Digital Forensics Process for Analyse

[Firmanavn]
Digital forensics process 1.0

Reference dokumenter:
Incident Response Plan (IR)
Acceptable Use Policy (AUP)
Digital Forensics Rapport

Dato / år 20XX

Ansvarlig: [Management name]

Dokument Ejer: [owner]

[Template:
This is a example mockup of a real world Business Continuity Plan (BCP)
This is subject to modification so the BCPis adjusted to the requirements to the company and comply with requirements

TLP:RED

LINK DK :https://www.cfcs.dk/da/handelser/traffic-light-protocol/
LINK EN: https://www.first.org/tlp/]

[DISCLAIMER:
Dette er lavet som en skabelon, som du kan hente og benytte som det passer dig og din virksomhed.
Dette er baseret på min viden og henvisning af begrundet viden (se defencia.dk - littertur. Det er som baggrund kombineret med min egen tilegnede erfaring!

Det vigtigste er at du benytter nedenstående i sammenhæng med begrundet gyldig viden for din virksomhed/ behov]

Ordforklaring

COC = Chain Of Custody

Artefakter = Artefakt er den fil, process, ændring mv. som er foretaget/fundet på et system i forbindelse med en skadelig handling eller hændelse

TLP:RED - Informationen er udelukkende forbeholdt hver enkelt specifik modtager og må ikke deles med andre.

Retainer aftale = Den aftale mellem [Firmanavn] og en 3 part leverandør af DFIR services. Det er en forudgående aftale om assistance til skadelige hændelser, som overskrider [Firmanavn]´s kapacitet og eller evner.

Plugins / Ingest modules = Plugins er en ekstra produkt funktionalitet i forbindelse med et stykke software som fx et forensics program.

DFIR = Digital Forensics og Incident Response

Triage = Triage er oversat fra forbinding og er set som et forsøg på at stoppe ulykken og prioritere, hvor meget analyse der skal udføres. En hurtig gennemgang af systemer eller lagringsmedier for at identificere, hvilke der indeholder data, der er mest sandsynlige at bidrage til undersøgelsen.

Live triage = Live triage er en adgang til kørende system hvor man arbejder på en PC som er tændt hvor triage anses til døde medier. Hurtig analyse af systemets aktuelle driftsstatus for at identificere tegn på kompromittering eller andre sikkerhedshændelser.

Fil Carving = Muliggør udtrækning af beviser fra beskadigede eller formaterede drev i forbindelse med cyberkriminalitet undersøgelser. Hjælper med at gendanne filer, der er blevet slettet af brugeren eller som følge af et softwarefejl.

Tags = Tags er den metode for at markere interessante fund på en maskine.

Forberedelse

[Hvad skal vi have forberedt inden da ? Se jumpbag Link:
https://www.defencia.dk/dfir/prepare/jump-bag

Dokumentation som dette dokument
Huske liste eller datafil for indsamling af artefakter for sagen.]

Retfærdiggørelse af service

IT-sikkerhedsafdelingen stiller en forensics service til rådighed for virksomheden.
Dette er for at kunne identificere Skadelige, utilsigtede og sager som modstrider lovgivningen efter landet som opereres i]

Uddannelse og forberedelse af det forensiske team.

[IT-sikkerheds-teamet skal kunne fremlægge en ren straffeattest og/ eller så på mål for en sikkerhedsgodkendelse (fx virksomheder som levere til myndigheder).
IT-sikkerheds teamet er trænet i interne processer og efter bedste praksis]

Datasikring

[Hvordan blev data indsamlet ?
Chain Of Custody (COC)
Hvem har indsamlet, haft adgang til data og hvordan blev data opbevaret og overleveret?
Hvad er datas beskaffenhed ? Mobiltelefon, PC, Netværksudstyr, Cloud, Medier]

Etablering af juridiske tilladelser og overholdelse af love og politikker.

[Hvordan overholder ledelse og HR reglerne for det gældende land?]

Bevisindsamling

Pre Analyse - Identifikation af potentielle digitale bevis kilder (computere, mobiltelefoner, netværksudstyr, cloud-tjenester).

[Hvad var den initiale indikator / Event som dannede grundlag for denne undersøgelse?

Hvor mange kilder er der indsamlet fra ?
Hvordan blev data indsamlet (se COC)
Hvad er aktive fravalg for analyse - fx mobiltelefoner
(eksempel . Dette havde ikke relevans for sagen idet, at udstyr benyttet fra kun PCére fra virksomheden]

Chain Of Custody (COC) - Sikring af beviserne for at forhindre tab, ændring eller skade.

[Hvad var omstændighederne for indsamling af data? hvad var der af fysiske omstændigheder (blev indsamlingen besværliggjort af fysiske omstændigheder? Var systemerne kun tilgængelige “live” eller “remote”]

Dokumentation af bevis indsamlingsprocessen, herunder tidsstempel, sted, og personen, der indsamler beviserne.

