Ofenzivna sigurnost

Ponašanje tima

Dorian Matić, 14.01.2026.

Pregled predavanja

1) Motivacija
2) Pitanja za ispite
3) Izazovi pri istraživanju ponašanja timova
4) Izvori podataka o ponašanju timova
5) Čimbenici ponašanja timova
6) Zaključak
7) Literatura

Motivacija

- **Što čini timove za kibernetičku sigurnost efikasnima?**
  - Kibernetička sigurnost je tehnička disciplina, ali ljudski faktor često čini razliku između uspjeha i neuspjeha
- Loša ustrojenost tima negativno utječe na njegove performanse
  - Ustrojstvo tima obuhvaća organizaciju, komunikaciju, vođenje i specijalizaciju članova
- **CILJ: Osposobiti buduće stručnjake za rad u timovima kibernetičke sigurnosti**
  - Osim tehničkih vještina, kod stručnjaka za kibernetičku sigurnost, ključno je razvijati i međuljudske vještine

Pitanja za ispite

1. Koji su čimbenici ponašanja timova promatrani?
2. Koji je stil vođenja učinkovitiji pri odgovaranju na incidente u usporedbi s administrativnim poslovima?
3. Koje su faze Tuckmanova modela razvoja tima?
4. Što je funkcionalna specijalizacija uloga i zašto je utvrđeno da je to karakteristika uspješnih timova?
5. Je li ugodna i česta komunikacija nužno odlika uspješnih timova? Objasnite.

Izazovi pri istraživanju ponašanja timova

- Problem „crne kutije”
  - Postoji značajne rupe u znanju o ponašanju timova [1][2]
  - Istraživanja se fokusiraju na pojedince (članove), a ne tim kao cjelinu
- Otežano prikupljanje podataka
  - Tehničke metrike (npr. *„server uptime”*) nisu dovoljne da objasne *zašto* je tim uspio
  - Potrebno je upotpuniti sliku mjerenjem ljudskih čimbenika poput razine stresa, količine komunikacije [1]

Izvori podataka o ponašanju tima

- **Procjena promatranjem** – stručni ljudski promatrači su ubačeni u timove kako bi ocijenili „soft skills”
- **Sociometrički senzori** – nošeni na tijelu kako bi mjerili glasnoću razgovora, pokrete, količinu vremena provedenog u razgovoru licem u lice
- **NIDS (Network Intrusion Detection System)** – sigurnosni alat za nadzor i analizu mrežnog prometa [3]

Čimbenici ponašanja timova

- **Obrasci komunikacije** – kako timovi komuniciraju, putem kojih medija i koliko
- **Dinamika vodstva** – stil i struktura vodstva timova
- **Specijalizacija uloga i evolucija tima** – koliko su članovi tima specijalizirani za svoje zadaće
- **Strateška koordinacija** – kako timovi pristupaju poslu, analiziraju situaciju i dijele zadatke

Obrasci komunikacije

- Količina komunikacije „licem u lice”
  - Pokazano je su timovi čiji članovi manje komuniciraju licem u lice uspješniji jer bolje razumiju svoje zadatke, odnosno uloge, i ne moraju se puno konzultirati
- Digitalni ili analogni kanali
  - Timovi preferiraju digitalne chat kanale (npr. Slack, Teams), čak i kad su i istom fizičkom prostoru [3]
  - Digitalni kanali omogućuju razmjenu podataka koje nije lako verbalno prenijeti, npr. IP adrese, log zapisi, isječci programskog koda.
  - Također, na digitalnim kanalima ostaje trajni zapis, koristan za rekonstrukciju tijeka incidenta
- Razmjena informacije
  - Uspješni timovi efikasnije razmjenjuju informacije, komunicirajući važno i smanjujući šum koji nastaje komuniciranjem nebitnih informacija

Dinamika vodstva

- Upravljački stil i stil koncensusa
  - Upravljački (zapovjedni) stil je efikasniji pri rješavanju incidenata, a stil koncensusa pri drugim zadacima[2]
- Centraliziranost komunikacije
  - U manje efikasnim timovima, voditelj je u središtu komunikacije, što ukazuje na mikromenadžment
- Koreografija, ne orkestracija
  - U uspješnim timovima, članovi nastupaju autonomno, bez čekanja eksplicitnih instrukcija voditelja

