HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

Iskustva i pouke iz kibernetičke vježbe X/2024

Mladen Gavrančić
direktor Ureda za informacijsku sigurnost

listopad, 2024.

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

LISTOPAD – EU MJESEC KIBERNETIČKE SIGURNOSTI

Izvor: https://geant.org/

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

SADRŽAJ

- Ključni razlozi za provedbu vježbe
- Vježba odgovora na kibernetičke incidente
  - Cilj vježbe
  - Vremenski okvir
- Scenarij i metodologija
- Analiza rezultata – „*Lessons learned*”
- Idući koraci

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

KLJUČNI RAZLOZI ZA PROVEDBU VJEŽBE

- **Značajno povećanje broja kibernetičkih napada**
  - U zadnjih 12 mjeseci došlo je do primjetne eskalacije kibernetičkih napada, postavljajući nova mjerila u raznolikosti i broju incidenata, kao i njihovih posljedica
- **Povećan broj ranjivosti**
  - ukupno 33.524 prema 24.690 godinu prije (NIST NVD razdoblje 1.7.2023. - 1.7.2024. vs 2022/2023)
- **Zahtjevi DORA Uredbe**
  - Obveze testiranja digitalne operativne otpornosti
  - Priprema internih procesa upravljanja IKT incidentima

Izvor: ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
NIST NVD - National Vulnerability Database

TROŠAK I POSLJEDICE POVREDE PODATAKA

- Prosječni trošak povrede podataka skočio je s 4,45 MUSD u 2023. godini na 4,88 MUSD, što je najveći porast od pandemije
- Gotovo polovica svih povreda podataka (46 posto) uključuje osobne podatke korisnika

Izvor: IBM Cost of a Data Breach Report 2024, https://www.ibm.com/reports/data-breacha

VJEŽBA ODGOVORA NA KIBERNETIČKE INCIDENTE

- HANFA Vježba odgovora na kibernetički incident provedena je 14. listopada 2024. u „tabletop“ formi udaljenim pristupom
- Na vježbi je sudjelovalo 11 značajnih financijskih institucija
- tijekom vježbe donosili su
  - Poslovne i tehničke odluke na razini Uprave i stručnih timova
  - Formirani su timovi zaduženi za odgovor na incidente
  - Aktivnosti sprječavanja širenja incidenta,
  - Aktivnosti otklanjanja uzroka incidenta i
  - Aktivnosti oporavka sustava te
  - Aktivnosti izvješćivanja regulatora, korisnika i javnosti.

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

CILJ VJEŽBE

Vježbom je sudionicima pružena mogućnost da unaprijede i uvježbaju:

- Postojeće procedure odgovora na kibernetičke incidente
- Aktivnosti detekcije i analize uzroka incidenata
- Procese donošenja poslovnih i tehničkih odluka tijekom incidenta
- Aktivnosti sprječavanja širenja i otklanjanja uzroka incidenta
- Procjenu vremena potrebnog za provođenje pojedinih aktivnosti i oporavaka sustava
- Komunikaciju unutar i izvan organizacije
- Proces usavršavanja na naučenim lekcijama

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

VREMENSKI OKVIR

- Poziv sudionicima na sudjelovanje u vježbi
- 9./10. listopada 2024. – provedba obuke za rad na platformi za provedbu vježbe
- 11. listopada 2024. – slanje Scenarija sudionicima
- **14. listopada 2024. – provedba vježbe**
- 15. – 24. listopada 2024. – aktivnosti nakon završetka Vježbe (analiza i slanje dodatne dokumentacije)
- 28. listopada 2024. – javna informacija

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

SCENARIJ I METODOLOGIJA

- Scenarij vježbe sadržavao je informacije o kibernetičkom napadu koji je pogodio kritični sustav institucije te uzrokovao prekid u odvijanju povezanih poslovnih procesa

- Vježba je provedena korištenjem platforme Cyber Conflict Symulator, sva komunikacija porukama i razmjenom dokumentacije kroz platformu je zabilježena te je omogućila analizu nakon završetka vježbe

