Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

10. UPRAVLJANJE VANREDNIM DOGAĐAJEM I KOMPJUTERSKIM INCIDENTOM

Cilj

- Definisati značaj
- Opisati glavne karakteristike upravljanja vanrednim događajem **(VD)**
- Opisati glavne karakteristike upravljanja kompjuterskim incidentom **(K/I)**

Proces planiranja VD

- Identifkovanje:
  - funkcija IKTS koje su kritične za poslovanje
  - resursa koji podržavaju kritične funkcije IKTS
- Procena potencijalnih VD ili nesreća
- Izbor strategije planiranja VD u IKTS
- Implementacija strategije za upravljanja VD
- Testiranje i revizija strategije za upravljanja VD

Identifkovanje kritičnih funkcija IKTS

- **Definicija kritične misije/poslova org**. - u planu zaštite IKTS
- **Kriterijumi za određivanje kritičnosti mislije:**
  - vreme oporavka sistema i akumulirani uticaj
  - njihova kombinaciji i proceniti promene od uticaja VD
- **Većina poslovnih servisa IKTS dostiže** tačku u kojoj je:
  - uticaj VD velik i bespredmetno je održavanje kontinuiteta
  - potreban oporavak servisa IKTS pre ove tačke
  - vreme postaje kritičan faktor u procesu upravljanja VD
  - potrebna redudantnost (zalihost) za svaki kritični servis/e
  - prioritet - povećati sposobnost org. da preživi VD

Identifikovanje kritičnih resursa IKTS i procena VD

- *Ljudski resursi*
- *IKTS kapaciteti za obradu*
- *Automatizovane apl. i podaci*
- *Servisi bazirani na IKTS*
- *Fizička IKT infrastruktura*
- *Dokumentacija*
  - za razvoj više scenarija, a ne planova za svaki scenario VD

Izbor strategije za upravljanja VD

Svaka sadrži tri dela:

