



Forenzična pripravljenost organizacij

- Pregled metodologije ZBS -

K.Sec, družba za svetovanje d.o.o.

**mag. Rado Ključevšek, univ.dipl.ing.rač., CISM, CISSP, MBCP, MBCI, CHFI
direktor, K.Sec d.o.o.**

Ljubljana, 9 .11. 2010

0 podjetju K.Sec



- **Sistemi informacijske varnosti**
 - Vzpostavljanje, izvedba, spremljanje in vzdrževanje ISMS skladnih z ISO/IEC 27001/27002
- **Načrtovanje neprekinjenega poslovanja**
 - Planiranje, izvedba, testiranje in vzdrževanje BCP temelječe na načelih DR11, BCI, BS 25999, ZBS
- **Drugo svetovanje pri varovanju poslovanja**
 - Upravljanje zapisov, e-arhivi (ZVDAGA, ISO 15489)
 - PKI, e-podpisi, svetovanje pri uporabi kriptografije
 - Upravljanje incidentov
 - Forenzična pripravljenost, forenzika
- **K.rmar** (www.neprekinjenostzagotovite.si), e-izobraževanja

Predstavitev predavatelja



Potek predstavitve

- Predstavitev digitalne forenzike in njen smisel
- Potrebe po forenzični pripravljenosti
- Dokazi in dokazovanje na področju informacijske tehnologije
- Pregled relevantne zakonodaje
- Koraki vzpostavitve forenzične pripravljenosti
- Osnovni forenzični odziv



Digitalna forenzika

Forenzika je uporaba znanosti pri reševanju pravnih problemov



K.Sec

Družba za svetovanje

ZAGOTAVLJAMO VARNO POSLOVANJE

- Del forenzične znanosti
 - Uporaba digitalnih tehnologij za formalno pravno dokazovanje v sodnih in drugih sporih, kjer se preiskuje IT
- Porast potreb po dokazovanju
 - Vse več je samo še digitalnih sledi
- Cilji digitalne forenzike
 - Ohranitev, ugotovitev, izbor, hramba, razlaga in dokumentiranje rokovanja z digitalnimi dokazi (dokazna sled)
 - Upoštevanje zakonitosti dokazovanja, narave pravnih procesov, zahtev za poročanje izključno na temelju dejstev
 - Nudenje strokovnega izvedenskega mnenja na sodiščih in drugih administrativnih postopkih



