EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# KIBERNETSKI VDORI, ZAZNAVANJE IN OMEJEVANJE

# VSEBINA

Kaj je kibernetski vdor in pravna opredelitev.

Vrste in značilnosti vdorov.

Faze izvajanja vdora.

Zaznavanje vdorov in odzivanje nanje.

# KIBERNETSKI VDOR

## Kaj JE kibernetski vdor

Vdor pomeni **nepooblaščen in uspešen** vstop v informacijski sistem ali omrežje, pri katerem napadalec pridobi dejansko prisotnost in možnost delovanja v sistemu na enega od teh načinov:

- nepooblaščena oseba pridobi dostop do sistema ali uporabniškega računa,
- v sistemu se izvaja zlonamerna programska koda,
- napadalec lahko pregleduje, spreminja ali nadzoruje podatke ali delovanje sistema.

## Kaj NI kibernetski vdor

Kadar kljub poskusom napadalca ni prišlo do nepooblaščenega dostopa v informacijski sistem, npr.:

- blokirana phishing e-pošta,
- zavrnjen nelegitimen poskus prijave, neuspešen brute-force,
- napad ki ga ustavi tehnični sistem (NGFW, WAF, IPS, EDR)
- zaznana zlonamerna datoteka, ki se ni izvedla,
- ranljivost, ki ni uspešno izrabljena.

# PRAVNA OPREDELITEV VDORA

Vdor je pravno gledano izveden takrat, ko nepooblaščena oseba pridobi dejanski dostop do informacijskega sistema ali dela sistema. Pri tem ni potrebno da pride do dejanske škode ali da so podatki ukradeni.

Nepooblaščen dostop pomeni:

- dostop brez dovoljenja, ko oseba nima pravice do uporabe sistema,
- dejanski dostop do sistema ali podatkov, ko napadalec lahko izvaja ukaze, bere ali spreminja podatke,
- ko ima napadalec možnost dejanskega vpliva in ni nujno, da jo izkoristi, zadostuje že možnost.

**Vdor v informacijski sistem je kaznivo dejanje, ki se preganja po uradni dolžnosti, zato je ob prijavi pristojnemu CSIRT smiselna/nujna prijava tudi na policijo;**
**če je posledica vdora tudi odtekanje osebnih podatkov, je potrebna prijava na IPRS.**

# KAJ PREDSTAVLJA KIBERNETSKI VDOR

## Varnostni incident

Vdor predstavlja resen varnostni incident, ki lahko:

- ogrozi zaupnost, celovitost ali razpoložljivost informacij in storitev,
- zahteva takojšnje ukrepanje,
- pomeni obveznost poročanja skladno z ZInfV-1.

## Končne akcije zlonamernih akterjev sledijo po vdoru

Sam vdor še ne povzroči škode, škodo povzročijo aktivnosti, ki jih zlonamerni akter izvede po vdoru, npr:

- kraja gesel in drugih prijavnih podatkov za prodajo na temnem spletu ali nadaljnjo uporabo npr. CEO prevara,
- kraja poslovnih dokumentov, baz poslovnih podatkov in osebnih podatkov, izsiljevanje z njihovo objavo,
- šifriranje podatkov in sistemov ter izsiljevanje za njihovo povrnitev,
- brisanje podatkov, onemogočanje sistemov in storitev in s tem povzročanje neposredne škode.

# KLASIFIKACIJA VDOROV

## Vdori imajo svoje značilnosti

| *Značilnost* | *Opis* | *Pogostost* | *Tveganje* |
|---|---|---|---|
| **Izvor** | Neposredni vdor v organizacijo, phishing, izraba ranljivosti, notranji vdor. | Velika | Visoko |
| | Preko posrednika, proizvajalci opreme, dobavitelji, partnerji, povezana podjetja. | Srednje | Visoko |
| **Usmerjenost** | Priložnostni napad, avtomatiziran napad z izrabo ranljivosti, ne izbira organizacije. | Velika | Srednje |
| | Ciljani napad, usmerjen v organizacijo ali osebo, pripravljen in izveden v več fazah. | Srednje | Visoko |
| **Namen** | Kibernetski kriminal, ransomware, izsiljevanje s podatkil, BEC. | Velika | Visoko |
| | Vohunjenje in kraja intelektualne lastnine. | Srednje | Srednje |
| | Onemogočanje delovanja sistemov, spreminjanje ali izbris podatkov, | Srednje | Visoko |
| **Trajanje in obseg** | Hitra, enkratna akcija, hitro dejanje, takojšen vpliv. | Velika | Srednje |
| | Dolgotrajen (persistent), traja več tednov, mesecev ali celo let, prikrivanje in brisanje sledi. | Majhna | Visoko |
| **Stopnja zahtevnosti** | Enostaven vdor, znana orodja, znane ranljivosti, lahko se zazna z enostavnimi orodji. | Srednja | Srednje |
| | Napredna, sofiticirana orodja in postopki, 0-day ranljivosti, počasno napredovanje in prikrivanje. | Majhna | Visoko |