– *hitne intervencije*

– *oporavak sistema*

– *nastavljanje rada*

Ili

– *hitne intervencije*,

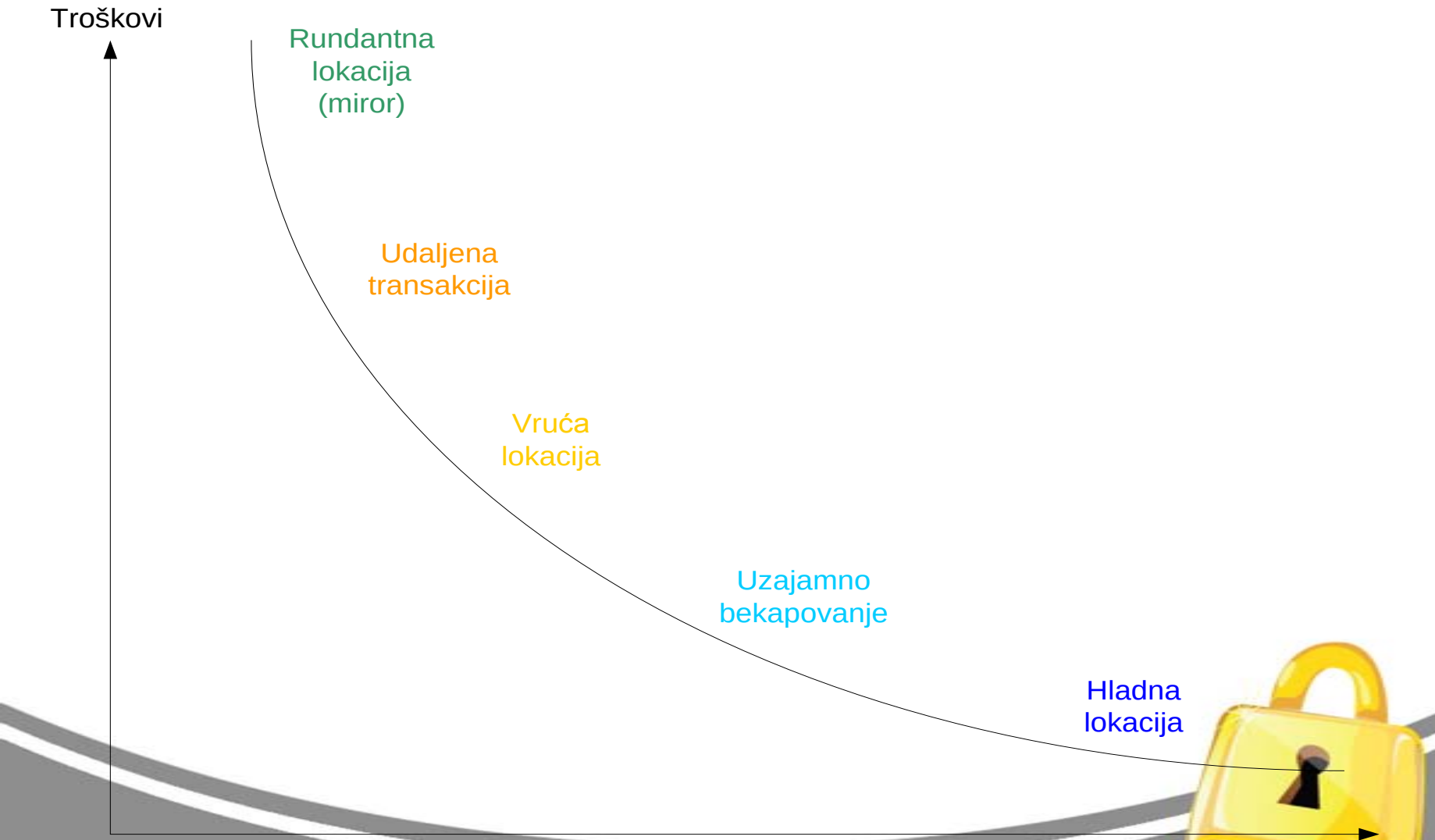
– *bekapovanje*

– *oporavak sistema*

Kapaciteti IKTS za obradu u VD

- *Glavna (primarna) lokacija*
- *Rezervna (hladna) lokacija*
- *Rezervna (vruća) lokacija*
- *Redundantna (miror) lokacija*
- *Recipročni ugovori (uzajamno bekapovanje)*
- *Udaljena (online) iznajmljena transakcija*
- Bilo koja kombinacija *(hibridni sistemi)*
- Osnovni aksiom oporavka IKTS - **bekapovanje**

Bekapovanje $T_o = f(R_l)$



Implementacija strategije za upravljanje VD

1. **Broj scenarija i verzija planova VD**?
2. **Pojedinačna odgovornost za pripremu plana**?
   - strategiju i način impl.-dokumentovati u politici i proced. org.
3. **Za male IKTS:** plan za VD deo plana zaštite IKTS
4. **Za velike IKTS:**
   - plan zaštite – sadrži kratak pregled plana za VD
   - plan za VD poseban dokument

- **Samo jedan plan VD:**
  - kritična koordinacija (menadžera resursa i funkcionalnih)
  - odrediti koordinatora za upravljanje VD
- **Više planova VD**: ispitati i eliminisati preklapanja

Dokumentovanje plana za VD

- **Plan za upravljanje VD treba da bude**:
  - napisan jasno i jednostavno,
  - redovno ažuriran i
  - ažurna kopija plana VD uskladištena na nekoliko sigurnih i dostupnih lokacija

Obuka zaposlenih za VD

- **Svi zaposleni** - da prođu obuku za slučaj VD
- **Novo zaposlene** -obučiti po dolasku u org.
- **Periodično** – uvežbavati uloge u VD
- **Najvažnije**:
  - simulacije prirodnih katastrofa
  - uvežbavanje ponašanja i postupaka zaposlenih za VD
- **Održavanje plana za VD** - ugraditi u procedure za upravljanje promenama u IKTS
- **Hitne intervencije** - posebno važna obuka
  - odgovor treba biti izvežban do automatizma
  - posebno u slučajevima spašavanja ljudskih života

Testiranje, revizija i međuzavisnoasti plana VD

- **Tipovi testiranja***:*
  - *Kontrolni pregled*
  - *Analiza*
  - *Simulacija krizne situacije*
- **Međuzavisnosti:**
  - *Politika zaštite*
  - *Fizička i zaštita od uticaja okruženja*
  - *Upravljanje incidentom*
  - *Operativne kontrole zaštite*

Pregled principa za upravljanje konfiguracijom

Namena:

- dobra inženjerska operativna praksa
- obezbeđuje da sistem funkcioniše kako treba
- da se promene u S/Z odvijaju na poznat/kontrolisan način
- da ne utiču negativno na funkcije sistema ili implementaciju politika zaštite

Proces se zasniva - na četiri osnovna principa:

- *identifikacija,*
- *kontrola promena konfiguracije,*
- *evidencija (registrovanje) stanja konfiguracije i*
- *revizija (auditing) procesa upravljanja konfiguracijom.*

Zahtev za promene konfiguracije

- Odobrava zvanično lice iz organizacije, uključuje hardver, softver, korisnike i osoblje za tehničku podršku IS
- Zahtev za hitne promene odobrava zvanični organ org., pre ili posle same promene
- Izvršene hitne promene konfiguracije dokumentuju se i odobravaju,
- Evidentira se personal za analizu i realizaciju zahteva

Procedure procesa upravljanja konfiguracija (razvijene i dokumentovane)

- *izrada plana za upravljanje promenama konfiguracije,*
- *upravljanje promenama osnovne konfiguracije IKT sistema,*
- *upravljanje promenama u IKT sistemu,*
- *upravljanje promenama servisa za kontrolu pristupa,*
- *monitorisanje promena konfiguracije,*
- *konfigurisanje minimuma servisa,*
- *kontrola i verifikacija bezbedne konfiguracije,*
- *upravljanje konfiguracijom računarske mreže,*
- *politika zaštite privatnosti i*
- *ograničavanje tipova saobraćaja.*

Upravljanje kompjuterskim incidentom

KLJUČNI TERMINI:

- Kompjuterski događaj
- Bezbednosni kompjuterski incident (K/I)
- Indikacije K/I
- Interventni tim
- Kapaciteti za upravljanje K/I
- Digitalna forenzička istraga

Kompjuterski događaj i incident

- **Kompkiterski događaj**:
  - bilo koje uočljivo dešavanje u IS
  - negativni događaj - sa negativnim posledicama
- **Kompjutrski incident (KI) - definicija:**
  - **ranije:** *bezbednosno relevantan događaj koji dovodi do gubitka CIA informacione imovine*
  - **danas**: *povreda ili pretnja za povredu politike zaštite*
  - *KI je simptom, a uzrok je realizovana pretnja (napad)*
- **Upravljanje K/I incidentom:**
  - samo neg. događaj u sistemu zaštite
  - isključuju vanredne negativne događaje

Primeri KI

- maliciozni napad na web server (pad sistema)
- ubačen crv inficira sve radne stanice u LANu
- hakerski napad iskorišćava ranjivost sistema za pristup datoteci pasvorda u serveru
- anonimni korisnik preti drugoj osobi preko e-mail-a
- trojanac na hostu koristi se za neovlašćeni pristup sistemu, *zombiranje* računara
- *rootkit* prikriva prisustvo trojanca ....

