EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PRESOJA UČINKOVITOSTI VARNOSTNIH UKREPOV – PRIMER KAMPANJE SPLETNEGA RIBARJENJA

NAMEN

- prikazati uporabo metodologije presoje učinkovitosti varnostnih ukrepov v praksi

- ponazoriti povezavo med:
  - oceno tveganj
  - varnostnim ukrepom
  - kazalniki
  - poročanjem in ukrepanjem

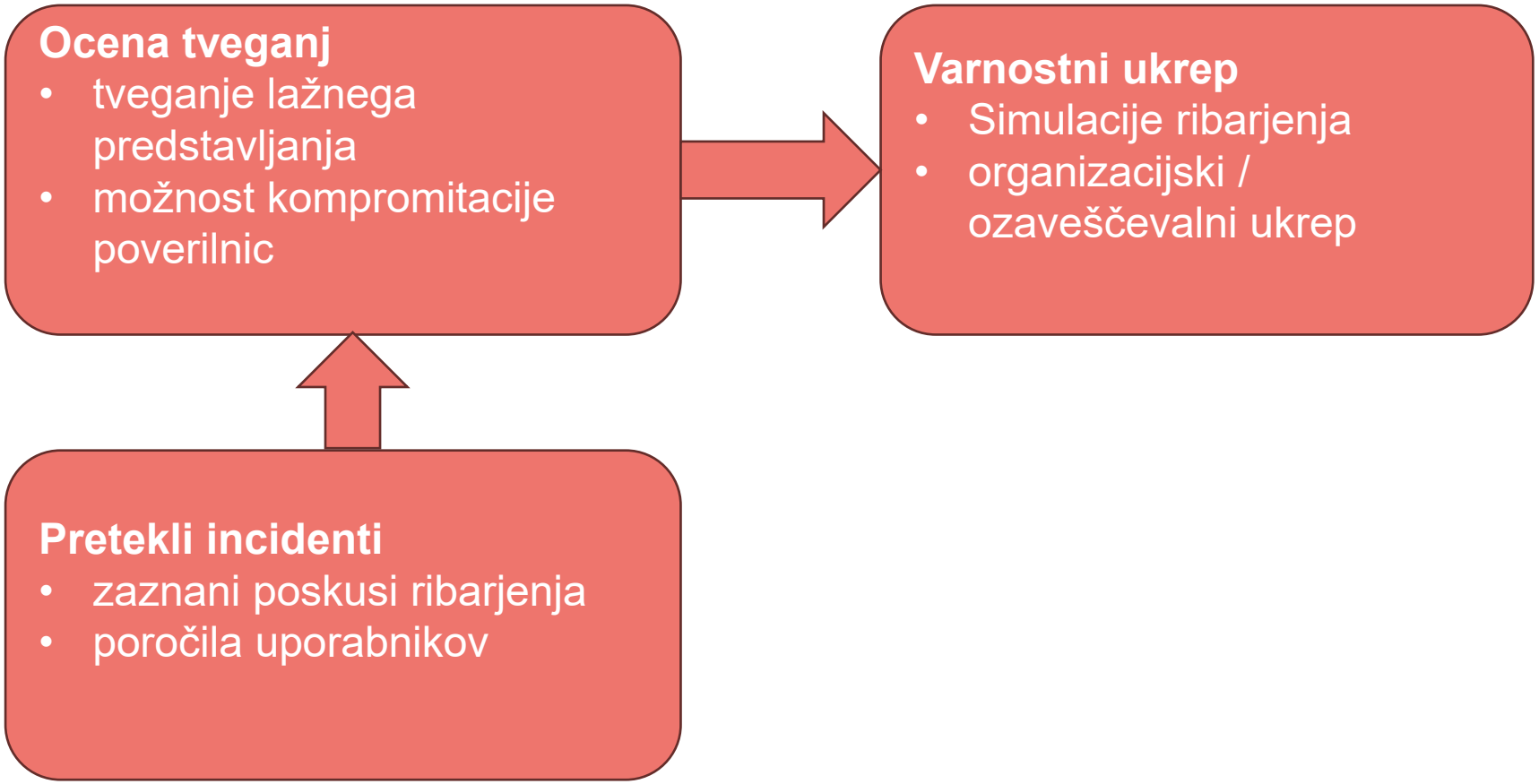
OPIS ORGANIZACIJE

- srednje velika organizacija (≈ 300 zaposlenih)
- obdelava osebnih in poslovno kritičnih podatkov
- občutljivost z vidika ZVOP-2 v primeru odtekanja podatkov
- zavezanost zahtevam ZInfV-1
- vzpostavljen sistem informacijske varnosti

Izhodišče:

- ocena tveganj prepoznava tveganje lažnega predstavljanja (ang.phishing)
- v preteklosti zaznani poskusi kompromitacije poverilnic

DOLOČITEV VARNOSTNEGA UKREPA



DOLOČITEV KAZALNIKOV USPEŠNOSTI

Namen presoje

(zakaj merimo)

presoja učinkovitosti ukrepa

primerjava skozi čas

podlaga za poročanje in ukrepanje

Kazalniki

(kako presojamo)

% vključenih uporabnikov

% klikov

% vnosa poverilnic

trendi po oddelkih

ponovitve napak

Izhodišče

(kaj presojamo)

identificiran varnostni ukrep

tveganje, ki ga ukrep naslavlja

NAMEN PRESOJE UČINKOVITOSTI

Presoja učinkovitosti ukrepa

- ali varnostni ukrep dosega svoj namen
- ali dejansko zmanjšuje izpostavljenost tveganju
- ali je primeren glede na kontekst organizacije

