EUROPEAN UNION AGENCY
FOR CYBERSECURITY

POSTOPKI ZA PRESOJO UČINKOVITOSTI VARNOSTNIH UKREPOV TVEGANJ

VSEBINA

- Namen in vloga politike za presojo učinkovitosti varnostnih ukrepov
- Povezava politike z zahtevami ZInfV-1 in ISO/IEC 27001:2022
- Metodologija presoje učinkovitosti varnostnih ukrepov
- Kazalniki uspešnosti in viri podatkov
- Poročanje vodstvu in stalno izboljševanje

REGULATORNI IN STANDARDNI OKVIR

- Zakon o informacijski varnosti (ZInfV-1) – zahteva po vzpostavitvi in izvajanju politike za obvladovanje tveganj ter spremljanje učinkovitosti varnostnih ukrepov
- ISO/IEC 27001:2022 – zahteva po spremljanju, merjenju, analizi in vrednotenju učinkovitosti ukrepov informacijske varnosti
- Mednarodni in evropski strokovni okviri (npr. NIST CSF, COBIT) kot podpora sistematičnemu pristopu k presoji
- Poudarek na dokazljivosti, ponovljivosti in primerljivosti rezultatov presoje

VLOGA IN POMEN POLITIKE

- politika vzpostavlja **sistematičen in ponovljiv okvir** za preverjanje, ali varnostni ukrepi dejansko obvladujejo tveganja
- omogoča **dokazljivo spremljanje učinkovitosti** tehničnih, logično-tehničnih in organizacijskih ukrepov
- predstavlja **podlago za poročanje vodstvu** o stanju informacijske in kibernetske varnosti
- omogoča **odločanje na podlagi podatkov**, trendov in odstopanj, ne zgolj na podlagi ocen ali predpostavk
- podpira **stalno izboljševanje varnostnega okolja** in krepitev kibernetske odpornosti organizacije

NAMEN POLITIKE ZA PRESOJO UČINKOVITOSTI VARNOSTNIH UKREPOV

- določiti **sistematičen pristop** k presoji uspešnosti oziroma učinkovitosti varnostnih ukrepov
- zagotoviti, da se varnostni ukrepi **spremljajo, merijo, analizirajo in vrednotijo**
- omogočiti **dokazljivo obvladovanje tveganj** za informacijsko in kibernetsko varnost
- zagotoviti **primerljive in preverljive rezultate** presoje skozi čas
- podpreti izvajanje **korektivnih in preventivnih ukrepov** na podlagi ugotovitev presoje

PODROČJE UPORABE POLITIKE

- politika se uporablja **v celotni organizaciji**
- vključuje **vse informacijske sisteme**, procese in podatkovna okolja
- nanaša se na **vse uporabnike**, ne glede na vlogo ali organizacijsko enoto
- zajema **tehnične, logično-tehnične in organizacijske varnostne ukrepe**
- upošteva **rezultate ocene tveganj** in **pretekle pomembne incidente**

CILJI POLITIKE ZA PRESOJO UČINKOVITOSTI VARNOSTNIH UKREPOV

- zagotavljanje **stalnega izboljševanja varnostnega okolja**
- prepoznavanje in odprava **pomanjkljivih, neuspešnih ali neučinkovitih varnostnih ukrepov**
- določitev **merljivih kazalnikov uspešnosti oziroma učinkovitosti**
- zbiranje in analiza podatkov za **odločanje na podlagi preverljivih dokazov**
- zagotavljanje, da se ukrepi za obvladovanje tveganj **uspešno izvajajo in vzdržujejo**

Metodologija presoje učinkovitosti varnostnih ukrepov

Vir: Chat GPT po https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Vzorcna-dokumentacija/8_POLITIKA-S-POSTOPKI-ZA-PRESOJO-UCINKOVITOSTI_ver_1.0.pdf

IDENTIFIKACIJA VARNOSTNIH UKREPOV

- identifikacija varnostnih ukrepov temelji na **rezultatih ocene tveganj**
- upoštevajo se **pretekli pomembni varnostni incidenti**
- zajeti morajo biti **vsi aktivni varnostni ukrepi**, ki vplivajo na obvladovanje tveganj
- ukrepi se razvrstijo glede na vrsto (tehnični varnostni ukrepi, logično-tehnični varnostni ukrepi in organizacijski varnostni ukrepi)

Npr.: Požarni zidovi, nadzor dostopa, šifriranje, ozaveščanje uporabnikov, itd..