Tipična taksonomija kompjuterskog incidenta

INCIDENT

ATTACK(S)

EVENT

Attackers	Tool	Vulnerability	Action	Target	Unauthorized Results	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonoumous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

Prednosti i nedostaci taksonomije incidenta

PROS

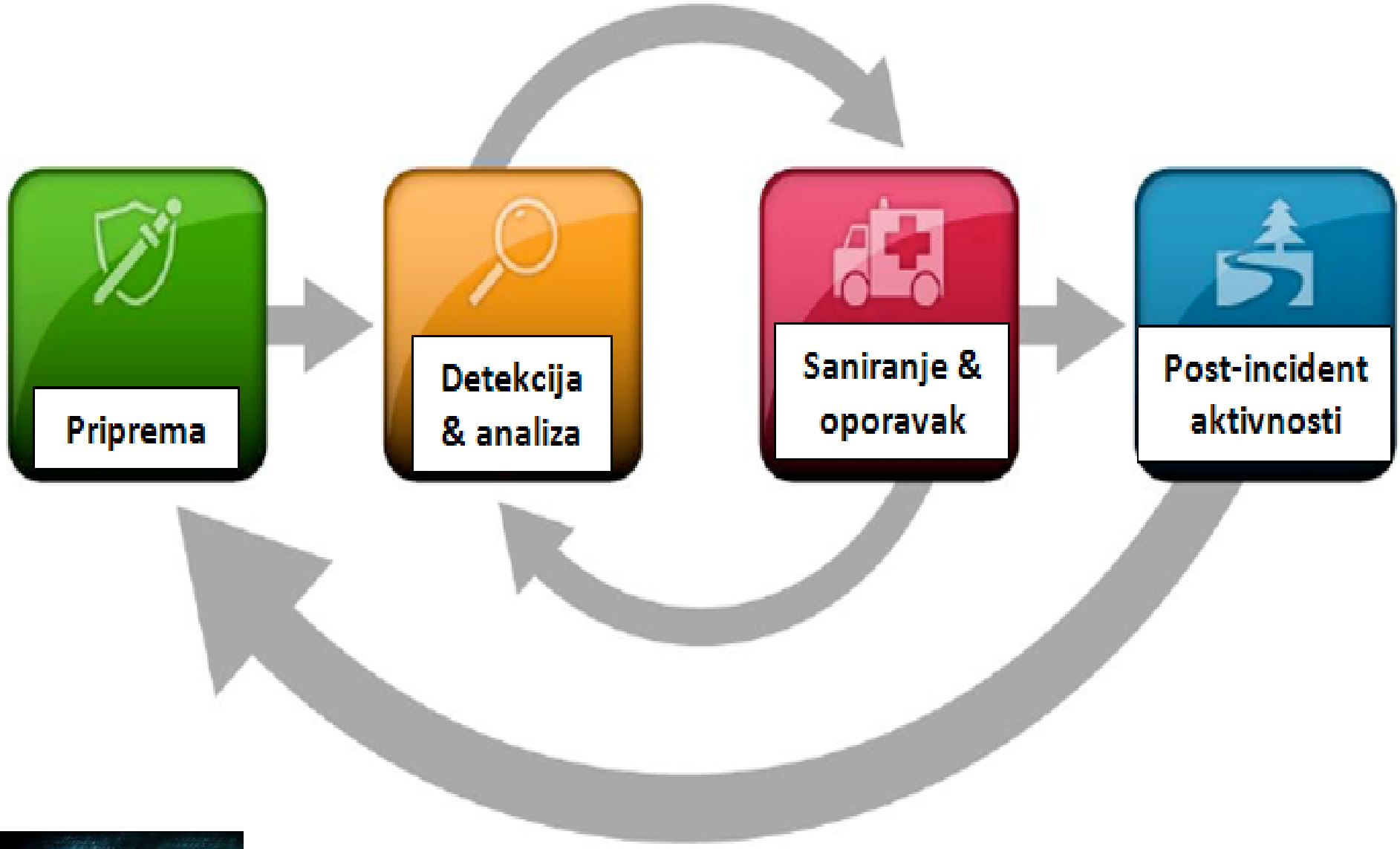
- systemisation and regularisation of work
- an opportunity to produce statistics
- an opportunity to observe trends
- a means of communication with:
  - management
  - the media
- a common language for naming threats