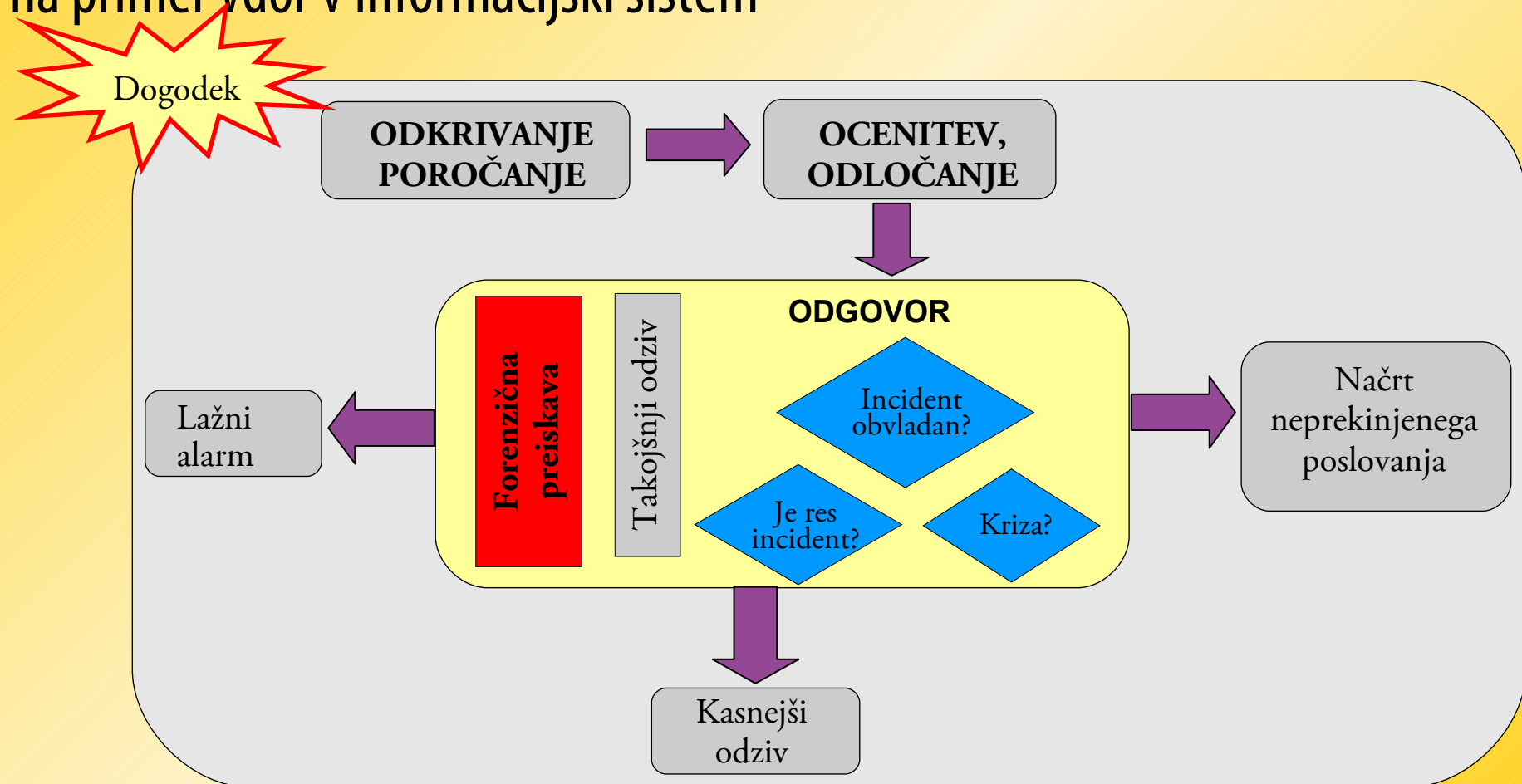
Smisel digitalne forenzike

Čedalje več je uporabe IKT
in s tem rastejo te potrebe

- Zmožnost dokazovanja dogodkov, dejanj in transakcij, ki so se zgodile na nekem računalniškem ali drugem sistemu IT
- Dokazovanje poslovnih dogodkov
 - Opravljene transakcije, dostopi, tiskanje, komuniciranje, zlorabe, prestopki proti pravilom, vdori, kriminalna dejanja ...
- Zgolj ugotavljanje dejstev z zajemanjem z namenskimi orodji
- Prva skrb
 - Ohranjanje dokazov in njihove dokazne vrednosti v izvorni obliki

Kontekst forenzične preiskave

- Tipično dojetanje povoda za preiskavo je incident
 - na primer vdor v informacijski sistem



- Vendar to ni edina uporaba!

Druga uporaba digitalne forenzike

Koristi na drugih področjih

- Odpravljanje težav pri delovanju IT in njene infrastrukture
 - Odkrivanje dogodkov, ki niso incidenti
- Okrevanje podatkov, ki so bili namerno ali slučajno zbrisani
- Hramba podatkov iz raznih virov
 - Izbris na opremi, ki se jo nato drugače uporablja
- Dokazovanje potrebne skrbnosti in skladnosti z zakonodajo in predpisi
- Spremljanje beleženja s pomočjo forenzičnih orodij

Forenzična pripravljenost [1]

