Ofenzivna sigurnost

TLP

Ante Čavar, 12.01.2026

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Ukratko o TLP-u
- Video uvod (TLP u vojsci)
- Analogija koraka
- Opširnije o koracima
- Mane i alternative
- Zaključak
- Literatura

Motivacija

- Jeste li ikada osjetili nervozu kada se dogodi problem koji od vas zahtjeva trenutno rješavanje, a niste znali kako mu pristupiti?
  - Takozvani “analysis paralysis” tj. paraliza zbog analize (previše podataka)
- Zbog velike količine podatak u stresnim i kompliciranim situacijama nema uvijek vremena konzultirati se sa nadređenim ili pitati za savjet
  - I ovdje TLP to rješava

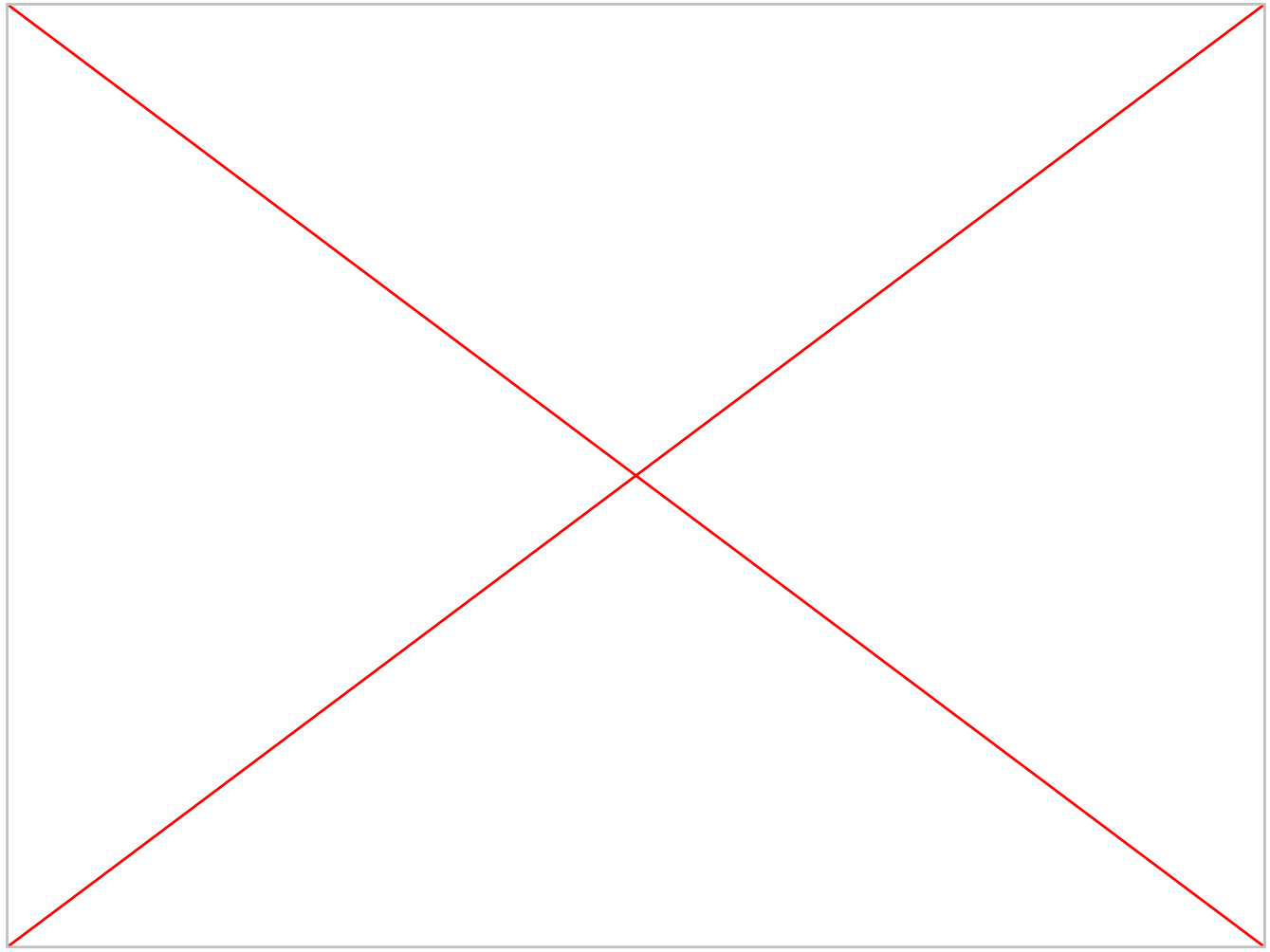
Pitanja za ispite

- Koji je glavni razlog za korištenje okvira poput TLP-a (Troop Leading Procedures) u stresnim situacijama kibernetičke sigurnosti?
- U koraku "Izrada privremenog plana", što je glavna svrha korištenja vojnog akronima METT-TC?
- Koliko koraka ima TLP i u kojem koraku se radi analiza provedenih akcija?
- Koja je alternativa TLP-u i zašto nam je ona bolja?
- Navedi i opiši jednu manu TLP-a.
- Za koga je TLP namjenjen?

