

<RSA> Sigurnost informacijskih sistema </RSA>

<AES> predavanja </AES>

<CISSP> Fizička sigurnost</CISSP>



Summary

- Planiranje dizajna sigurnosne ustanove
- Dizajniranje programa fizičke sigurnosti



Lekcija 1. Planiranje dizajna sigurnosne ustanove

- Prva linija odbrane
- Prijetnje fizičkoj sigurnosti
- Odgovornost za fizičko stanje

Prva linija odbrane

- Jedan od slojeva unutar slojevitog odbrambenoga modela
- Unutar organizacije fizička sigurnost se sastoji od:
 - Bezbjednosti
 - Sigurnosti
- Hacking i „tehnički“ napad nije jedini način da se ukradu informacije
- Prijetnje fizičkoj sigurnosti:
 - Prirodne prijetnje
 - Sistemi opskrbe
 - Ljudski uzrokovane prijetnje



Prijetnje fizičkoj sigurnosti

- Donn B. Parker „Fighting Computer Crime: A New Framework for Protecting Information (Wiley, 1998)“ je identifikovao sedam izvora potencijalnoga gubitka fizičkih resursa:
 - Temperatura
 - Gasovi
 - Tekućine
 - Živi organizmi
 - Tijela u kretanju
 - Pokreti
 - Energetske anomalije



Odgovornost za fizičko stanje

- Odgovornost je nešto što se obično ostavi u drugi plan
- Svaka akcija vezana za fizičku sigurnost može imati posljedice
- Postoji prostor za parnične postupke i tužbe:
 - Prijava kvara koji kasnije vodi prema narušavanju sigurnosti
 - ATM mašina koji se nalazi u okolini pogodnoj za fizički napad
 - Nedostatak procedura
 - i sl.



Lekcija 2. Dizajniranje programa fizičke sigurnosti

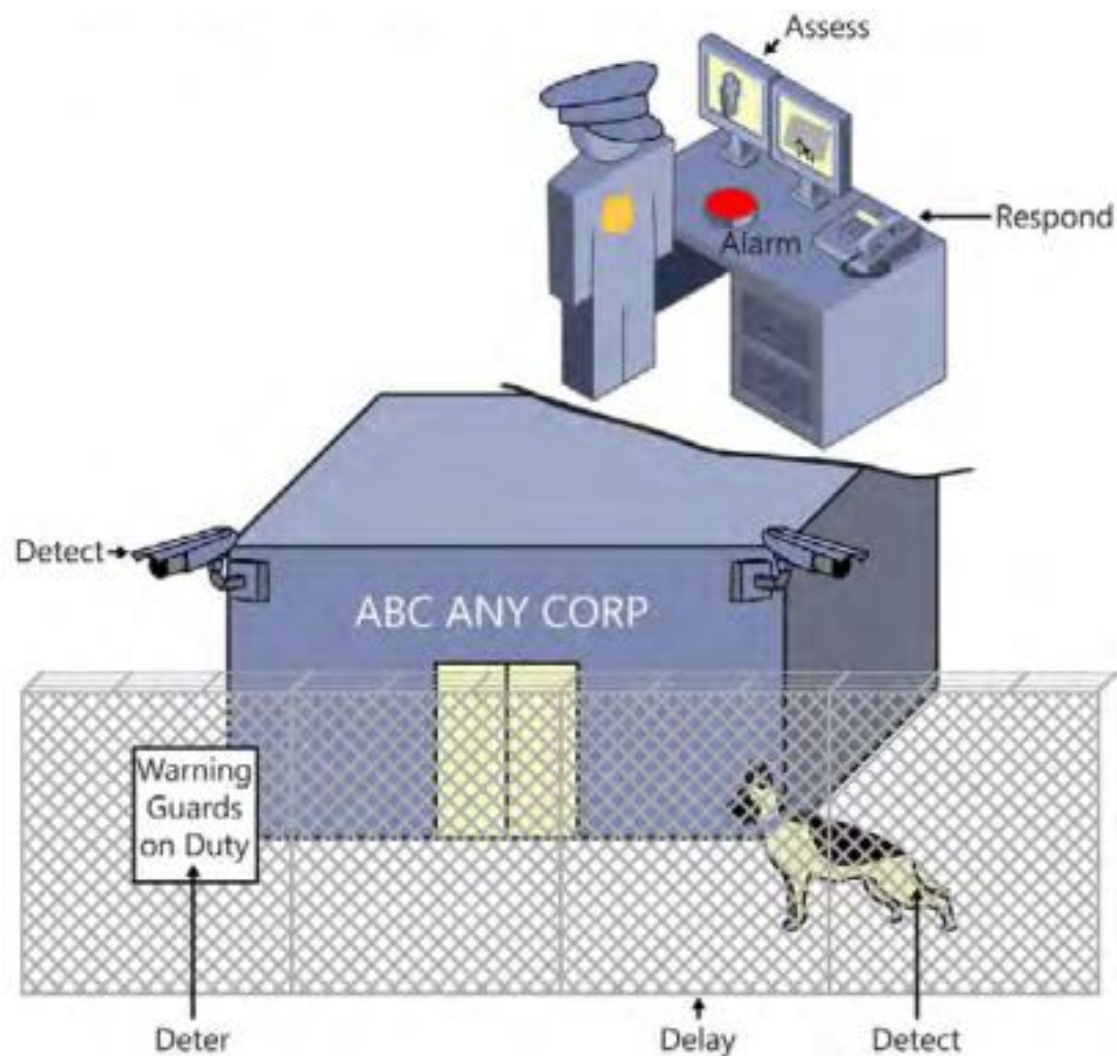
- Proces dizajniranja programa fizičke sigurnosti
- Deter, Delay, Detect, Assess, Respond
- Crime prevention through environmental design (CPTED)
- Target hardening
- Osiguranje prenosnih uređaja
- IDS sistemi
- Ostalo