[Hvem var til stede? Hvad var tiden og tidszone (Også på beviset)
Hvad var specifik indsamling på det tidspunkt]

Forundersøgelse / begrundelse af mistanke for undersøgelse.

[Begrundet mistanke grundlag.
Kan vi identificere om sagen er omfattet af en straffelovsparagraf
se danskelove.dk]

Hypotese? (Malware, intern trussel (fx underslæb, brud på interne regler og lovgivning))

[Hvad omfatter sagen, hvad skal vi være opmærksom på,
Hvad skal vi søge efter?
Har vi en ordliste som ofte benyttes?]

Bevis Analyse

[Hvad skal analyseres og hvad er i fokus?
Er der områder vi skal klar over, som fx fejlfortolkning af værktøjer og kræver manuelt analyse eller validering af fund]

TLP:RED - Informationen er udelukkende forbeholdt hver enkelt specifik modtager og må ikke deles med andre.

Anvendelse af forskellige teknikker og værktøjer til at undersøge de indsamlede data.

[Hvilke værktøjer blev benyttet? for eksempel FTK, KAPE, CyLR?
Hvordan blev data indsamlet? var det live eller døde medier ?
Hvordan blev integritet tjek udført ?
Hvad var versioneringen på det software der blev benyttet?]

Genoprettelse af slettede filer og krypterede data.

[Hvilke data kunne der genskabes?
Hvad var mediet der blev genskabt fra?
Hvilket værktøj blev brugt til "fil carving"(se ord-definition]

Identifikation og dokumentation af relevante beviser, der understøtter undersøgelsen.

[Hvad er det der gør det indsamlede bevis interessant?
Hvad er det, som er specifikt fundet?

Eksempel.
Kost 1 - Malware fundet i brugerens folder (C:\Users\<Bruger>\Documents)
Kost 2 - Malware fundet i mailboks og sikret til medie <medie navn og nummer>
Kost 3 - Malware identificeret på bruger drev/tjeneste. sikret og slettet <Dato/tidsstempel>

Kort beskrivelse af fund og den interesse det skabte i skrivende stund.]

Software benyttet i samlet analyse og efterforskning

[Eksempel.
Autopsy - Version 4.21 inkluderet ingest modules fra github side <dato>
FTK - Version 4.7.1.2 - benyttet til data replikering af kost 1, kost 2 mv.
KAPE - Version 1.3.0.2
Har nogen programmer kendte fejl eller mangler, skal dette beskrives og hvorfor man benyttede værktøjet. Hvad ønskede vi at identificere / løse en opgave?]

Overvejelse mellem Virksomhed og “retainer aftale”

Hvad skal leveres til leverandøren ?

[Hvordan blev filer pakket?
Hvilken kryptering anvendes der ?
Hvad tjeneste blev benyttet til at sende filer eller fysisk levering?
Hvordan blev eventuelle pinkoder udvekslet?]

Hvad kan vi forvente ?

[Hvad skal leverandøren udføre af opgaver ?
Hvad er forventningen af opgavens udførelse ?
Hvad er tidsforbruget initialt og hvordan identificeres eventuelt et merforbrug?]

Hvad skal vi som virksomhed levere og beskrive beviset ? (se bevisindsamling) og forventningsafstemning.

Virksomhed X leverer til virksomhedens (retainer) data filer omfattende sag X. Med henblik
på analyse af data for at identificere eller bekræfte mistanke om aktiviteter af skadelig karakter]

Bevis Præsentation

Sammenstilling af fundne beviser i en struktureret rapport.

[Hvilke beviser er i fokus for sagen]

Forklaring af tekniske detaljer på en forståelig måde for ikke-tekniske interessenter.

[Kort opsummering af data og empri]

Præsentation af beviserne i retlige eller administrative processer.

[Hvad repræsenterer de forskellige artefakter, beskrevet i fagsproget.
benyt kildehenvisninger hvor dette er passende / nødvendigt]

Liste af tags og interessante fund.

[Udprint en liste af de artefakter der blev fundet interessante med deres respektive tags]

Gennemgang og evaluering

Gennemgang af processen og resultaterne for at identificere eventuelle forbedringer.

[Hvad gik godt, hvad gik skidt?
Hvad kan eventuelt forbedres ?]

Evaluering af effektiviteten af de anvendte metoder og værktøjer.

[Hvad var tidsforbruget og hvad blev analyseret automatisk baseret på værktøjerne og deres filtrering og ordliste]

opdatering af politikker og procedurer baseret på erfaringerne fra undersøgelsen.

[Blev der implementeret ændringer for processen og hvad skal dokumenteres i virksomhedens process fremadrettet ?]