Ukratko o TLP-u

- Sistematski pristup planiranju, pripremanju i izvedbi (vojnih) operacija na razini manjih jedinica
  - namijenjen zapovjednicima
  - Vojska, marinci
  - brigade, specijalizirani timovi…
- **MDMP** (Military Decision-Making Process), no “usitnjenija” i dinamičnija verzija
- Koraci navedeni ne moraju teći linearno već se njihov poredak i način izvršavanja mijenjaju ovisno o situaciji

Video uvod



Analogija koraka u kontekstu kibernetičke sigurnosti

Korak	Vojni kontekst	Kibernetička analogija
1. Primitak misije	Dobitak zapovijedi (OPORD)	Primitak obavijesti o incidentu
2. Izdavanje naredbe upozorenja (WARNO)	Izvješće podređenima da se pripreme	Slanje WARNO tima, priprema alata ovisno o situaciji
3. Izrada privremenog plana (METT-TC)	Analiza neprijatelja, terena i resursa	Analiza vektora napada, topologije mreže i dostupnih alata/ljudstva
4. Inicijaliziranje pokretanja (mobilizacija)	Premještanje postrojbe na lokaciju.	Priprema infrastrukture, izolacija segmenata mreže…
5. Provođenje izviđanja	Izviđanje neprijateljskih pozicija	Skeniranje mreže, analiza logova, lov na prijetnje
6. Završavanje plana	Finalizacija operativnog plana	Definiranje ROE (Rules of Engagement) i konačne strategije ublažavanja
7. Izdavanje naredbe	Izdavanje krajnje zapovijedi	Zadnje informiranje tima prije početka ofenzivne/obrambene operacije
8. Nadzor i "pročišćavanje"	Nadzor, vježbe	Nadgledanje sustava nakon/tokom operacije

Tablica 1. Analogija vojnih termina u kontekstu kibernetičke sigurnosti

Opširno: Primitak misije

- Ticket u JIRA-i, poziv CISO-a, alarm s IDS-a, poziv incident respondera
- naglasak na analizi vremena
  - koliko je prošlo od alarma, kada se prvi oglasio, koliko će nam trebati da se mobiliziramo
- Cilj ovog koraka je razumijevanje i definiranje prioriteta i ograničenja

Opširno: Izdavanje naredbe upozorenje WARNO

- Obavještavanje podređenih relevantnih ljudi
  - forenzičari pripremaju snapshotove, mrežni admini provjeravaju vatrozid…
- Naglasak na brzini
- Cilj je mobilizacija resursa i ljudi dok nadređeni razmišlja što i kako dalje

Opširno: Izrada privremenog plana

- METT-TC
  - *Mission, Enemy, Terrain, Troops, Time, Civilians*

Cilj je definirati:

- koja je misija (konačni cilj)
- tko je neprijatelj (APT, pojedinac, grupa)
- kako izgleda naš kompromitirani segment mreže i njegova okolina
- tko je od ljudstva dostupan (on-site, može doći on-site, nedostupni)

Opširno: Mobilizacija

- Nema direktnog prijevoda u kontekstu kibernetičke sigurnosti
- Podrazumijeva:
  - podizanje virtualnih mašina za analizu (sandbox)
  - priprema alata koji će potencijalno trebati
  - prikupljanje informacija prethodnih incidenata (radi usporedbe i potencijalnih podudaranja)
  - …

Opširno: Izviđanje

- Ne vjeruj slijepo inicijalnoj analizi (iz 1. koraka)
- Nmap - skeniranje mreže
- provjera integriteta datotek (Tripwire)
- analiza mrežnih (PCAP) zapisa

Opširno: Završavanje plana

- Dopuna i izmjene inicijalnog plana na temelju informacija dobivenih iz prethodnih koraka
- Definiramo:
  - tko smije pričati sa medijima i što smije reći
  - tko priča sa upravom
  - tko rješava koji dio problema
  - kako ćemo se oporaviti od incidenta
  - koje su naknadne radnje koje moramo poduzeti

Opširno: Izdavanje naredbe

- Upravo ono što naslov kaže
- Provodimo plan na način kako smo to definirali u prethodnom koraku
- U ovom koraku se očekuje da svatko zna koji mu je posao i kako ga mora napraviti

Opširno: Nadzor i usavršavanje

- Najbitniji korak za unaprjeđivanje i doradu procesa
  - jesu li naredbe izvršene kako treba
  - što smo napravili a nismo morali
  - što nismo napravili a trebali smo
  - što smo mogli brže napraviti
  - kako spriječiti da se incident ponovi
- Također podrazumijeva i trenutno provođenje prethodne naredbe