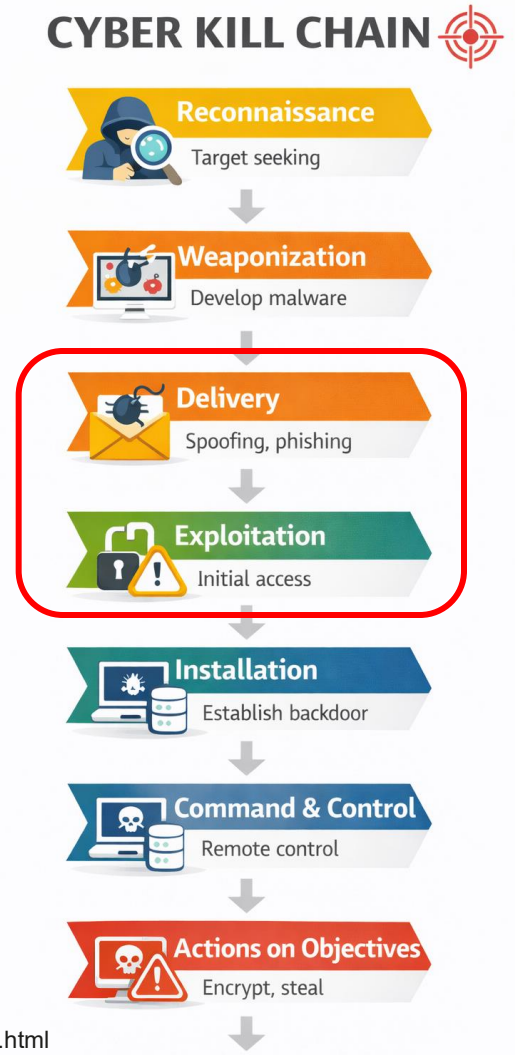
# FAZA ZAČETNEGA VDORA

## Faza začetnega vdora (intrusion) glede na Cyber Kill Chain

Cyber Kill Chain ne opredeljuje eksplicitno faze vdora.

Glede na aktivnosti je akcija vdora uvrščena med Delivery in Exploitation :

- Reconnaissance
- Weaponization
- **Delivery** – dostava artefaktov za omogočanje začetnega dostopa
- **Exploitation** – izraba ranljivosti za zagon škodljive kode
- Installation
- Command & Control
- Actions on Obj.




Slika ChatGPT po https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

# FAZA ZAČETNEGA VDORA

## Faza začetnega vdora (intrusion) glede na MITRE ATT&CK

MITRE ATT&CK prav tako ne opredeljuje eksplicitno faze vdora.

Glede na tehnike je akcija vdora uvrščena med:

- **Initial Access** - pomeni fazo, v kateri napadalec prvič pridobi nepooblaščen dostop do informacijskega sistema ali omrežja, kar pomeni, da so premagani ali obiti varnostni mehanizmi. To še ne pomeni trajne prisotnosti, kar je po MITRE v fazi Persistence.
- **Execution** – pomeni fazo, ko si napadalec pridobi možnost izvajanja kode, izvajanje ukazov na sistemih in pridobivanje podatkov.


https://attack.mitre.org/

# VDORI V PRAKSI

## Večina vdorov v praksi ni zaznanih

Začetni vdori (*initial access*) pogosto niso zaznani.

Zaznane so aktivnosti, ki vdoru sledijo, nameščanje in sprožanje škodljivih programov, izvedba akcij, ki onemogočajo storitve, se pravi ko je škoda že povzročena.

Vdor je dejanje napadalca, zaznava je sposobnost organizacije da to dejanje opazi.

Napadalec lahko napad pripravlja dolgo časa, izvede ga lahko v nekaj minutah ali sekundah. Lahko se pritaji in ostane neopažen, lahko zelo hitro napreduje na ostale faze napada (*kill chain*), odvisno kaj je njegov končni cilj (*action on objective*).

Primerjava zaznavanja z varovanjem objekta:

- Ograja, ključevnice = preventiva
- kamera, senzorji = zaznavanje
- Varnostnik = SOC zaznava in odziv

# ZAZNAVANJE VDORA

## Kibernetski napad in obramba ni fair-play

Odvija se „igra“ med zlonamernimi akterji in branilci, pri čemer imajo zlonamerneži vnaprejšnjo prednost.