- Sposobnost organizacije:
 - Maksimalna uporaba možnosti za uporabo digitalnih dokazov
 - Minimalni stroški forenzične preiskave
- Dejavniki forenzične pripravljenosti:
 - Forenzične raziskave so drage
 - Stroški preiskav so lahko majhni:
 - zbrani, pripravljeni in varovani potencialni dokazi
 - pravno sprejemljivi dokazi z visoko dokazno vrednostjo
 - Poslovna učinkovitost tudi v manjših sporih
 - obtožbe, ki se ji sicer ne bi splačali sprožiti in voditi

Smiselnost je
predvsem v zmanjševanju
potencialnih stroškov

Forenzična pripravljenost [2]

- Dejavniki forenzične pripravljenosti:
 - Majhni stroški tudi v drugih pravnih procesih
 - Organizacija v vlogi, ko se brani
 - Ko mora posredovati dokaze kot priča
 - Poznavanje možnih virov dokazov
 - Zbiranje dokazov na legalen in stroškovno učinkovit način
 - Vnaprej preišljeno
 - Izpeljevanje preiskave iz incidenta
 - Stopnjevanje forenzične preiskave
 - Vključevanje organov pregona
- Forenzične preiskave so izvzete

Kaj vse vpliva
na izgradnjo
forenzične
pripravljenosti

Stroškovna učinkovitost [1]

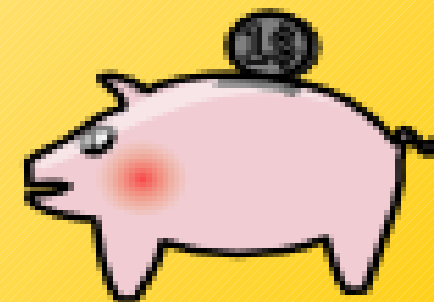
- Dejavniki stroškov:
 - Časovna usklajenost sistemov
 - Varnostna utrjenost sistemov
 - Način beleženja
 - Kaj se beleži
 - Sistem za odkrivanje vdorov
 - Način forenzičnega pridobivanja dokazov
 - Pristop k rokovanju z dokazi preiskovanca

1/2 ure napada lahko pomeni
48 ur forenzične preiskave



Stroškovna učinkovitost [2]

- Koristi forenzične pripravljenosti:
 - Zbiranje dokazov za obrambo v pravnem postopku
 - Obširno zbiranje dokazov je svarilo notranji grožnji
 - Ob incidentu se takoj lahko vodi učinkovito, nemotečo preiskavo
 - Zmanjšani stroški in čas
 - Internih preiskav
 - Zahtev sodišča, regulatorja ali pravnih zahtev za predložitev podatkov
 - Širši cilji varovanja informacij
 - Zaščita intelektualne lastnine
 - Zlorabe
 - Izsiljevanje



Stroškovna učinkovitost [3]

- Koristi forenzične pripravljenosti:
 - Izkazovanje primerne skrbnosti in dobrega upravljanja
 - Prikaz izpolnjenih regulatorskih zahtev
 - Izboljšanje in olajšanje odnosov z vključenimi organi pregona
 - Izboljšanje možnosti za uspešen pravni postopek
 - Zagotovitev dokazov za komercialne spore
 - Zagotovitev podpore sankcijam proti zaposlenim