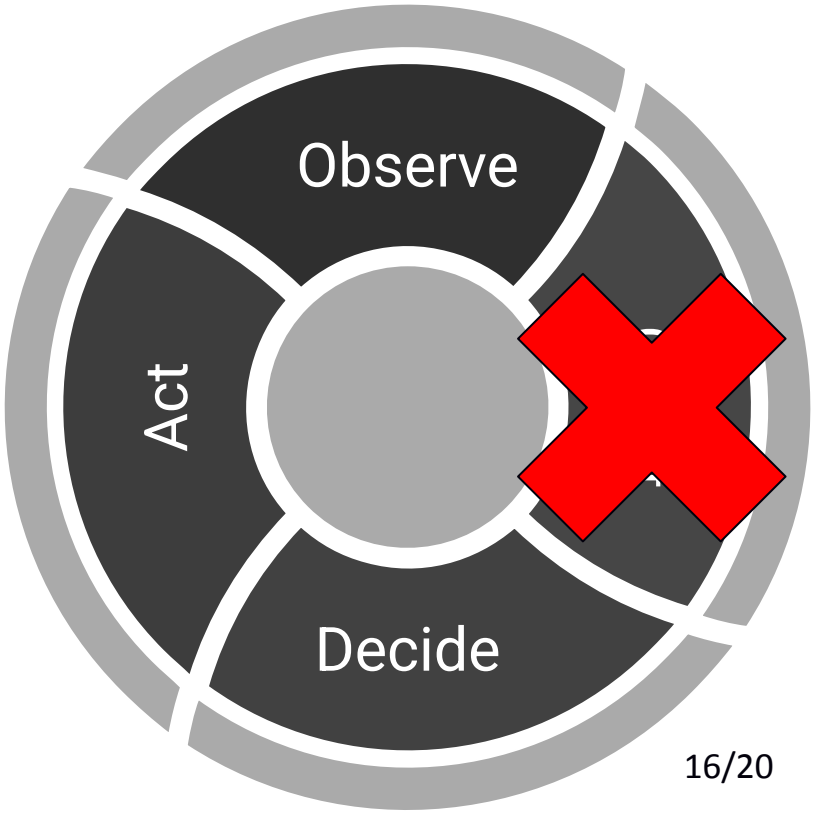
Mane

- **Hijerarhijska ukočenost** - TLP je zamišljen za strukturu gdje vođa planira a podređeni izvršavaju bez preispitivanja vođe; gubitak dragocjenih sekundi zbog zapovjednog lanca
- **Linearna zamka** - koliko god koraci bili dinamični, TLP je inherentno sekvencijalan; držanje redoslijeda može dovesti do toga da planiramo za situaciju koja je postojala prije 10 minuta
- **Kognitivno opterećenje vođe** - TLP agregira svu odgovornost na jednu osobu od kog se očekuje da donese odluku za svaku stvar; u kibernetičkim incidentima nastaje tolika količina informacija da nije moguće da uz razumijevanje istih davati naredbe efektivno

Alternative

- **OODA Loop** (Observe-Orient-Decide-Act)
  - rješava problem tromosti
- **Mission Command**
  - daj timu cilj, pusti ih da sami nađu cilj
- Heuristika i intuicija
  - iskusnim ljudima ne treba pretjerani nadzor

Slika 1. OODA petlja



Zaključak

- U kontekstu vojske - zlatni standard
  - nama i ne baš
- Dobar za standardizaciju i trening neiskusnih timova kako bi znali što uopće raditi u krizi
- Za iskusne timove procedura je previše troma i trebalo bi se zamijeniti agilnijim i dinamičnijim sustavima (OODA petlja)

Literatura

- https://www.youtube.com/watch?v=MW8PLWazisE - posjećeno 10.1., Troop Leading Procedures
- https://safety.army.mil/Portals/0/Documents/MEDIA/SMALLUNITLEADERCARDS/Standard/Troop-Leading-Procedures.pdf - posjećeno 10.1.
- https://en.wikipedia.org/wiki/Troop_Leading_Procedures - posjećeno 10.1.
- https://en.wikipedia.org/wiki/Military_Decision_Making_Process - posjećeno 10.1.
- https://www.educationconnection.com/army-study-guide/troop-leading-procedures/ - posjećeno 10.1.
- https://www.ssh.com/academy/military-cybersecurity-protecting-operations - posjećeno 10.1
- https://thedecisionlab.com/reference-guide/computer-science/the-ooda-loop - posjećeno 11.1.

Dodatna literatura

- https://rdl.train.army.mil/catalog-ws/view/100.ATSC/B2CD5B93-A4F0-40F3-82E3-AAA34EA2ECAD-1395943497063/report.pdf - posjećeno 10.1.
- https://www.187fw.ang.af.mil/Portals/1/08%20--%20TLP%20and%20Convoy%20Planning%20%28SFC2%29.ppt - posjećeno 11.1.

Hvala!