Primjer 1: MACCDC (2016)

- **Natjecanje:** Dva tipa izazova [2]
  1. rušenje servera zbog aktivnog djelovanja napadača (incidenti)
  2. ”poslovni” zahtjevi za pisanjem politika/pravilnika (scenariji)
- **Rezultat:** Isti stil vodstva (zapovjedni/stil koncensusa) *nije* odgovarao za oba izazova.
- **Pouka:** Uspješni voditelji prilagođavaju svoj stil vodstva tipu izazova pred timom.

Specijalizacija uloga i evolucija tima

- Specijalizacija po ulogama
  - Članovi uspješni timovi su specijalizirani po ulogama koje obavljaju. [3]
  - Npr. specijalist za „networking”, za Kubernetes, za administraciju Windowsa
- Dubina i širina vještina
  - U uspješnim timovima, članovi imaju i dubinu i širinu znanja. Osnovna tehnička znanja su prisutna kod svih članova, ali svaki pojedinac u nekom području ima dubinu. [3]
- Evolucija tima
  - Tuckmanov model: *”forming”, „storming”, ”norming”, „performing”*
  - U radu novih timova dolazi do konflikata ili konfuzije pri radu (*„storming”*), a iskusni timovi rade u jasno definiranim ulogama, što ih čine uspješnijima (*„performing"*)

Primjer 2: Baltic Cyber Shield (2010)

- **Natjecanje:** Šest timova brani mrežu elektrodistribucijskog sustava od tima profesionalnih napadača [1]
- **Rezultat:** Jedini studentski tim (Tim „E”) je bio drugi
- **Pouka:** Iskustvo pojedinaca koji čine tim, nije presudno za uspjeh tima.
  - Disciplina i kvalitetan ustroj omogućuju timovima s manje iskusnim članovima da ostvare dobar rezultat

Strateška koordinacija

- Proaktivna ili reaktivna strategija
  - Timovi koji djeluju unaprijed (proaktivno) se pokazuju uspješnijima od timova koji reagiraju na incidente
- Dijeljeni mentalni modeli
  - Dijeljena svijest tima o međusobnim vještinama omogućuje uspješno dodjeljivanje zadataka bez eksplicitne koordinacije
- Dokumentiranje
  - Uspješni timovi podrazumijevaju pisanje tehničke dokumentacije i prijavljivanje incidenata strateškim ciljevima, a ne nepotrebnom administracijom

Primjer 3: Baltic Cyber Shield (2010)

- **Natjecanje:** Šest timova brani mrežu elektrodistribucijskog sustava od tima profesionalnih napadača [1]
- **Rezultat:** Pobijedio je tim ”D”, ali automatizirane metrike (NIDS) su im bile loše
- **Pouka:** Tim „D” je imao proaktivnu strategiju
  - izmijenili su arhitekturu mreže, umjesto fokusa na rješavanje pojedinih incidenata
  - Automatizirane metrike nisu točne u ovakvim situacijama

Zaključak

- Uspješnost ustrojavanja sigurnosnih timova ovisi o shvaćanju načina funkcioniranja postojećih, uspješnih timova
- Prakse uspješnih timova
  - „Više komunikacije” ne garantira uspješnost
  - Specijalizacija uloga unutar timova je ključna
  - Tip vodstva mora biti prilagodljiv situaciji
  - Iskustvo tima kao cjeline *nije* suma iskustava članova
- Navedene prakse su široko primjenjive. I na timove izvan kibernetičke sigurnosti

Literatura

1. Granåsen, et al., (2016), *Measuring team effectiveness in cyber-defense exercises: A cross-disciplinary case study*, Cognition, Technology & Work, 18(1), 121-143. https://doi.org/10.1007/s10111-015-0350-2
2. Buchler, et al., (2018), *Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition*, Computers & Security, Volume 73,114-136, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.10.013
3. Buchler, et al., (2018), *Cyber Teaming and Role Specialization in a Cyber Security Defense Competition*, Frontiers in Psychology, Volume 9, ISSN 1664-1078, https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2018.02133

Hvala!