HANFA

HRVATSKA AGENCIJA ZA
NADZOR FINANCIJSKIH USLUGA

Ulazimo u eru DORA-e – stanje digitalne otpornosti

dr.sc. Ante Žigman
Predsjednik Upravnog vijeća

28.10.2024.

DORA : POČETAK U 2020.

- 24 rujan 2020. Europska komisija objavila je prvi draft Digital Operational Resilience Act (DORA).

- Zakonski tekst nadograđuje postojeće zahtjeve upravljanja IKT rizicima koje su već razvile pojedine EU institucije i povezuje niz inicijativa u jednu Uredbu

- DORA uspostavlja znatno čvršću osnovu za EU nadzorna i regulatorna tijela, omogućuje proširenje fokusa nadzora financijskih institucija

- Do sada: financijska stabilnost i zaštita potrošača

- **Od sada i : provjere sposobnosti financijskih institucija da održe visoku razinu otpornosti u poslovanju tijekom ozbiljnih prekida zbog nastupa rizičnih IKT događaja**

2020: STANJE KIBERNETIČKIH NAPADA

Verizon Data Breach Investigations report

32000 incidenata – rekordnih 3950 proboja

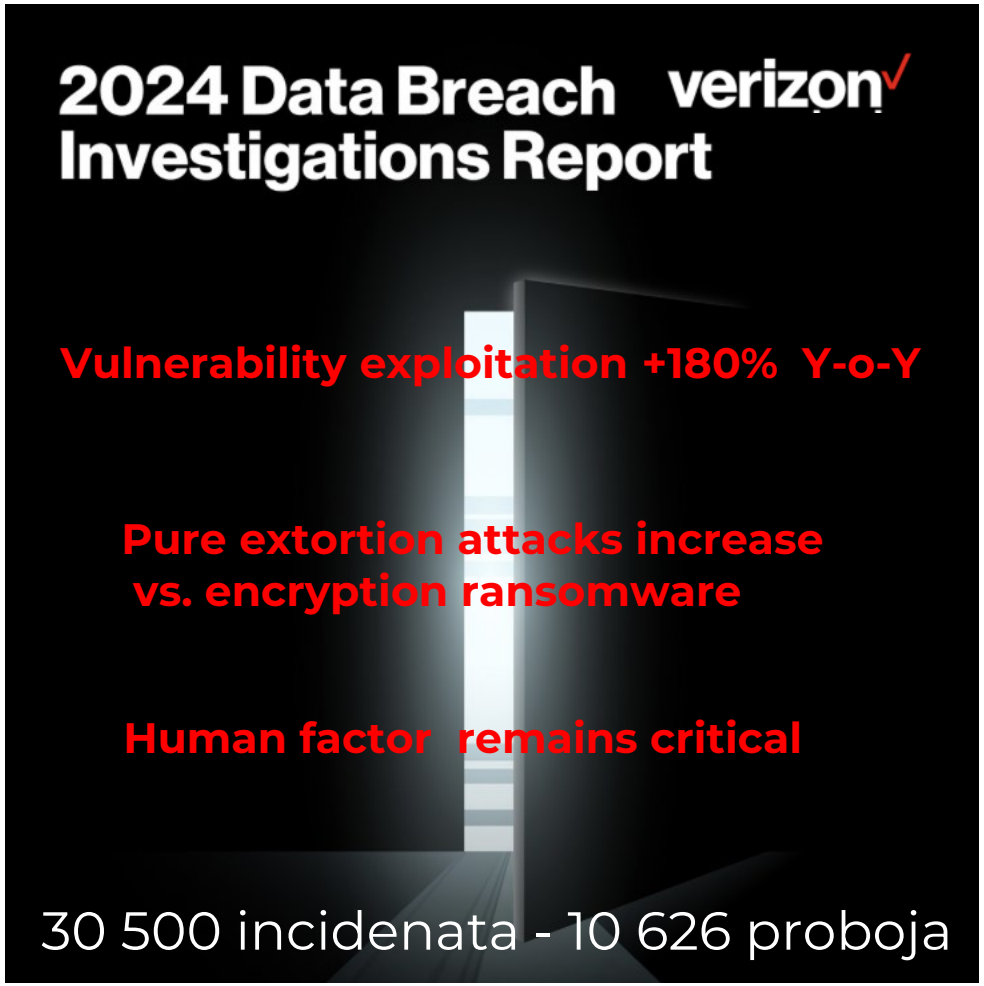
Lessons Learned

Ljudski štit je ključan – svijest i navike:

96% social phishing napada je došlo kroz mail

- RIZIK JE BIO 2020. MJERLJIV -

ŠTO SE PROMJENILO - TRI PUTA VIŠE PROBOJA



HANFA: siječanj 2024. Ransomware/Vulnerability

Kratko razdoblje prekida poslovanja

Javnost / ključni stakeholderi upoznati promptno

Brz oporavak ključnih funkcija

Fazni oporavak svih procesa

Suradnja, komunikacija i veliki interni napori

Suradnja i podrška povezanih ključnih sudionika

Hvala na suradnji i razumjevanju!