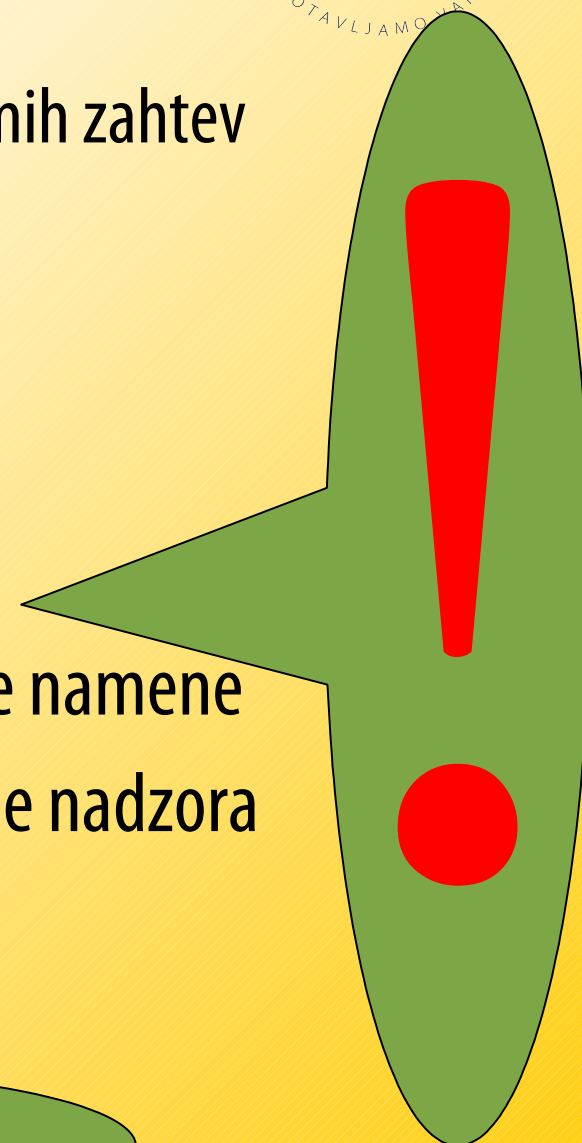
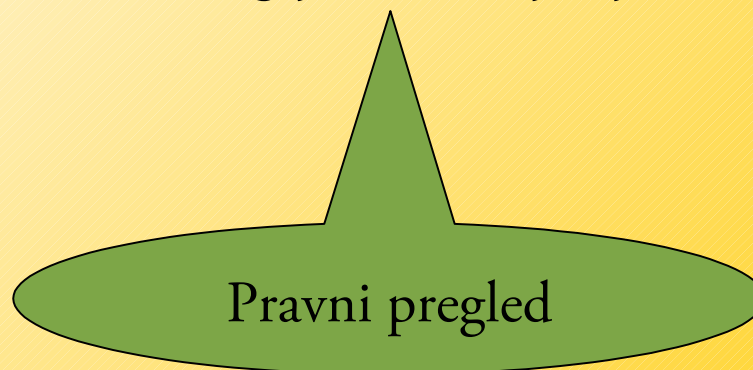
Relevantna zakonodaja

- Ustava RS
 - Nedotakljivost zasebnosti
 - Varstvo osebnih podatkov
 - ZVOP je izvedba te ustavne pravice
- Zakon o kazenskem postopku
 - Preiskava na podlagi pisne privolitve ali pisne odredbe sodišča
 - Omejitev zasega naprav
- Zakon o delovnih razmerjih
 - Delodajalec mora spoštovati delavčevo zasebnost
 - Na drugi strani je lastninska pravica delodajalca
 - Interni akti glede zasebne uporabe opreme
 - Tehta se sorazmernost pravic, upravičenost interesov

Našteta je le najbolj splošna zakonodaja!

Pogoji za forenzično preiskavo

- Opredelitev scenarijev za preiskave
 - V okviru zakonskih kontrol in pomembnih poslovnih zahtev
- Dokumentiran način nadzora
 - Sorazmeren s potrebami in posegi v zasebnost
- Seznanitev osebja z nadzorom
- Politika uporabe ITK opreme za zasebne namene
- Seznanitev osebja s politiko uporabe opreme za zasebne namene
- Seznanitev zaposlenih z uporabo tehnologije za izvajanje nadzora
- Če so vpleteni osebni podatki:
 - Pisna privolitev
 - Odredba sodišča



