Ofenzivna sigurnost

Uspostava APT organizacije

izv. prof. dr. sc. Stjepan Groš

Sadržaj

- Uspostava APT organizacije
- Vrste operacija koje provode APT-ovi
- Ključni dijelovi APT organizacije
- Planiranje i vođenje operacija

Osnovna ideja predmeta

- Pretpostavit ćemo u predavanju da imamo na raspolaganju APT grupu
- Bavit ćemo se pitanjima
  - Što bi takva grupa trebala imati i kako bi trebala izgledati?
  - Kako upravljati tom grupom?
  - Kako koristiti tu grupu za provođenje napada?
  - Interakcija te grupe s drugim grupama

Uspostava APT organizacije

- Pretpostavimo da ste dobili zadatak uspostaviti APT organizaciju – **Kako biste to napravili?**
- To pitanje nam je bitno jer procesi koje pokušavamo uspostaviti ovise o onome što imamo!
- Pretpostavimo za početak da krećemo od ničega
  - Kasnije ćemo razmotriti neke varijacije na temu

Vrste ofenzivnih operacija (1)

- Špijunske operacije
  - Operacije širokog dosega
    - Operation Triangulation [https://en.wikipedia.org/wiki/Operation_Triangulation]
  - Industrijska špijunaža
- Sabotaže
  - Ciljani napad na infrastrukturu koja nije spojena na Internet [Stuxnet]
  - Napad na elektro-energetsku infrastrukturu [Ukrajina]

Vrste ofenzivnih operacija (2)

- Napad na dobavni lanac
  - Cilj napada je netko drugi
  - Primjer: SolarWinds

Ključni dijelovi APT organizacije

- Jezgreni timovi (engl. core teams)
  - Funkcije koje su potrebne za sve operacije
- Timovi za provođenje misija
  - Kreiraju se na temelju potreba specifičnih operacija
- Administrativni timovi
  - Pravna, logistička, financijska i tehnička podrška
  - Prisutne u svim organizacijama

Jezgreni timovi (1)

- Tim za obavještajni rad i analizu podataka
  - Ljudi specijalizirani za obavještajni rad
  - Prikupljaju i obrađuju podatke o potencijalnim ciljevima
  - Također obrađuju eksiltrirane podatke
- Tim za otkrivanje ranjivosti i razvoj eksploita
  - Snabdjeva timove za misije ili tim za razvoj zlućudnog koda sa eksploitima
  - Ranjivosti samostalno istražuje ili dobavlja od trećih strana

Jezgreni timovi (2)

- DevOps tim za razvoj zlućudnog koda
  - Razvija zlućudni kod za timove za misije
  - Uspostavlja i održava svu infrastrukturu za potporu zlućudnog koda (C&C)
  - Sastoji se od programskih, sistemskih i mrežnih inženjera
- Operativni tim
  - Provodi proces planiranja i izvršavanja operacija

Timovi za provođenje misije

- Ad-hoc ili privremeni timovi koji se uspostavljaju kada
  - Je potrebno specijalističko domensko znanje
    - Primjerice, napad na upravljački sustav
  - Prolongirano djelovanje
  - Multidisciplinarni

Administrativni timovi

- Pravna služba (engl. legal department)
- IT tim
- Ljudski resursi
- Financijska služba
- OPSEC tim

Dodatni resursi na raspolaganju

- Izvođači (engl. contractors)
- Kibernetički kriminalci
- Dobavljači zloćudnog koda

Planiranje operacija na nivou organizacije (1)

- Na nivou APT organizacije za planiranje se može upotrebljavati MDMP
  - Military Decision Making Process
  - Proces koji se upotrebljava u vojsci na razini brigade i više
- MDMP je strukturirani proces kojim definiramo kako ćemo ostvariti misiju (zadaću)
- Odmah, ili što prije, se generira WARNORD (engl. warning order)

Planiranje operacija na nivou organizacije (2)