CONS

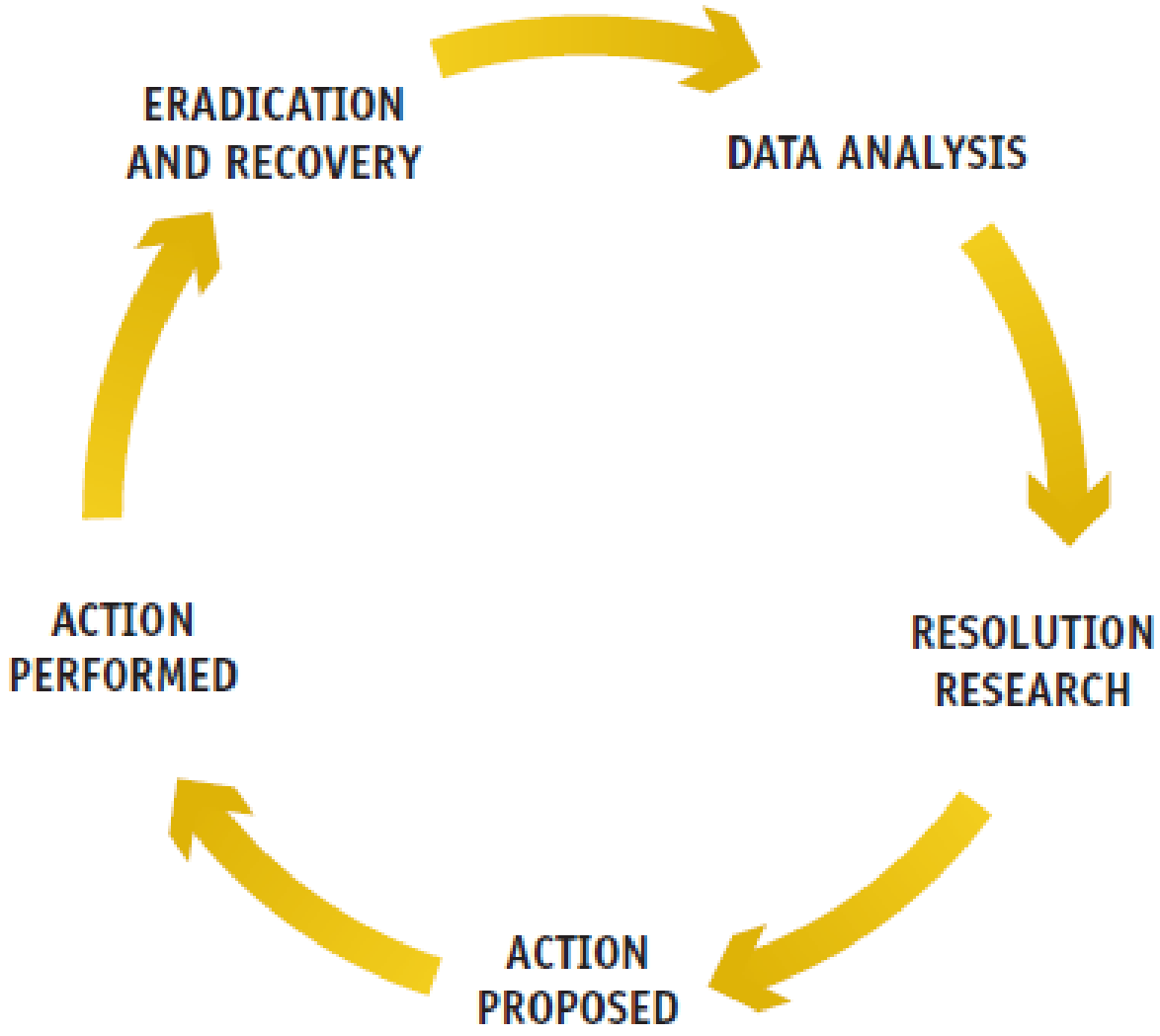
- an increase in the complexity of incident work
- an increase in the duration of incident handling
- not a real picture of internet threats
- the difficullty of ambiguous classification

Taksonomija kompjuterskog incidenta

Primer: Životni ciklus procesa upravljanja KI



Primer: Ciklus rešavanja incidenta



Proces upravljanja KI - PRIPREMA

1. Uspostavljanje kapaciteta:

- uspostavljanje politika i procedura
- formiranje interventnog tima (CIRT)
- identifikovanje članova proširenog tima
- upravljanje incidentom (priprema – analize)

2. Upravljanje specifičnim tipovima incidenata

- odbijanje izvršavanja servisa -DoS
- maliciozni napadi (virusi, crvi, Trojanci ili drugi kodovi)
- neovlašćeni pristup
- nepropisno korišćenje
- kombinovani napad.

Proces upravljanja KI -PRIPREMA

- **Struktura Politike za upravljanja KI:**
  - *izjava uprave o angažovanju*
  - *namena i ciljevi politike*
  - *obim i granice politike*
  - *identifikacija incidenta i posledica*
  - *definisanje interventnog tima (uloge, odgovornosti)*
  - *izveštavanje o incidentu i sankcije za nesprovođenje*
  - *određivanje prioriteta saniranja incidenata*
  - *merenje performansi kapaciteta*
  - *načini i forme izveštaja*
- **Procedure:** iz *politike za upravljanje incidentom*

Priprema
-Uspostavljanje kapaciteta-

1. Formiranje interventnog tima:

- **Osnovni kriterijumi:**
  - dobro razumevanje obima i granica procesa
  - edukativna komponenta korisnika
  - centralizovano upravljanje (komunikacija i izveštavanje)
  - stručni kadrovi za primenjene tehnologije (uključujući specjalistu za digitalnu forenzičku istragu, tehnike i alate)
  - dobre veze sa drugim entitetima (po potrebi).

Priprema
-Uspostavljanje kapaciteta-

- **Modeli struktura interventnih timova:**
  - *Centralni interventni tim*
  - *Distribuirani interventni tim*
  - *Koordinirani tim*
- **Model popune:**
  - Interno zaposleni članovi tima
  - Delimično iznajmljeni spoljni članovi tima
  - Potpuno iznajmljeni članovi tima