Primerjava skozi čas

- spremljanje trendov kazalnikov
- zaznavanje izboljšav ali poslabšanj
- preverjanje vpliva izvedenih sprememb

Podlaga za poročanje in ukrepanje

- objektivna podlaga za poročanje vodstvu
- utemeljevanje korektivnih in preventivnih ukrepov
- podpora odločanju na upravljavski ravni

KPI – MERJENJE UČINKOVITOSTI

KPI indikator	Primer cilja
Povprečen čas zaznave incidenta (MTTD)	< 4 ure
Čas odziva na incident (MTTR)	< 12 ur
Pokritost naprav z EDR/AV zaščito	> 95 %
Odprava kritičnih ranljivosti	v 14 dneh
Test obnove varnostnih kopij	100 %, 2× letno
Zaznani in blokirani poskusi ribarjenja	padajoč trend

Primer KPI za podporo presoji učinkovitosti – ciljne vrednosti so odvisne od konteksta organizacije.

MERJENJE TVEGANJ - KRI

Kako organizacija spremlja, kdaj tveganje preseže sprejemljivo raven

KRI indikator	Prag tveganja (primer)
Odprte kritične ranljivosti (CVSS > 8)	> 10 starejših od 14 dni
Neavtorizirani dostopi	> 5 potrjenih primerov / mesec
Incidenti zaradi dobavne verige	≥ 1
Aktivni uporabniški računi brez MFA	> 2
Neuspeli zapisi varnostnih dnevnikov (ang. log backup)	> 2 dni zamude

Primer KRI za podporo spremljanju tveganj – pragovi so določeni glede na tveganja in kontekst organizacije.

ZBIRANJE PODATKOV

Viri podatkov

- orodja za simulacijo ribarjenja
- varnostni dnevniki (SIEM / MDR / EDR)
- sistemi za upravljanje ranljivosti
- poročila uporabnikov

Obdelava podatkov

- periodično zbiranje (mesečno / kvartalno)
- preverljivost in sledljivost virov
- primerljivost skozi čas

Kazalniki in presoja

- izračun kazalnikov
- analiza trendov in odstopanj
- podlaga za poročanje

ANALIZA PODATKOV

Povzetek rezultatov

- vključenost zaposlenih: **visoka**
- stopnja klikov: **nad pričakovano vrednostjo**
- vnosi poverilnic: **nad ciljno vrednostjo**
- izrazita odstopanja med oddelki
- ponavljajoče napake pri delu zaposlenih

Interpretacija

- ozaveščevalni ukrep **ni dovolj učinkovit** za vse skupine
- posamezni oddelki predstavljajo **povečano tveganje**
- enkratno usposabljanje **ne zadostuje**

Povezava s tveganji

- tveganje lažnega predstavljanja ostaja **povišano**
- možnost kompromitacije poverilnic **ni zadostno zmanjšana**
- potreba po **ciljno usmerjenih ukrepih**

KAJ IN KAKO BI V TEM PRIMERU POROČALI VODSTVU?

Povzetek

- Simulacija ribarjenja je bila izvedena skladno z načrtom
- kazalniki kažejo **nezadostno učinkovitost ukrepa**
- zaznana so **odstopanja med oddelki**
- tveganje kompromitacije poverilnic ostaja **povišano**

Ključne ugotovitve

- enotno ozaveščanje **ni enako učinkovito za vse skupine**
- ponavljajoče napake kažejo na **potrebo po ciljnem pristopu**
- obstoječi ukrep zahteva **prilagoditev, ne ukinitev**

Predlagani ukrepi

Korektivni ukrepi:

- ciljno usposabljanje za oddelke z odstopanji
- ponovitev kampanje z bolj realističnimi scenariji

Preventivni ukrepi:

- prilagoditev vsebin glede na vloge zaposlenih
- pogostejše, krajše kampanje
- vključitev rezultatov v letni program ozaveščanja

Odločitev vodstva

Vodstvo odloči o:

- potrditvi predlaganih ukrepov
- dodelitvi virov
- spremljanju učinkov v naslednjem ciklu presoje

ZAKLJUČEK PRESOJE

KLJUČNE LEKCIJE IZ PRIMERA

- prisotnost varnostnega ukrepa **ne pomeni njegove učinkovitosti**
- kazalniki omogočajo **objektivno presojo**, ne občutkov
- človeški dejavnik zahteva **ciljno in prilagodljivo obravnavo**
- presoja učinkovitosti je **ponavljajoč se proces**, ne enkratna aktivnost

VREDNOST PRESOJE ZA ORGANIZACIJO

- omogoča **utemeljeno poročanje vodstvu**

- podpira odločanje o:
  - nadaljnjih vlaganjih
  - prioritetah ukrepov
  - razporejanju virov
  - prispeva k **zmanjševanju tveganj**, ne le k formalni skladnosti

NASLEDNJI KORAKI

- izvedba potrjenih korektivnih in preventivnih ukrepov
- ponovna presoja učinkovitosti v naslednjem ciklu
- uporaba rezultatov za **stalno izboljševanje ozaveščevalnih ukrepov**

Presoja učinkovitosti varnostnih ukrepov omogoča, da organizacija preide od formalne skladnosti k dejanskemu upravljanju kibernetske varnosti.

RAZMISLEK

- Kje v vaših organizacijah presoja učinkovitosti največkrat obstane? Kaj bi bil prvi ukrep, ki bi ga predlagali vodstvu?
- Kdo in kdaj določi kazalnike za ukrepe?
- Kako zagotoviti objektiven pogled?
- Kako vemo, da so kazalniki ustrezni?
- Kaj je pomembnejše: KPI ali KRI?

HVALA ZA VAŠO POZORNOST

info@enisa.europa.eu

www.enisa.europa.eu