Metodologija za forenzično pripravljenost



- Pripravljena za Združenje bank Slovenije
 - Sistematičen pristop
 - Vključuje opredelitev vlog, odgovornosti, dokumentacije
 - Ozaveščanje, vzdrževanje
- Forenzična pripravljenost naj zagotavlja:
 - Dokaze na področju informacijske tehnologije, ki so na razpolago brez nepotrebnega dodatnega vložka pri
 - Iskanju, pripravi, analizi in zagotavljanju njihove sprejemljivosti in dokazne vrednosti
 - Pravilen odziv v okviru incidenta
 - Ne uniči dokazov na škodo hitrega okrevanja organizacije
- Deset korakov za izgradnjo forenzične pripravljenosti



Vsebina in statistika metodologije

- 3 glavna poglavja
 - Uvod
 - Forenzična pripravljenost
 - Forenzični odziv
- Statistika:
 - 65 strani
 - 32 priporočil
 - Več kot 2200 vrstic
 - Več kot 20.000 besed
- Prilagoditev branži



Osnovna dilema odziva organizacije

- Pri odzivu na dogodek, kjer se predvideva forenzična preiskava, se odločamo med dvema možnostma:
 - Izgubiti poslovanje pri izključenih informacijskih in komunikacijskih sistemih
 - Obdržati dokaze o dogajanju
 - Hitro okrevati in nadaljevati s poslovanjem ter tako močno oslabiti svojo pozicijo
 - Tvegati nevračljive izgube zaradi uničenja dokazov



Rešitev se ne sme prevaliti na IT, saj je ta kasneje v vsakem primeru označena kot napačna

10 korakov forenzične pripravljenosti [1]

Korake je predlagal Robert Rowlingson
v International Journal of Digital Evidence

- Opredelite poslovne scenarije, ki potrebujejo pridobivanje digitalnih dokazov
- Ugotovite razpoložljive vire in različne tipe možnih dokazov
- Določite zahteve za zbiranje dokazov
- Vzpostavite sposobnost za varno zbiranje dokazov izpolnjujoč ugotovljene zahteve
- Vzpostavite politiko varnega shranjevanja in rokovanja z možnimi dokazi



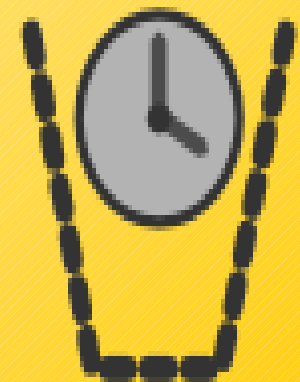
10 korakov forenzične pripravljenosti [2]

- Zagotovite usmerjenost spremljanja na odkrivanje in odvratanje večjih incidentov
- Opredelite okoliščine za sprožitev celovite formalne preiskave z digitalnimi dokazi
- Usposablajte in ozaveščajte zaposlene glede občutljivosti dokazov v pravnih procesih
- Dokumentirajte na dokazih temelječ primer in njegove vplive
- Zagotovite pravni pregled pri odzivu na incident



1. korak

- Opredelite poslovne scenarije, ki potrebujejo pridobivanje digitalnih dokazov
- Možnosti:
 - Naslonitev na ugotovljena tveganja (na primer Basel II)
 - Iz tega izhajajo scenariji z možnimi pravnimi spori in pri tem potrebnimi digitalnimi dokazi
 - Ugotovljena tveganja po ISO/IEC 27001 so tehnična in manj primerna
 - Poslovni scenariji in možne koristi organizaciji
 - Primeri iz bančnega sveta
 - Možen pristop
 - Opredelitev scenarijev opisno na podlagi vprašanj



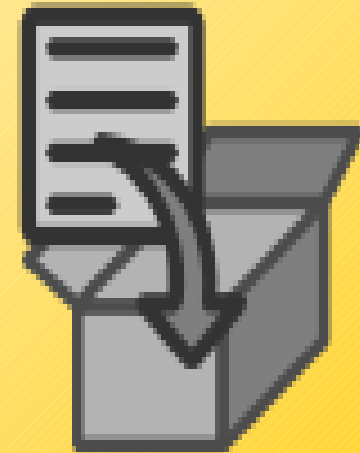
2. korak

- Ugotovite razpoložljive vire in različne tipe možnih dokazov
 - Tehnološko odvisen korak, ki nima enoznačnega odgovora
 - Vprašanja o izvorih podatkov
 - Mnogo različnih vrst in virov podatkov
 - Spremljanje aktivnosti mora biti legalno
 - Sestavljanje dokazov je lahko dvorezno