- Element presenečenja, napadalec izbira čas in točko napada,
- Pri zbiranju in sestavljanju informacij za vdor, začetnem izvidovanju, izbiri ranljivosti in določanjuđ korakov napada, ki jih branilec ne pozna,
- Na voljo imajo veliko časa za pripravo tehnik in orodij za izvajanje napada, imajo veliko „testno okolje“ za njihovo izboljševanje,
- Uporabljajo legitimna orodja v okolju žrtve in delujejo prikrito, pod radarjem zaznave,
- Imajo nizko ceno neuspeha, ni problem če kakšen napad ne uspe, to izkoristijo za izboljšave,
- Imajo psihološko prednost, nimajo odgovornosti, delujejo anonimno in brez pravil (razen internih in med povezanimi akterji), ne tvegajo ugleda.
- Branilci imajo pravne in regulatorne omejitve, ne morejo napadati nazaj, morajo delovati transparentno, poročati.
- Napadalcu je dovolj le en ukraden račun ali ena izkoriščena ranljivost, ena C&C povezava za kontrolo.

# MEHANIZMI ZAZNAVANJA VDOROV V PRAKSI

### Na osnovi oznak (signature)

Znani indikatorji napadov (IoC) kot so hash vrednosti datotek, IP, domene

Zelo natančna zaznava z antivirus, IPS, NGFW, SIEM.

Ne zaznava 0-day in posebej prirejenih napadov.

### Vedenjska zaznava (behaviour)

Odstopanje od običajnega delovanja, sumljivo obnašanje.

Zazna tudi neznane napade, UEBA, EDR, neobičajne prijave.

Lahko povzroča lažne alarme.

### Zaznava anomalij (anomaly-based)

Statistično odstopanje od normalnega stanja, baseline.

Bazira na učenju normalnega stanja, uporabno predvsem pri analizi mrežnega prometa, NDR, ADS.

### Korelacijsko zaznavanje

Povezovanje več dogodkov v celoto, kjer posamezni dogodek ni incident ampak je to kombinacija dogodkov.

Korelacija dogodkov v SIEM, XDR, SOAR.

### Točke zaznavanja

Na končnih točkah, EDR, XDR.

V omrežju, NDR, ADS.

V logih, SIEM.

Na ravni identitet, AD, EntraID, UEBA.

V zunanjem okolju, CTI.

### Avtomatizacija zaznave

Zaznava uporabnika, administratorja, SOC analitika preko SIEM ali drugih orodij.

Zaznava v orodju, SOC analitik preveri in potrdi, najpogosteje.

Avtomatska zaznava in odziv preko, XDR, SOAR.

### Zaznave glede na fazo napada

Zaznava še pred vdorom, faza izvidovanja, uporaba CTI,

Zaznava v teku vdora, namestitvi kode, vzpostavitvi C&C kanala.

Zaznava ob sprožitvi končne akcije, povzročitvi vidne škode.

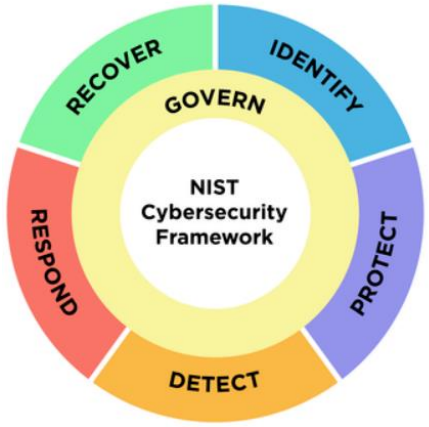
# ODZIVANJE NA INCIDENTE

## NIST Cybersecurity Framework

NIST CSF je eno glavnih vodil (*framework*) v kibernetski varnosti.

Zadnja verzija 2.0 iz začetka leta 2024 je uvedla sledeče spremembe:

- Razširitev področja uporabe, ne le kritična infrastruktura, temveč vse organizacije.
- Dodan nov funkcionalni steber Upravljanje (*Govern*).
- Poudarek na obvladovanju tveganj in dobavni verigi.




Vključuje funkcijo Zaznava (*Detect*), ki ima dve kategoriji

- **Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events,
- **Adverse Event Analysis (DE.AE):** Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents,

ti vsebujeta 11 podkategorij in 35 primerov uporabe oziroma kontrol.

Ne opisuje točno kako in s čim te kontrole izvajati.