Identificirani varnostni ukrepi predstavljajo ***izhodišče za nadaljnjo določitev kazalnikov in spremljanje učinkovitosti.***

DOLOČITEV KAZALNIKOV USPEŠNOSTI

- za **vsak identificiran varnostni ukrep** se določijo ustrezni kazalniki
- kazalniki omogočajo **spremljanje in merjenje**, ali ukrepi dosegajo svoj namen
- kazalniki morajo biti **merljivi, ponovljivi in primerljivi skozi čas**
- določeni so tako, da omogočajo **analizo trendov in odstopanj**
- kazalniki predstavljajo **osnovo za nadaljnjo analizo in poročanje**

PRIMERI KAZALNIKOV USPEŠNOSTI

- število zaznanih in blokiranih poskusov vdora (na določeno časovno obdobje)
- čas od pojava varnostnega dogodka do njegove zaznave
- povprečen čas za odpravo kritičnih ranljivosti po zaznavi oziroma seznanitvi
- odstotek vseh zaposlenih, ki so bili udeleženi v „anti-phishing“ kampanji in so bili neuspešni pri testiranju
- število podanih priporočil za odpravo kritičnih ranljivosti pri izvedenih varnostnih testih (varnostnih pregledov in vdornih testov)

OBVEZNI KAZALNIKI NE GLEDE NA UKREPE O KATERIH SE POROČA VODSTVU

- odstotek uporabnikov, ki so opravili usposabljanje o informacijski varnosti
- odstotek dobaviteljev, pri katerih je bilo preverjeno izvajanje varnostnih ukrepov
- odstotek uspešnih obnov podatkov po testih restavriranja varnostnih kopij

ZBIRANJE PODATKOV

- podatki se zbirajo **redno (mesečno oziroma kvartalno)**
- zbiranje podatkov temelji na **različnih tehničnih in organizacijskih virih**
- viri podatkov vključujejo:
  - SIEM / MDR / EDR / XDR sisteme
  - IDS / IPS rešitve
  - sisteme za izdelavo varnostnih kopij podatkov
  - sisteme za upravljanje tehničnih ranljivosti (ang. *patch management*)
  - rezultate revizij, samoocen in notranjih presoj
  - rezultate revizij ključnih dobaviteljev
  - rezultate izvedbe »anti-phishing« kampanj
  - obvestila in poročila uporabnikov

ANALIZA ZBRANIH PODATKOV

- analiza se osredotoča na **trende kazalnikov** in **odstopanja od pričakovanih vrednosti**
- identificirajo se **šibke točke v zaščitnih ukrepih**
- ocenjuje se **uspešnost oziroma učinkovitost odzivnih ukrepov** na varnostne incidente
- analizira se **vpliv izvedenih sprememb** na varnostno stanje organizacije

DOLOČANJE PRIČAKOVANIH VREDNOSTI

Pričakovane vrednosti se določijo glede na:

- **velikost** subjekta
- **stopnjo** izpostavljenosti tveganjem
- **verjetnost** pojava incidentov
- **resnost** morebitnih incidentov
- **družbeni in gospodarski vpliv** incidentov

POROČANJE IN UKREPANJE

- rezultati analize se predstavijo **vodstvu in odgovornim za varnost**
- poročanje poteka v obliki **poročila o uspešnosti oziroma učinkovitosti varnostnih ukrepov**
- poročilo vključuje:
  - rezultate analize zbranih podatkov
  - trende kazalnikov in zaznana odstopanja
  - priporočila za izboljšanje
  - predlog načrta **korektivnih in preventivnih ukrepov**, kadar je to potrebno