3. korak

- Določite zahteve za zbiranje dokazov
 - Že imamo zbrane dokaze za vsak scenarij?
 - Stroški zbiranja so pomembni
 - Značajan vir so lahko revizijske sledi
 - Dejavniki zbiranja
 - Meta podatki
 - Podvajanje, podkrepitev
 - Združevanje dokazov in učinkov
 - Čas hranjenja
 - Velikost dokaza, ...



4. korak

- Vzpostavite sposobnost za varno zbiranje dokazov izpolnjujoč ugotovljene zahteve
 - Preverjanje legalnosti zbiranja
 - Varovanje beležk, centralizirano beleženje
 - Fizično varovanje podatkov
 - WORM mediji
 - Principi varnega beleženja
 - Infrastruktura (SIEM), nepotrebni podatki, varovanje procesov, ravnanje ob napakah, prenos dnevniških datotek, kategorije



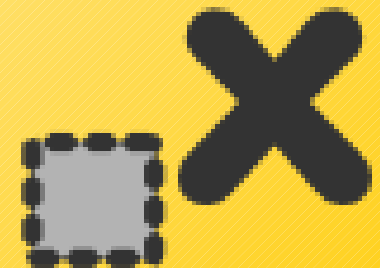
5. korak

- Vzpostavite politiko varnega shranjevanja in rokovanja z možnimi dokazi
 - Zavarovanje za daljše obdobje
 - Paradigma varnega prostora
 - Skrbniška veriga
 - Določila ZEPEP o dokazni sprejemljivosti in vrednosti
 - Hranjenje v skladu z zakonodajo
 - Principi varnosti beležk
 - Preverjanje celovitosti, omejitev dostopov, fizično varovanje, arhivski mediji, primeren format, zaščita arhiviranih dnevnikov, varno uničevanje



6. korak

- Zagotovite usmerjenost spremljanja na odkrivanje in odvracanje večjih incidentov
 - Analogija s sistemi za odkrivanje vdorov
 - Pregledi, revizije zbranih podatkov
 - Pogostnost odvisna od tveganj
 - Uporaba orodij
 - Poslovna stran določa sumljive dogodke
 - Občutljivost proženja se spreminja



7. korak

- Opredelite okoliščine za sprožitev celovite formalne preiskave z digitalnimi dokazi
 - Kriteriji za sprožitev forenzične preiskave
 - Trdnost suma, škoda, ugled, vpliv, cilj, ponavljanje, okoriščanje
 - Kdo odloča o preiskavi
 - Usposobljenost osebja in zunanja pomoč
 - Omejitev poznavanja imen preiskovalcev in njihovih vlog v njih



8. korak

- Usposablajte in ozaveščajte zaposlene glede občutljivosti dokazov v pravnih procesih
 - Osnovna pravila za vključeno osebje v incident:
 - Zabeleške
 - Poročanje
 - Izogibanje kompromitiranim sistemom
 - Očuvanje dokazov pri prvem odzivu
 - Predpisi za rokovanje z gradivom



9. korak

- Dokumentirajte na dokazih temelječ primer in njegove vplive
 - Dokumentira se pristop k izgradnji primera
 - Primeri situacij za dokumentiranje
 - Sestavni deli dokumentacije
 - Varovanje dokumentacije
 - Uporaba razbremenilnih dokazov
 - Predstavitev dokazov
 - Upravljanje napak