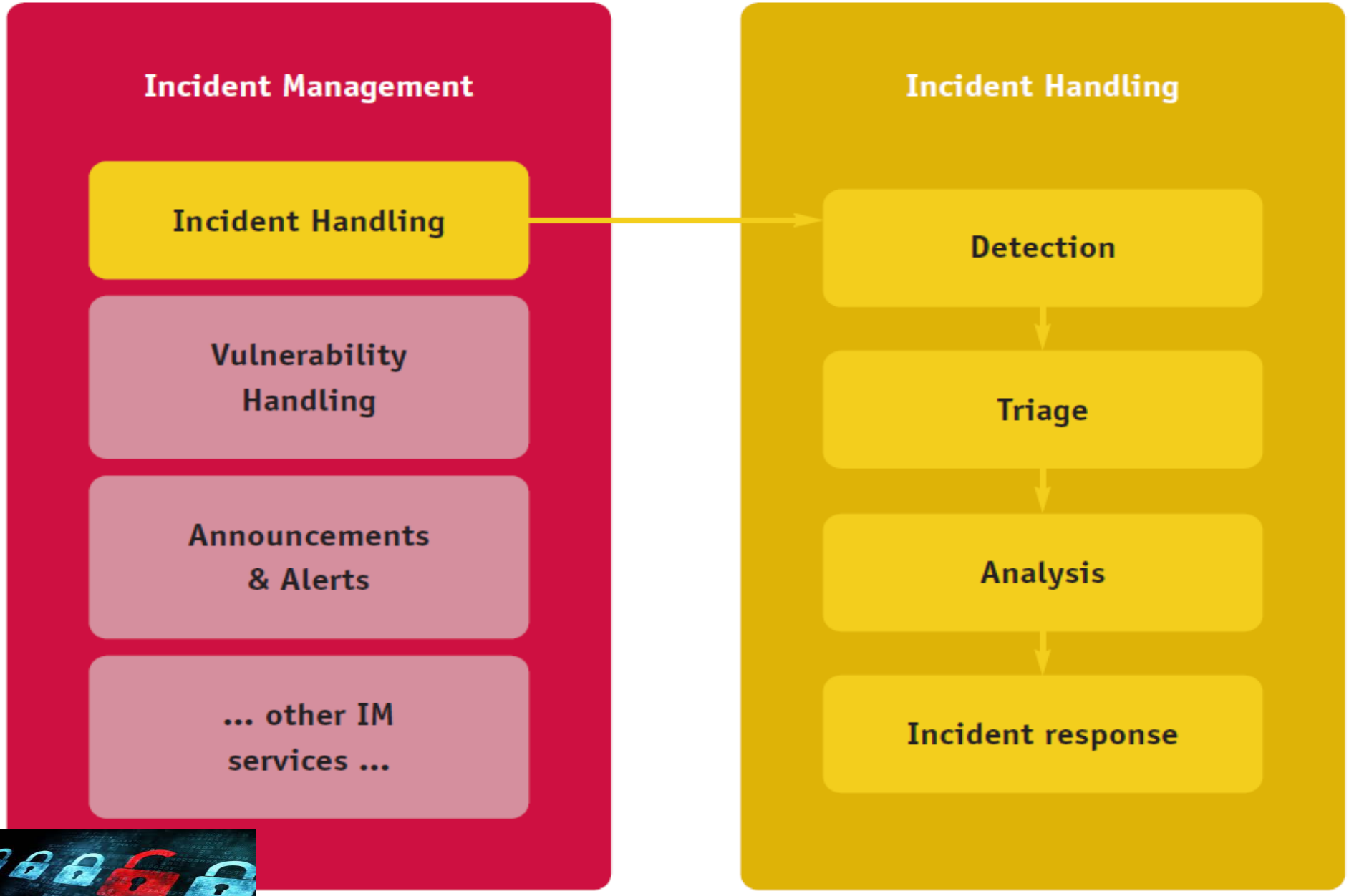
Priprema
-Uspostavljanje kapaciteta-

- **Prednosti formiranja kapaciteta za upravljanje KI:**
  - Saniranje posledica i oporavak IKTS (kontrola štete)
  - Preventivne mere sprečavanja potencijalne štete:
    - Svest o potrebi zaštite i obuka korisnika u zaštiti
    - Upravljanje bezbednosnim popravkama (zakrpama)
    - Zaštita hosta
    - Zaštita računarske mreže
    - Sprečavanje malicioznih kodova
  - Korišćenje podataka za analizu rizika
  - Poboljšanje kapaciteta organizacije za VD
  - Poboljšanje programa obuke

Upravljanje incidentom
- Detekcija i analiza KI-

- **IDS** (*Intrusion Detector Systems)*
- **IPS** (*Intrusion Protection Systems)*
- **IDPS** – konvergencija IDS i IPS
- **Detekcija i analiza KI**:
  - **nagoveštaji KI**:
    - *predznaci* i *indikatori* (pratiti, analizirati)
  - **težina procesa:** veliki broj, lažni alarmi, teško prepoznavanje indikacija...