Proces dizajniranja programa fizičke sigurnosti

- Odabir tima
- Vršenje analize rizika
- Odabir prihvatljivog rizika
- Analiza postojećih kontramjera
- Testiranje novih ili nadogradnja postojećih kontramjera
- Odobrenje menadžmenta
- Monitoring i evaluacija

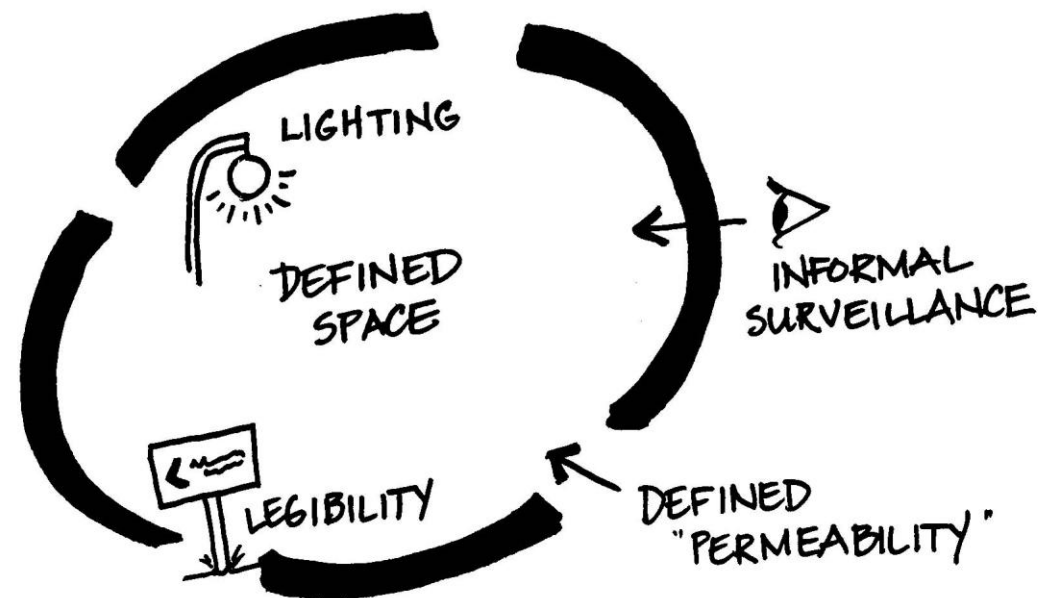


Prekid, Odgoda, Otkrivanje, Procjena, Odgovor



Crime prevention through environmental design (CPTED)

- Metodologija koja pomaže u dizajnu fizičkog okruženja, a sa ciljem reduciranja kriminalnih aktivnosti tako što utiče na ljudsko ponašanje.
- Uvodi psihološke, podsvjesne i vidljive granice kako bi ljudi ostali izvan osiguranog okruženja
 - Arhitektura
 - Lokacija
 - Materijali
 - Sigurne zone
 - Lokacija data centra



Target hardening

- Kombinacija položaja, prirodnih i vještačkih prepreka
 - Zidovi, brisani prostor, drveće i sl.
- Dizajn prozora
 - Standardni, žičani, zatamljeni i sl.
- Vrata
 - Klasična, mehanička, otporna na fizičke uticaje
- Brave
 - Pristup i lokacija ključeva
- Zaštita komunikacija
 - Posebne zone, bijeli šum, Faradejev kavez
- Čuvari
 - Ima svoje prednosti i mane
- Kamere
 - Rezolucija, lokacije i retenetion period
- Obratiti pažnju na „ Piggybacking ili tailgating“



Osiguranje prenosnih uređaja

- Fizičko vezivanje uređaja
- Praćenje uređaja putem adekvatnog softvera
- Brisanja sadržaja usljed različitih razloga
- Prijedlozi:
 - Detaljan inventar laptopa i telefona kod uposlenika
 - OS sa postavkama organizacije
 - BIOS lozinke
 - Enkripcija diska
 - Registracija kod proizvođača
 - Rezevne kopije podataka na stacioniranoj lokacija
 - Kada se ostavlja u automobilu, koristiti prtljažnik (prije dolaska na destinaciju)



IDS sistemi

- Alarmi
- Toplinski senzori
- Detektori pokreta
- Detektori pritiska



Ostalo

- Grijanje
- Ventilacija
- Klimatizacija
- Temperaturni senzori
- Detektori vlage
- Protivpožarni sistemi



Pitanja