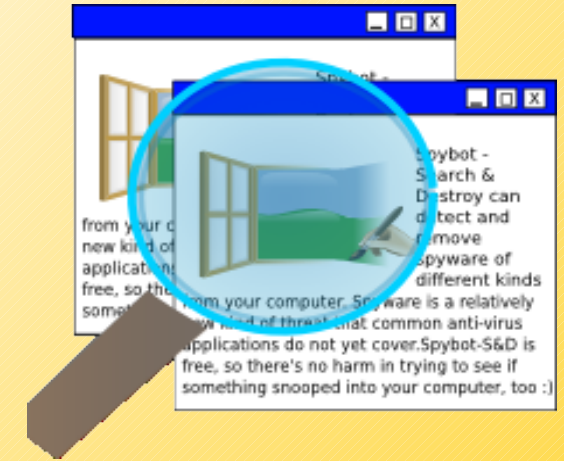
10. korak

- Zagotovite pravni pregled pri odzivu na incident:
 - Svetovanje o nadaljevanju preiskave med incidentom
 - Stroškovna učinkovitost
 - Odločanje glede na teže dokazov
 - Področja pravnih nasvetov so specifična
 - Vključevanje organov pregona, kriteriji



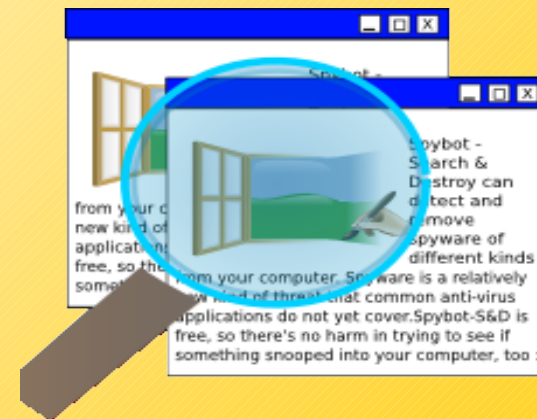
Forenzični odziv [1]

- Prvi odziv je pomemben, da se dokazi ohranijo in celo ne uničijo
- Opredeli se pristop k prvemu odzivu
 - Prilagoditev posameznim organizacijam
 - Pravni pregled
 - Odobritev s strani vodstva
- 5 osnovnih principov za zbiranje digitalnih dokazov
 - Spreminjanje podatkov, forenzična usposobljenost, revizijska sled in neodvisni pregled, odgovornost vodje preiskave in drugih oseb



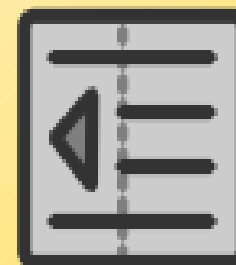
Forenzični odziv [2]

- Priprava na forenzični odziv mora biti opravljena
- Sprožitev preiskave
- Zavarovanje prizorišča
- Dokumentiranje prizorišča, beleženje!
- Diagram ukrepanja
- Postopki odzivov glede na različne situacije



Postopki forenzičnega odziva

- Postopki odzivov glede na različne situacije:
 - Ravnanje pri ugasnjenih računalnikih
 - Ravnanje pri prižganih računalnikih
 - Ravnanje pri ročnih napravah (telefoni, dlančniki, fotoaparati in podobno)
 - Pri drugih napravah, ki ji ni smiselno izključiti
- Vodenje dokumentacije o dokaznem gradivu
 - Deli skrbniške verige



Zaključni poudarki



- Forenzična pripravljenost lahko zmanjša stroške v primeru sporov
- Pravočasno se je treba pripraviti na uporabo forenzike
- Sodelovanje med IT in poslovnim delom je nujno
- Previdno pri ogrožanju zasebnosti
- Forenzična pripravljenost ni nadomestilo za delo organov pregona in ni namenjena samostojnemu preiskovanju kriminala



Hvala za pozornost!

Stik:

- info@ksec.si
- rado.kljucevsek@ksec.si
- www.ksec.si