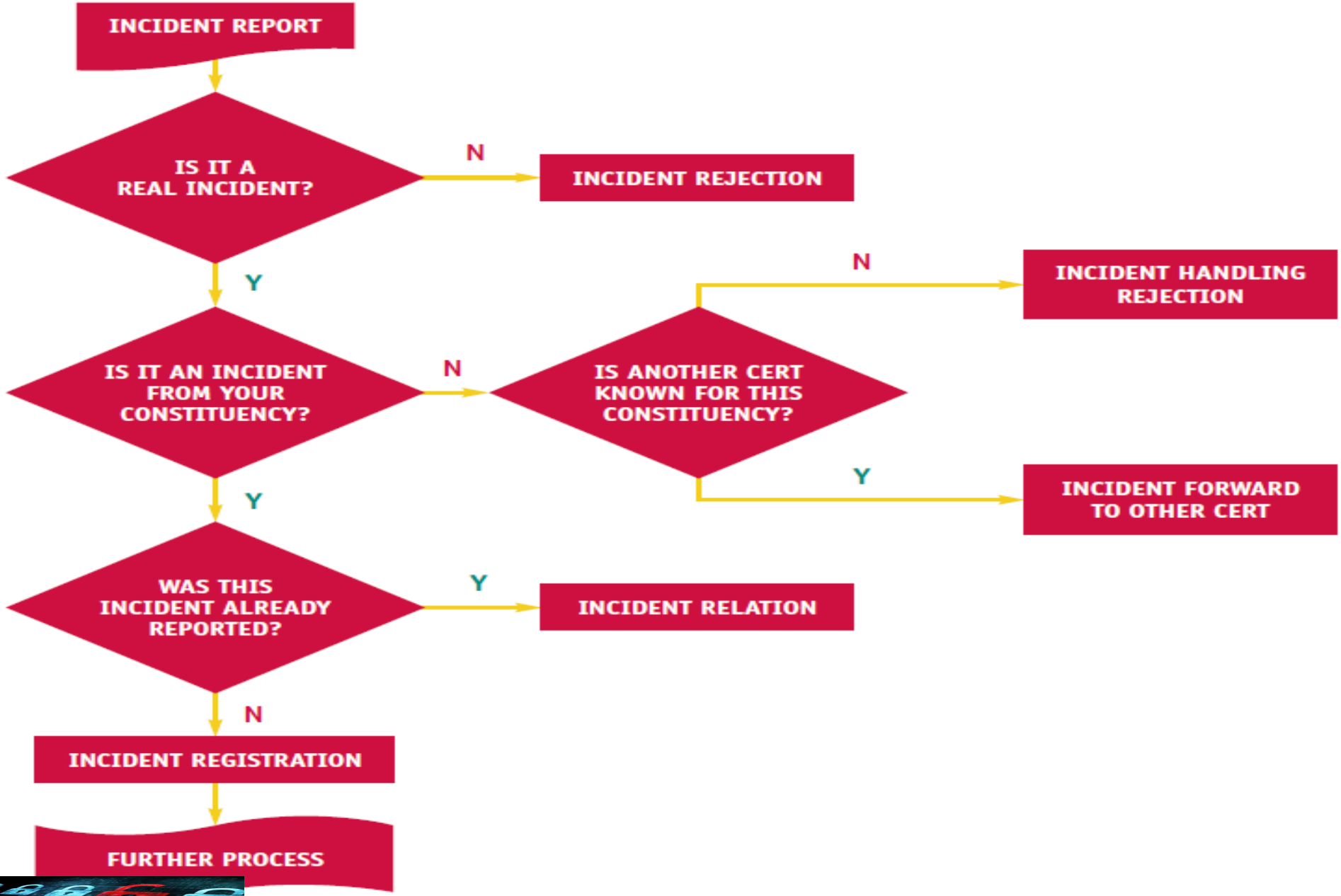
Primer: Upravljanje i rukovanje incidentom



Primer: Proces rukovania incidentom

Primer: Tok procesa saniranja incidenta

Primer: Dijagram toka procesa izveštaja o incidentu



Upravljanje incidentom u RM
-Preporučena procedura-

- *Izrada profila mreža i sistema*
- *Razumevanje normalnog rada i ponašanja IKTS*
- ***Centralizovano logovanje***
- *Izrada **politike zadržavanja log podataka***
- *Analiza **korelacije događaja***
- *Održavanje **sinhronizacije časovnika** svih hostova*
- *Korišćenje informacija iz baze znanja*
- *Korišćenje Internet brauzera za pretraživanje*
- *Aktiviranje snifera paketa za skupljanje dodatnih podataka*

Upravljanje incidentom u RM 1
-Preporučena procedura-

- *Filtriranje i analiza indikatora **KI***
- *Formiranje dijagnostičke matrice* **KI:**
  - *kolona* - kategorija **KI**, *red*- simptom, *ćelija* – događaj **KI** (najčešći simptom)
- *Traženje pomoći od drugih* CIRT i CERT
- *Dokumentovanje incidenta*
- *Određivanje prioriteta u upravljanju incidentom*
  - tekući i potencijalni tehnički efekti incidenta
  - kritičnost pogođenih objekata
- *Obaveštavanje o incidentu* (koga i kako)

Upravljanje KI - saniranje posledica i oporavak sistema

1. **Strategija** zavisi od tipa KI:
   - virusna infekcije preko e-maila
   - mrežno distribuirani DoS napad

   Preopruka: razviti strategiju za glavne kategorija KI
2. **Kriterijume za strategiju** - eksplicitno dokumentovati:
   - Potencijalna oštećenja i krađu objekata
   - Obavezu čuvanja dokaza za **forenzičku analizu i veštačenje**
   - Raposloživost servisa
   - Vreme i resursi potrebni za implementaciju strategije
   - Efektivnost stragtegije (delimično, potpuno saniran incident)
   - Trajnost rešenja (hitno, privremeno, permanentno rešenje)

Primer: Određivanje prioriteta

Prema intenzitetu napada

Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

Prema tipu objekta napada

PRIORITY	.GOV ORGANISATION	SLA CUSTOMER	OTHERS
RED	1	1	2
YELLOW	2	1	3
ORANGE	3	2	3

Primer: Indikatori DoS/DDoS napada

Unusual slowdown of network services

Unavailability of a particular web site

Dramatic increase in the volume of spam

Primer: DDoS napad

Primer: Taksonomija DDoS napada

DDoS attacks can be classified according to:

