporezanimi nohti)
      - geometrija roke (temelji na dolžini prstov, velikosti dlani in prosojnosti kože - vsi parametri predstavljajo kodo dostopa)

Pooblaščen in nepooblaščen dostop

- možni ključi za vstop v RC
  - biometrične naprave
    - vedenjske- analizirajo karakteristike, ki se nanašajo na obnašanje
      - razpoznavanje glasu (zapiše se digitalna slika glasu posameznika; uporablja se lahko tudi za zaklepanje naprav in ne le vrat)
      - razpoznavanje podpisa (uporabljata se posebna podloga in pisalo za verifikacijo podpisa. Identifikacijo sestavljajo hitrost podpisa, pritisk pri podpisu, hitrost pri zapisu črtice na t oz. pike na i)
      - razpoznavanje vzorcev tipkanja (na osnovi določenih skupin črk ugotavljamo - spoznavamo pisca)

Hiter pregled komponent fizičnega varovanja

- mehanizmi identifikacije
- kontrola vstopa
- obhodi varnostnikov
- nadzor s kamerami
- "knjižnična" kontrola
- alarmne naprave
- detektorji požara in avtomatski gasilni sistemi
- direktna povezava s policijo/gasilci
- javni naslov
- evakuacijski načrt in načrt ponovne vzpostavitve sistema

Hiter pregled komponent fizičnega varovanja

- varnostne kopije na ločenem sistemu
- postavitev računalniških prostorov izven "prometnih" poti
- postavitev računalnikov na notranje stene in ne blizu oken
- ločeno napajanje, gretje in hlajenje od ostalih prostorov
- seznanitev vzdrževalcev in čuvajev (receptorjev, vratarjev) s pomenom računalniških sistemov
- namestitev RC izven nevarnih mest (letališča, reke, skladišč kemičnih snovi)
- RC naj ne bo dobro označen
- strop in stene RC naj bodo vodotesni

Hiter pregled komponent fizičnega varovanja

- v RC naj bodo odtoki večji, obstajajo naj detektorji nivoja vode
- izdelava ločenega načrta v primeru požara
- prepoved kajenja, pitja in prehranjevanja ob računalnikih in v RC
- namestiti negorljive materiale v RC
- namestitev nelomljivih stekel
- namestiti veliko gasilnih aparatov v RC
- jasno označiti glavna stikala

Hiter pregled komponent fizičnega varovanja

- redno testirati detektorje ognja in alarme
- namestiti jeklenke s kisikom v RC
- omejiti dostop do RC; dovoliti le pooblaščenim
- namestiti varnostnika pri vseh vhodih v RC
- pregledati vse pošiljke, pakete in večjo pošto pred vnosom v RC

- redno izdelovati varnostne kopije in jih shranjevati na ločenih, prav tako varovanih mestih

Biometrične zaščitne naprave

Biometrične zaščitne naprave

- izkoriščajo človeške značilnosti za identifikacijo in verifikacijo oseb:
  - fizične karakteristike
  - vedenje karakteristike
- FAR (False Acceptance Rate) - verjetnost uspešne identifikacije neavtoriziranega uporabnika
- FRR (False Rejection Rate) - verjetnost neuspešne identifikacije avtoriziranega uporabnika

Biometrične zaščitne naprave: delovanje

- zajem podatkov
- identifikacija lastnosti
- izdelava predloge (template)
- shranjevanje ali primerjava

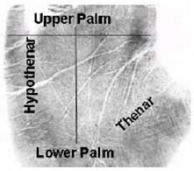
Biometrični podatki

- so običajno zapisani v obliki karakteristik ali predlog
- iz takšnih karakteristik je teoretično možno rekonstruirati izvor
- "preklicni" biometrični podatki
  - izvorna slika se pred obdelavo popači
  - vsak lahko izdela svoj način popačenja
  - v primeru razkritja podatkov zamenjamo algoritem popačenja

Varnost biometričnih podatkov

- shranjuje se lahko le predloga (template)
- teoretično se predloga izračuna na podlagi enosmerne funkcije
- v praksi vsi algoritmi zastarijo
  - spomnimo se zgoščevalnih funkcij
- Kako naj zamenjamo svoje lastnosti? Ali lahko zamenjamo, kdo smo??

Prstni odtis in odtis dlani



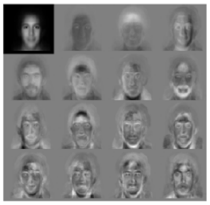
Upper Palm - zgornji del dlani
Lower Palm - spodnji del dlani
Hypothenar - hipotenar
Thenar - tenar

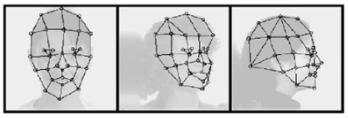
- prepoznavanje preko Minucijev na grebenih povrhnjice
- najbolj razširjena metoda
- obstaja možnost zlorabe

Geometrija roke

- merjenje razdalj med segmenti na človeški roki
- primerna samo za verifikacijo, ker ni dovolj unikatna
- potrebne je nekaj vaje za uporabo

Prepoznava obraza

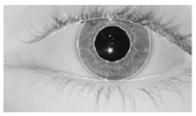




- 3 glavne metode: PCA,LDA,EBGM
- preprosta za izvedbo
- ni potrebe po stiku z napravo
- spremembe položaja obraza in osvetlitev lahko otežijo prepoznavo

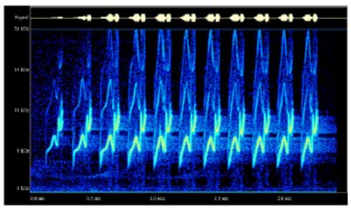
Skeniranje šarenice in mrežnice

- najmlajši metodi
- spadata med najbolj varne nasploh
- povsem unikatni za vsakega človeka
- za skeniranje uporaba infrardeče svetlobe
- neupravičeno nezaupanje ljudi



Prepoznava glasu

- prepoznava značilnosti glasu in ne izgovorjave
- frekvenca, dolžina, jakost, višina, kvaliteta in dinamika tona
- kljub spremembam skozi leta dovolj zanesljivo za verifikacijo



Dinamični podpis

- dinamično zajeta smer, pritisk na podlago, oblika podpisa
- se praktično ne da ponarediti
- skozi čas podvrženo spremembam

Dinamika tipkanja

- pritisk izveden na posamezno tipko
- čas med pritiskom na določeno kombinacijo tipk
- posebne tipkovnice
- kombinacija skupaj z geslom