Microsoft Excelov delovni list

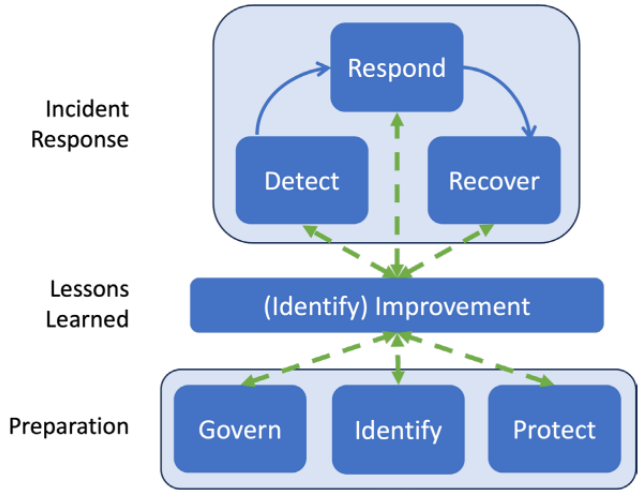



**Fig. 2. Incident response life cycle model based on CSF 2.0 Functions**

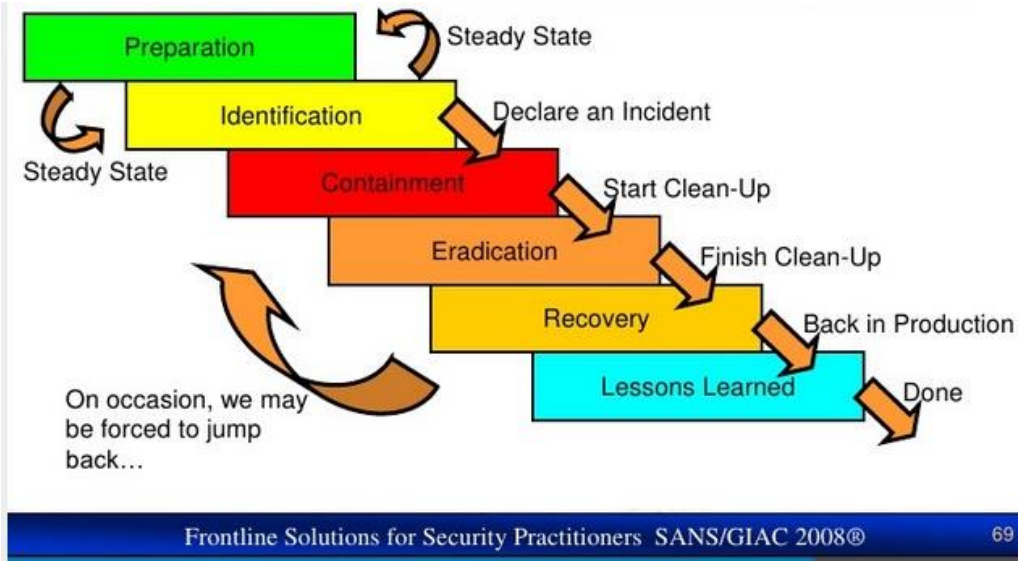
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

# ODZIVANJE NA INCIDENTE

## SANS Incident Management Framework

Določa 6 faz upravljanja s kibernetskimi incidenti

- **Priprava (*Preparation*)** Vzpostavitev politik, oblikovanje odzivne ekipe (CSIRT), uvedba spremljanja ter priprava orodij še pred nastankom incidenta.
- **Identifikacija (*Identification*)** Zaznavanje anomalij, analiza dnevniških zapisov in opozoril, potrditev dejanskega incidenta ter hitro obveščanje ključnih deležnikov.
- **Zajezitev (*Containment*)** Izvajanje kratkoročnih ukrepov za takojšnjo zaustavitev grožnje (npr. izolacija sistemov) ter dolgoročnih ukrepov za preprečevanje ponovitve.
- **Odstranitev (*Eradication*)** Odprava temeljnega vzroka, kot so zlonamerna koda ali ranljivosti, ter zagotovitev, da je grožnja v celoti odpravljena.
- **Obnovitev (*Recovery*)** Varna ponovna vzpostavitev sistemov, obnova storitev in spremljanje morebitnih preostalih težav.
- **Nauki (*Lessons Learned*)** Ključna analiza po incidentu za oceno odziva, prepoznavanje pomanjkljivosti in posodobitev postopkov za prihodnje incidente.




https://www.sans.org/security-resources/glossary-of-terms/incident-response

Značilnost SANS modela

- Tehnična usmerjenost (Technical Focus):Ponuja poglobljena navodila za tehnične vidike zaznavanja in odzivanja, v večji meri kot širši okviri, kot je NIST.
- Praktičnost in uporabnost (Practical & Actionable):Temelji na resničnih scenarijih ter je zasnovan za takojšnjo uporabo s strani varnostnih ekip.
- Strukturiran proces (Structured Process):Zagotavlja doslednost, jasno opredeljene vloge ter učinkovito obravnavo varnostnih vdorov.

# HVALA

+111 123 456 789

info@enisa.europa.eu