The Degree of Automation

- Manual attacks
- Semi-automatic attacks
  - Attack by direct communication
  - Attack by indirect communication
- Automatic attacks
  - Attacks using random scanning
  - Attacks using hit list scanning
  - Attacks using topology scanning
  - Attacks using Permutation Scanning
  - Attacks using Local Subnet Scanning

Propagation mechanism

- Attacks using Central Source Propagation
- Attacks using Back-chaining Propagation
- Attacks using Autonomous Propagation

Primer: Taksonomija DDoS napada -1

Exploited Vulnerability

- Protocol Attacks
- Brute-force Attacks
  - Filterable Attacks
  - Non-filterable Attacks

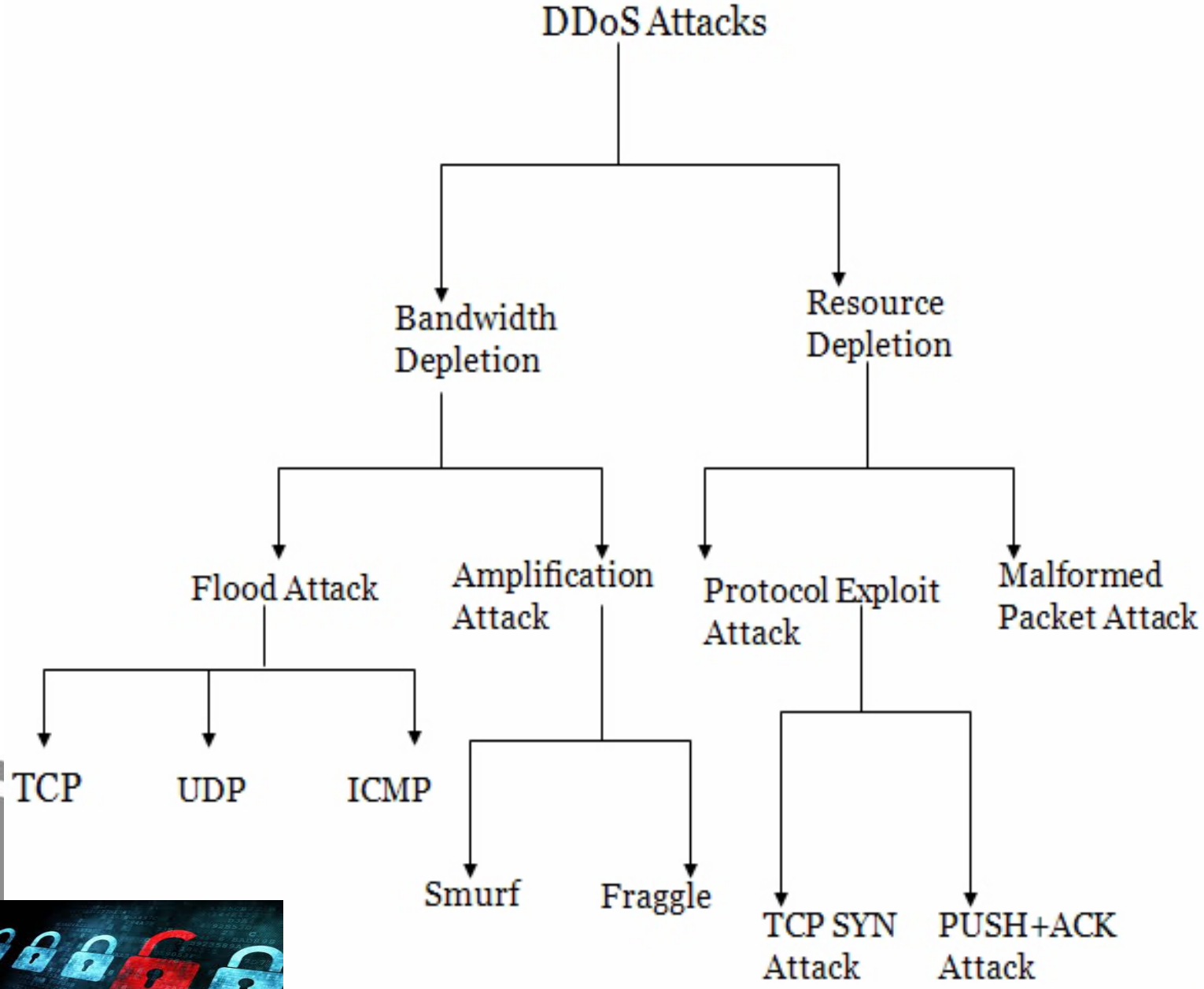
Attack Rate Dynamics

- Continuous Rate Attacks
- Variable Rate Attacks
  - Increasing Rate Attacks
  - Fluctuating Rate Attacks

Impact

- Disruptive Attacks
- Degrading Attacks

Primer: Taksonomija DDoS napada -2



Primer: Tehnike detekcije DDoS napada

Activity profiling is the process of calculating the average packet rate for a network flow, which consists of consecutive packets with similar packet fields

Time interval between the consecutive matching packets determines the flow's average packet rate or activity level

Individual flows with similar characteristics can be clustered together for easy monitoring

Traffic activities that indicate a DoS attack:

- Increase in average packet flow rate
- Increase in the overall number of distinct clusters

Primer: Detekcija DDoS napada sa CISCO *NetFlaw*

NetFlow is the in-built service in the Cisco routers that monitors and exports data for sampled IP traffic flows

When NetFlow identifies a new flow, an entry is added to the NetFlow cache; this entry then is used to switch packets and to perform ACL checking

NetFlow sampling includes:

- Source and destination IP address
- Source and destination TCP/UDP ports
- Port utilization numbers
- Packet counts and bytes per packet