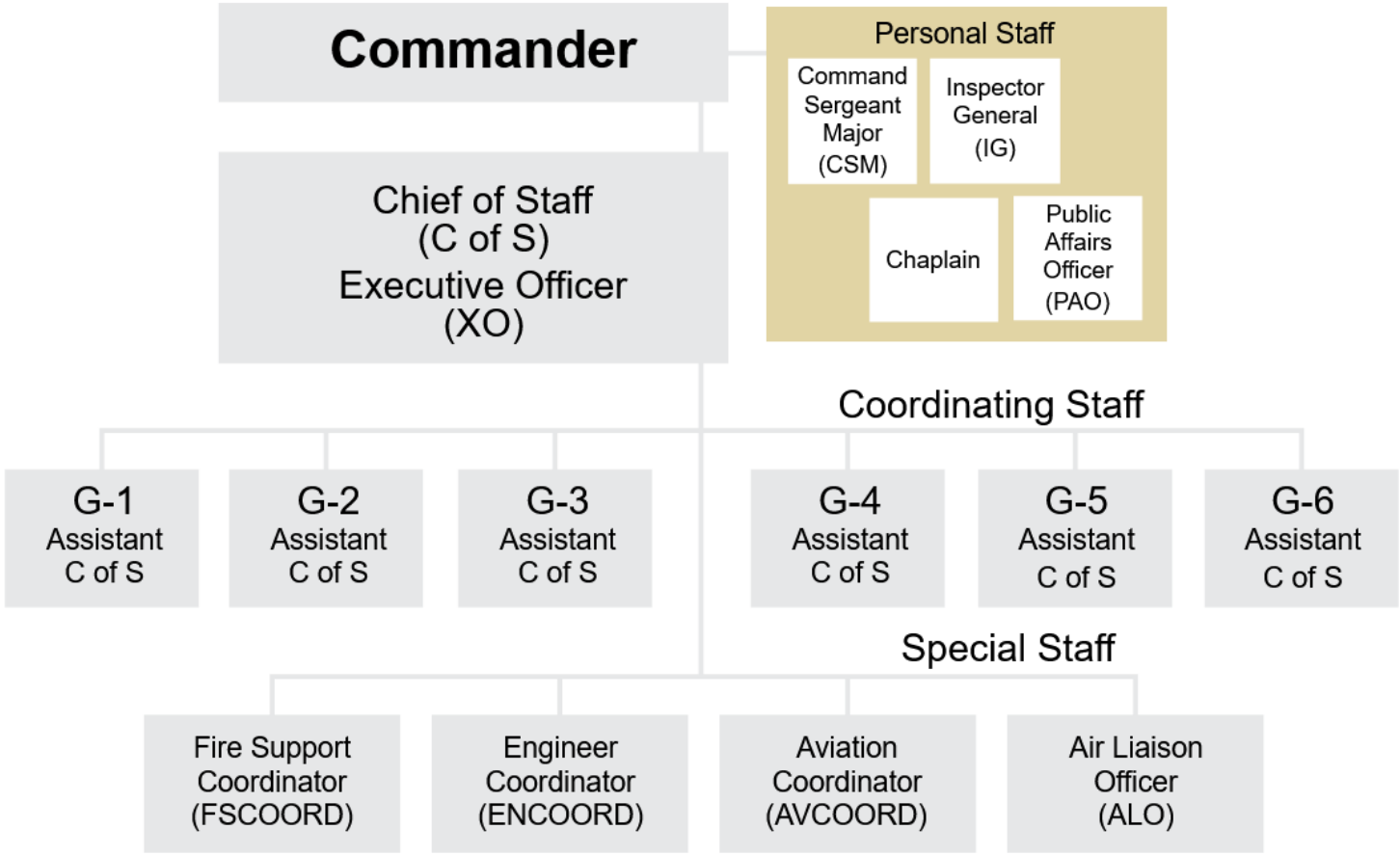
- MDMP uzima u obzir interne i eksterne resurse i sposobnosti
- Temeljni rezultat je slijed akcija (Coarse of Action, COA)
- Izlaz je u obliku OPORD (engl. operation order)
  - Dokument koji definira što treba napraviti i postići nižim jedinicama

Vođenje tima

- Za vođenje tima može se upotrebljavati TLP
  - Troop Leading Procedures
  - Metoda kojom se u vojsci vode manje jedinice
  - Postoji struktura, ali nije formalan i zahtjevan kao MDMP
- Timom upravlja zapovjednik (ili voditelj tima)
- Dobija WARNORD i OPORD
- Alternativa ili komplement su razne agilne metode

Struktura vojnih jedinica

- Personnel (G1) (S1)
- Intelligence (G2) (S2)
- Operations and training (G3) (S3)
- Logistics (G4) (S4)
- Civil-military operationS (G5) (S5)
- Signal operations (G6) (S6)



Literatura

Ahmad, Atif, et al. "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack." Computers & Security 86 (2019): 402-418.

Hvala!