PRESOJA USPEŠNOSTI OZ. UČINKOVITOSTI OZAVEŠČEVALNIH UKREPOV „ANTI-PHISHING“ KAMPANJE

- „anti-phishing“ kampanje so **ključni ukrep za dvig kibernetske odpornosti uporabnikov**
- predstavljajo **pomemben element presoje človeškega dejavnika** v informacijski in kibernetski varnosti
- vključene so kot **sestavni del metodologije presoje učinkovitosti varnostnih ukrepov**
- omogočajo preverjanje **dejanske ravni ozaveščenosti zaposlenih** o tveganjih lažnega predstavljanja

CILJI „ANTI-PHISHING“ KAMPANJE

- preverjanje **pozornosti in ozaveščenosti zaposlenih** o tveganjih lažnega predstavljanja
- identifikacija uporabnikov, ki predstavljajo **večje varnostno tveganje**
- usmerjanje **nadaljnjih izobraževalnih in ozaveščevalnih aktivnosti**

KAZALNIKI USPEŠNOSTI OZ. UČINKOVITOSTI

- odstotek vključenih uporabnikov v kampanjo ***(cilj > 90 % zaposlenih)***
- odstotek „klikov“ na „phishing“ povezave ***(nižji je boljši; cilj < 10 %)***
- odstotek vnosov poverilnic ***(cilj < 3 %)***
- trendi uspešnosti po posameznih oddelkih ali lokacijah
- ponovitve napak pri posameznikih ***(koliko uporabnikov večkrat nasede)***

ZBIRANJE IN ANALIZA PODATKOV

- „anti-phishing“ kampanje se izvajajo **periodično (npr. vsako četrtletje)**
- rezultati se zbirajo prek **namenskih orodij za simulacijo »phishinga«**
- zbrani podatki se analizirajo **v sodelovanju s kadrovskim oddelkom**
- analiza služi zagotavljanju **ustreznih nadaljnjih korakov**

POROČANJE IN UKREPANJE

- uporabniki, ki kliknejo na »phishing« povezave ali vnesejo poverilnice, se **obvestijo in usmerijo na dodatno izobraževanje**

- agregirani rezultati »anti-phishing« kampanj se vključijo v **letno varnostno poročilo**

- rezultati se uporabijo kot **osnova za izboljšanje ozaveščevalnih vsebin in pristopa** v naslednjih kampanjah

POGOSTOST IZVAJANJA PRESOJE

- presoja uspešnosti oziroma učinkovitosti varnostnih ukrepov se izvaja **redno, najmanj enkrat letno**

- presoja se izvede **po večjih spremembah**, kot so:
  - uvedba novih informacijskih sistemov
  - večje organizacijske spremembe
  - pomembne spremembe tveganj

- presoja se izvede **v primeru pojava pomembnih incidentov**, v okviru analize po incidentu

- presoja se izvede tudi **v primeru pomembnih sprememb ocene tveganj**

ODGOVORNOSTI

- **vodja informacijske varnosti(ang. CISO)** je odgovoren za:
  - koordinacijo izvajanja presoje učinkovitosti
  - pripravo poročil o uspešnosti oziroma učinkovitosti varnostnih ukrepov
  - podajo priporočil vodstvu
- **IT oddelek oziroma pogodbeni izvajalec** je odgovoren za zagotavljanje potrebnih podatkov
- **vodstvo organizacije** je odgovorno za odločanje o ukrepih na podlagi podanih analiz in priporočil

STALNO IZBOLJŠEVANJE

- na podlagi ugotovitev presoje se politika in postopki **po potrebi posodabljajo**
- cilj posodobitev je zagotavljanje **uspešnosti oziroma učinkovitosti** varnostnih ukrepov
- politika in postopki se vzdržujejo **skladno z zakonodajnimi zahtevami**, mednarodnimi standardi in najboljšimi praksami
- stalno izboljševanje prispeva k **višji ravni kibernetske odpornosti organizacije**

HVALA ZA VAŠO POZORNOST

info@enisa.europa.eu

www.enisa.europa.eu