Lessons Learned

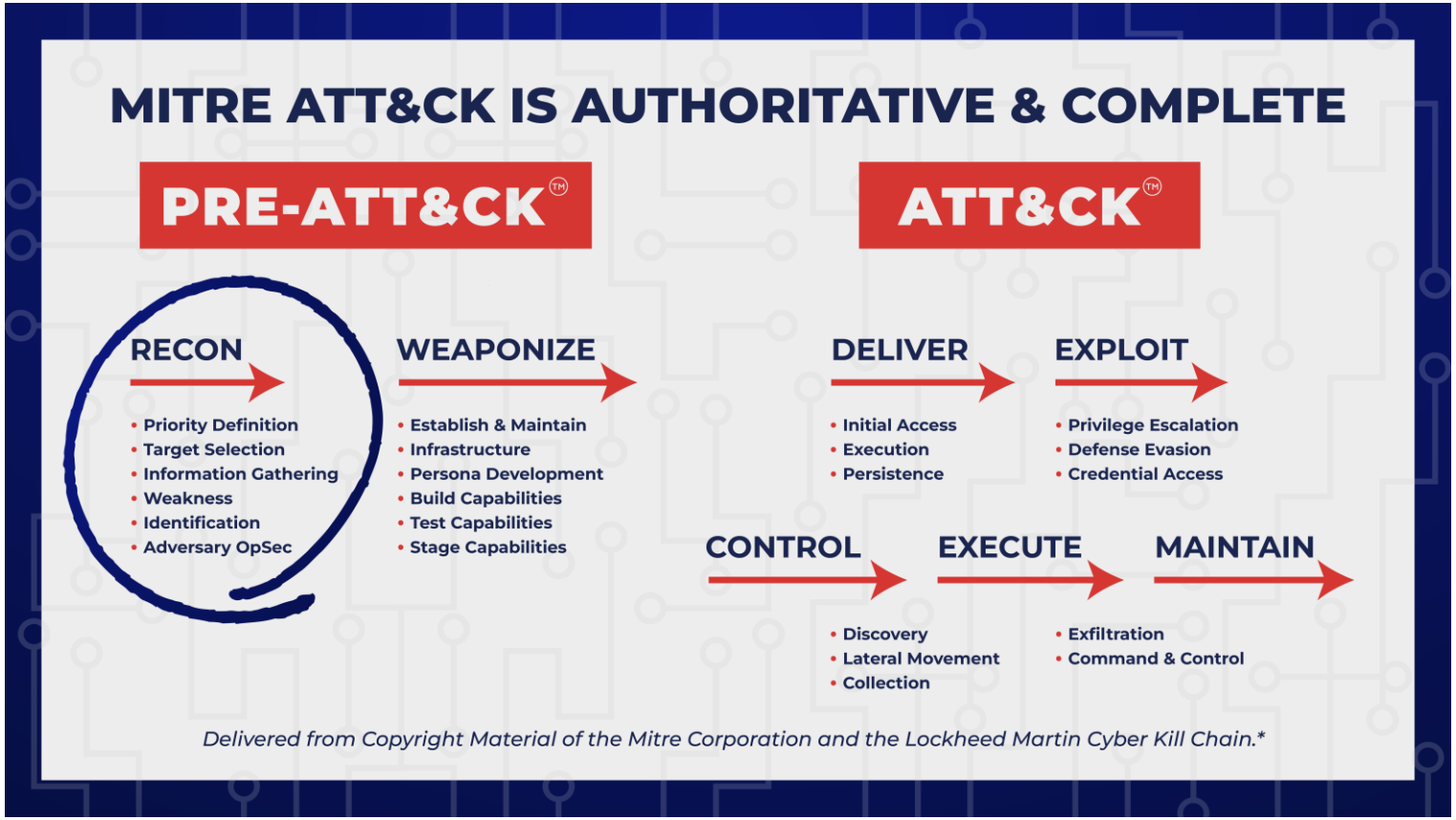
Proces upravljanja rizikom ojačan

Identificirane potrebne akcije i dugoročne politike

- RIZIK RASTE -

ANALIZA - JASNO SE RAZLIKUJU FAZE NAPADA

Lockheed Martin postavio je analizu koja se danas koristi u MITRE ATT&CK okviru



Napad počinje **izviđanjem** – provjera što je dostupno, kakve slabosti imate, gdje mjere kasne

VLASTITI PRIMJER – NAKON NAPADA

- HANFA prima mail očito sumnjivog sadržaja u svibnju koji traži da se otvori privitak
- Više korisnika prijavljuje službama IT i Informacijske sigurnosti
- Svim korisnicima šalje se upozorenje da mail ne otvaraju
- U međuvremenu, mail je provjeren i utvrđeno da je bezopasan

U drugom koraku:

Analiza pokazuje da su mail primili **SAMO članovi Upravnog vijeća i direktori**

- RIZIK JE STVARAN -

IZVIĐANJE (JOŠ PRIMJERA)

HANFA je angažirala „etičke hakere” da obave izviđanje

Thomas Murray Cyber(UK) obavio je izviđanje SVIH subjekata nadzora Hanfe

- Neinvazivno skeniranje dostupnih sustava na internetu
- Analiza otkrivenih slabosti, ranjivosti koje omogućuju prodor
- Provjera dostupnih informacija na „dark webu”
- Usporedba ukupnog profila rizičnosti s drugim subjektima
- Ne objavljujemo podatke tvrtki
- Pojedinačni podaci su dostupni za daljnju analizu

NAŠ NOVI MINDSET – *ASSUME BREACH*

Analize i iskustvo nas uči da se incidenti događaju

Jedino što nam preostaje je priprema.