    - Cyber Conflict Symulator – platforma domaćeg razvoja tvrtke Utilis i FER, sponzorirana od EU fondova, koristi se za vojne i civilne svrhe

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

ANALIZA REZULTATA

- Nakon vježbe sudionici su proveli internu analizu vježbe – analiza provedenih akcija i aktivnosti
- Hanfa je analizu provela uvidom u provedene aktivnosti i upitnik koji je sadržavao tri dijela (završno izvješće, upitnik/pitanja i ocjenu vježbe), a koji su sudionici dostavili nakon vježbe
- Inicijalna procjena:
  - Sudionici su tijekom vježbe identificirali akcije i aktivnosti koje su nužne za oporavak sustava i nastavak poslovanja
  - Sudionici su pravovremeno poslali obavijest o incidentu i prijelazno izvješće sukladno definiranim vremenima
  - Uočeni su različiti pristupi u rješavanju incidenta, kao i značajna razlika u broju provedenih akcija i aktivnosti

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

ANALIZA REZULTATA - „LESSONS LEARNED”

- **Sudionici**
  - Kao rezultat vježbe većina sudionika definirala je korektivne radnje kojima će unaprijediti proces odgovora na IKT/kibernetičke incidente → ispunjen jedan od ciljeva vježbe
- **Hanfa**
  - Analizom ocjena i povratnih informacija od sudionika Hanfa je identificirala područja u kojima su moguća unaprjeđenja te će isto uzeti u obzir u budućim vježbama

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

ANALIZA REZULTATA – OCJENA VJEŽBE

- Koliko je za Vašu instituciju vježba bila korisna? **ocjena 4,8**
- Kako ocjenjujete provedbu same vježbe? **ocjena 4,6**
- Smatrate li da bi bilo korisno redovito provoditi ovaj tip vježbe?
  - Pozitivan odgovor – prijedlozi da se održava na godišnjoj razini
- Što bi promijenili/predložili u cilju poboljšanja kvalitete vježbe?
  - Individualni pristup (postavke komponenti sustava u platformi)
  - Više interakcije s moderatorom vježbe
  - Druge vrste scenarija (Ransomware, DoS i dr.)
  - HANFA izvještaj s najboljim praksama (nakon analize)
  - Prezentirati primjer uspješnog odgovora na kibernetički napad na jednom primjeru

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

PRIJEDLOZI ZA SVE INSTITUCIJE (NEOVISNO O VJEŽBI)

- Razraditi različite scenarije kibernetičkih napada koje će uzeti u obzir prilikom izrade, ažuriranja i testiranja planova kontinuiteta poslovanja
- Osigurati klasifikaciju IKT imovine i informacijske imovine te međuovisnosti
- Razmotriti ovisnosti o trećim stranama i njihove uloge u odgovoru na IKT/kibernetičke incidente
- Definirati jasne metode izračuna troškova i gubitaka uzrokovanih značajnim IKT/kibernetičkim incidentima

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Detecting and Mitigating Active Directory Compromises