Primer: ICMP Trace Back

ICMP traceback messages are used to find the source of an attack

ICMP traceback message includes:

- Router's next and earlier hop address
- Timestamp
- Role of the traced packet
- Authentication information

Traceback mechanism allows the victim to find out an attacking agent on traced packets

It maintains logs of the DDoS attack information to do a forensic analysis and assists in enforcing law if the attacker does severe financial damage

This mechanism is based on the number of attacking agents

Primer: Problemi istrage DDoS napada

Attackers know that they can be traced, so they attack for a limited time

Attacks come from multiple sources

Anonymizers protect privacy by impeding tracking

Attackers may destroy logs and other audit data

Communication problems slow down the tracing process

There is no mechanism for performing malicious traffic discrimination

False positives, missed detections, and detection delays

There are some legal issues which makes the investigation process difficult

Upravljanje KI - opšti zahtevi za istragu KI

- Razumeti **kako je napadač ušao** u IKTS (**DF istraga**)
- **Ući u trag napadaču** (tel centrala, ISP, angažovanje organa za istragu KI i kriminala)
- Otkriti **motiv** napadača
- Skupiti što više **posrednih** dokaza o napadu
- **Suziti listu osumnjičenih** (da nije interni)
- **Dokumentovati štetu** nanetu žrtvi napada
- Doneti odluku za dalju istragu (ne/angažovati policiju)
- Uvek tretirati da će slučaj završiti na sudu

Upravljanje KI -Akvizicija i rukovanje digitalnim dokazima (DD)

1. **Formirati u čuvati log datoteku za sve digitalne dokaze** :
   - identifikacione informacije
   - ime, zvanje, broj telefona svakog člana tima za istragu
   - vreme i datum svakog rukovanja sa dokazom
   - lokacija skladištenja i čuvanja dokaza
2. **Većina forenzičkih alata - za akviziciju i analizu DD**:
   - Identifikovanje/oporavak fragmenata datoteka (*unused*), (*deleted*), (*slack*) i sl.
   - ispitivanje strukture datoteka, hedera i drugih karakteristika
   - prikazivanje sadržaja grafičkih datoteka (steganografija)
   - kompleksna pretraga hardvera, softvera i okruženja
   - grafičko prikazivanje strukture direktorijuma
   - generisanje izveštaja

Upravljanje KI -Identifikacija napadača

- Vrednovanje IP adrese napadača
- Skeniranje sistema napadača
- Istraživanje napadača pretragom web-a
- Korišćenje baza informacija o incidentima
- Monitorisanje mogućih komunikacionih kanala napadača

Upravljanje KI - Oporavak sistema

- eliminisati preostale komponente incidenta:
  - brisanje malicioznih kodova,
  - dezaktiviranje probijenih korisničkih naloga ...
  - brisanje tragova – nije potrebno ili u toku oporavka
- restauracija sistema iz bekapa za normalan rad
- poboljšavanje zaštite da se spreče slični incidenti
- zamena kompromitovanih datoteka
- instalacija zakrpa, jače lozinke i perimetar RM
- podizanje nivoa sistema logovanja

Upravljanje KI - Analiza iskustava

- Šta se tačno desilo i u koje vreme?
- Ponašanje uprave/zapolsenih u saniranju KI?
- Sproveđenje dokumentovane procedure?
- Adekvatnost procedure?
- Informacije potrebne neposredno po izbijanju KI?
- Preduzete akcije koje su mogle sprečiti oporavak?
- Postupak sledeći put sa sličnim incidentom?
- Korektivne akcije za sprečavanje sličnih incidenate?
- Dodatni alati i resursi za saniranje novih incidenata?

Upravljanje KI -Korišćenje izveštaja

- za proces obuke o zaštiti
- za ažuriranje politike i procedura za **upravljanje KI** (**U KI**)
- za otkrivanje grešaka u procedurama za **U KI**
- za ažuriranje dokumenata za **U KI**
- za izradu analitičkih izveštaja za svaki **KI**
- za izrada formalne hronologije događaja (za sud)

Međuzavisnost sa drugim servisima zaštite

- Planranje vanrednih događaja u IKTS
- Operativna podrška IKTS
- Obuka u zaštiti i stvaranje svesti o potrebi zaštite
- Upravljanje bezbednosnim rizikom
- Personalna zaštita
- Edukacija i obuka članova interventnog tima
- Politika zaštite

Preporuke

- Uspostaviti kapacitete za upravljanje KI u org.
- Redukovati učestanost KI merama zaštite
- Dokumentovati politiku/procedure/uputstva **U KI**
- Promovisati značaj detekcije i analize incidenta
- Izraditi *Uputstvo za upravljanje KI* sa prioritetima saniranja
- Koristiti iskustva iz saniranja KI
- Održavati visoko nivo svesti o potrebi izgradnje kapaciteta za **U KI**

Predlog pobolišania relevantnih učesnika

INCIDENT TARGET	ISP/ICP	CERTs	LEGAL	SOURCE OF INCIDENT
COLLECT ALL AVAILABLE LOGS	RETAIN LOGS	MEDIATE CONTACT TO THE LOCAL ISP/ICP	SHARE LEGAL ADVICE	LOG EVENTS
DESCRIBE AN INCIDENT	ASSIST IN OPERATIONAL ACTION	ADVICE IN SIMILAR CASES	SUPPORT LEGAL ACTION	SEARCH FOR SUSPICIOUS USERS
Teach an incident / advise how to avoid it	Explain the mechanism	Share a lesson learnt	Inform about a result / propose a legal action	Advise how to avoid being "an attacker"

Pitanja