Naši kolege i prijatelji u FMA, razvili su niz aktivnosti u nadzoru IKT rizika u Austriji

Također, proveli su nedavno vježbu odgovora na kibernetički napad

Hanfa je provela prije dva tjedna vlastitu vježbu s 11 društava

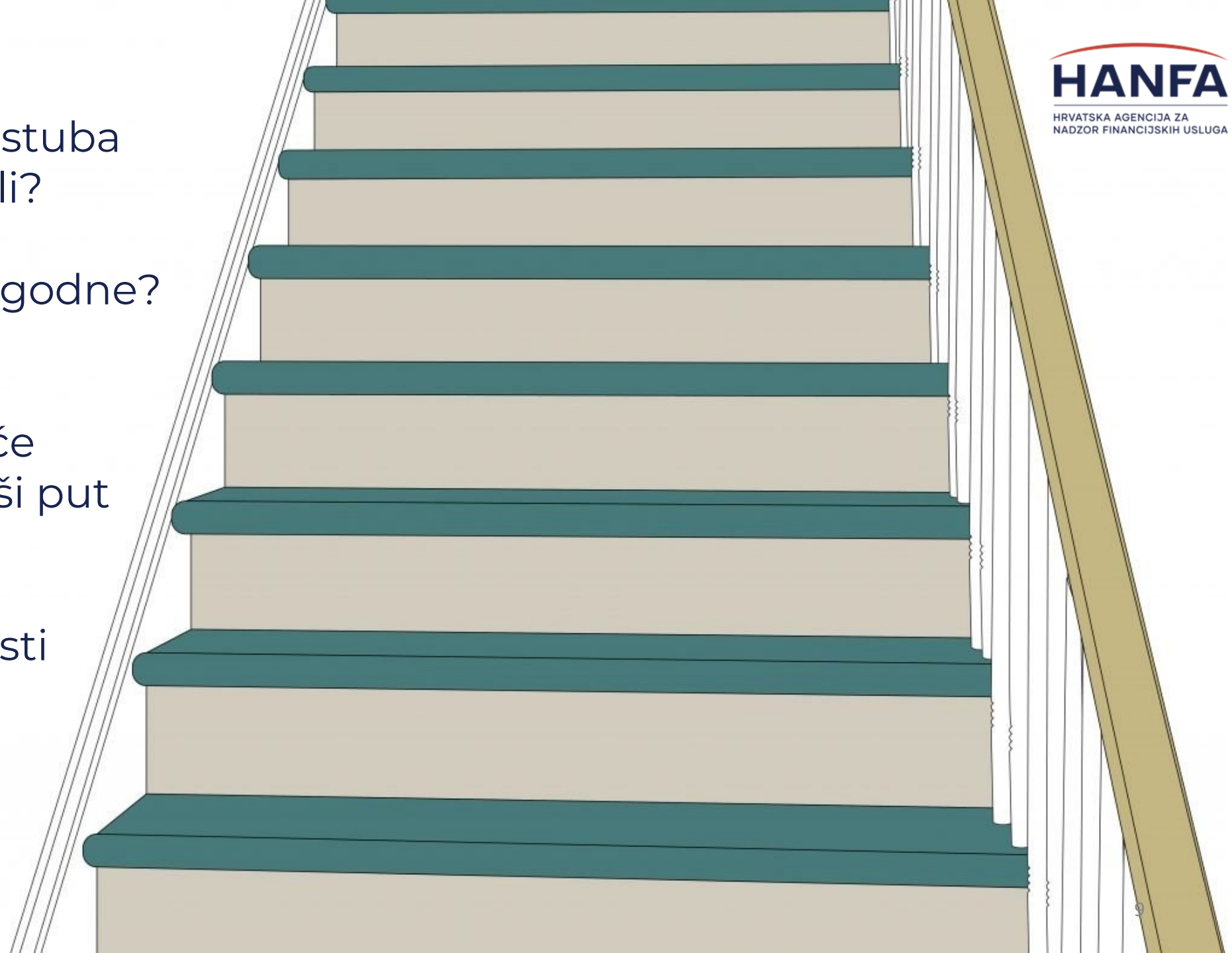
Incidenti će se događati – potrebno je vježbati i pripremiti se da utjecaj bude manji

DORA: koliko ste stuba /prepreka postavili?

jesu li strme i neugodne?

Običan napadač će uvijek izabrati lakši put

→ šansa je da će umjesto vas napasti nekog drugoga



HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

HANFA

HRVATSKA AGENCIJA ZA
NADZOR FINANCIJSKIH USLUGA

HVALA NA POZORNOSTI!