First published: September 2024

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

HANFA
HRVATSKA AGENCIJA ZA

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Table of contents

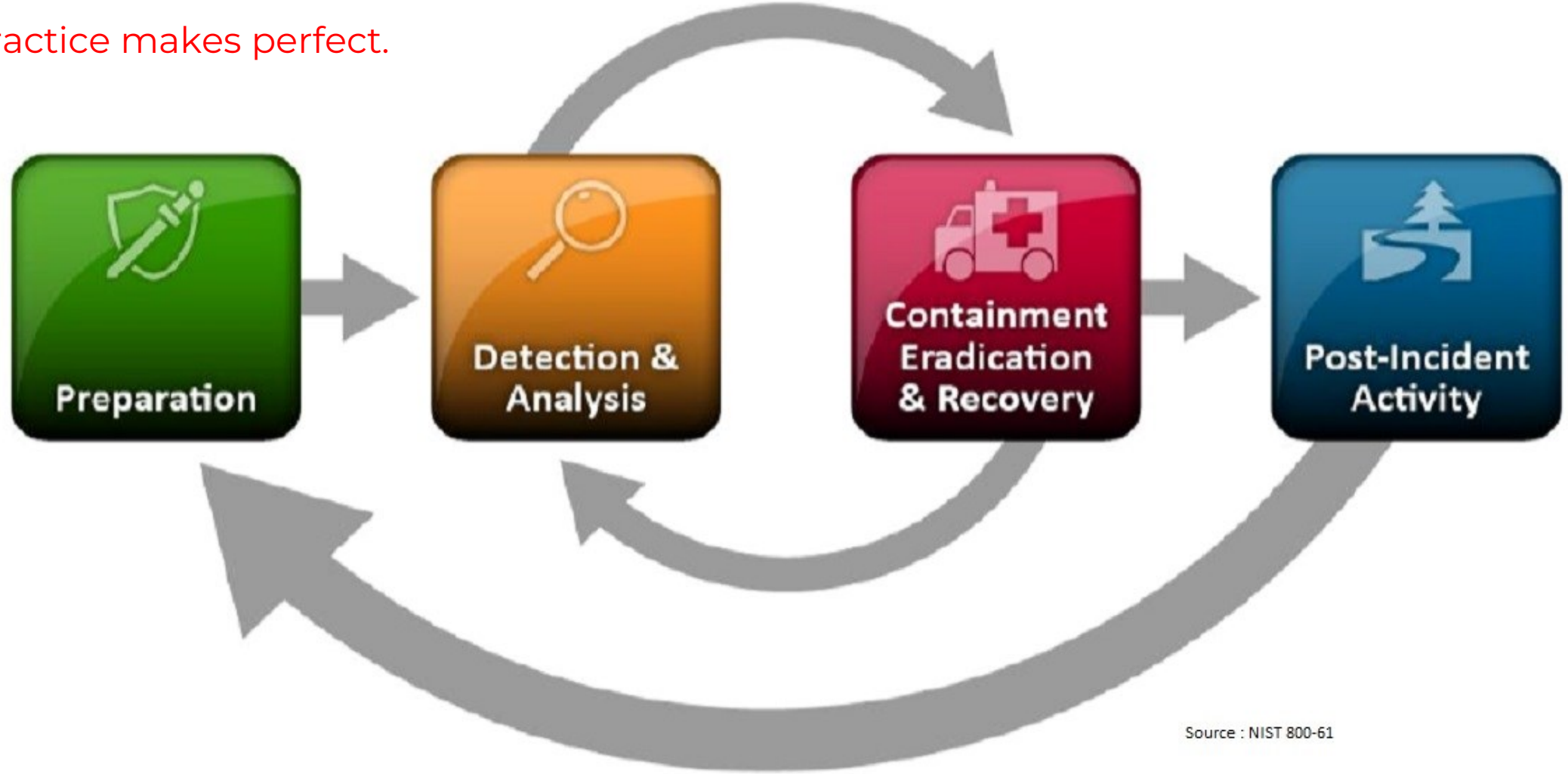
Detecting Active Directory compromises with canaries

Detecting Active Directory compromises can be difficult, time consuming and resource intensive, even for organisations with mature security information and event management (SIEM) and security operations centre (SOC) capabilities. This is because many Active Directory compromises exploit legitimate functionality and generate the same events that are generated by normal activity. Distinguishing malicious activity from normal activity often requires correlating different events, sometimes from different sources, and analysing these events for discrepancies. For some Active Directory compromises, the detection relies on the presence of one event and the absence of another. The complexity of detecting Active Directory compromises is one of the leading causes of their success and their prevalence against organisations.

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

INCIDENT – ASSUME BREACH MINDSET

Practice makes perfect.



Source : NIST 800-61

HANFA

HRVATSKA AGENCIJA ZA
NADZOR FINANCIJSKIH USLUGA

HVALA NA PAŽNJI!

PITANJA?