Willem Loman
Senior Bedrijfsrechercheur Forensische IT
w.loman@hoffmannbv.nl

Dinsdag 15 november 2016

Digital Forensic Readiness

Inhoud

- Wat is forensic readiness?
- Waarom forensic readiness?
- Welke (technische) vragen moeten gesteld worden?
- Wat houdt digital forensic readiness concreet in?

Wat is forensic readiness?

Voorbereid zijn op een digitaal forensisch onderzoek.

Wat is forensic readiness?

Onderzoeksscenarios's:

- Lekken van vertrouwelijke bedrijfsinformatie
- Valse facturen of aangepaste betalingen
- Ongeauthoriseerde toegang tot mailboxen/documenten
- Anonieme of valse e-mailberichten
- Sabotage van computersystemen
- Ongewenst surfgedrag (privé/porno)
- Hacking/malware

Wat is forensic readiness?

Factoren die bij forensic readiness een rol spelen:

- Organisatorische maatregelen
- Menselijke factoren
- Technische maatregelen

Wat is forensic readiness?

- Voorbeelden van organisatorische maatregelen
  - Is er een ict-reglement?
  - Zijn er interne regels/procedures die invloed hebben op een (forensisch) onderzoek?
  - Zijn verantwoordelijkheden vastgelegd? (o.a. geheimhoudings-verklaringen)
  - Is er een procedure ‘vertrek systeembeheerder’?
  - Ondersteunt de informatiebeveiliging de bedrijfsdoelstellingen?
  - …

Wat is forensic readiness?

- Voorbeelden van menselijke factoren
  - Worden wachtwoorden door gebruikers gedeeld of zijn er algemene accounts in gebruik?
  - Vergrendelen gebruikers hun computer bij afwezigheid?
  - Is er bij medewerkers draagvlak voor informatiebeveiliging?
  - Zijn medewerkers in staat fishing e-mails te herkennen?
  - …

Wat is forensic readiness?

- Voorbeelden van technische maatregelen:
  - Wordt inkomende/uitgaande e-mail gearchiveerd?
  - Zijn er logbestanden beschikbaar van bijvoorbeeld het internetgebruik van medewerkers?
  - Is vast te stellen wie zich wanneer heeft aangemeld op specifieke computersystemen?
  - Wordt de toegang tot bestanden/e-mailpostbussen/databases vastgelegd?
  - …

Waarom forensic readiness?

- Doelgerichter onderzoek
- Effectiever onderzoek
- Kortere doorlooptijd
- Lagere (onderzoeks)kosten

(Technische) vragen

- Welke data is er beschikbaar, in welke vorm, hoe beveiligd en waar opgeslagen? (denk ook aan specifieke bedrijfsapplicaties)
- Over welke periode en/of hoeveel data wordt er bewaard?
- Wie heeft er (fysiek) toegang tot de data en wie beheert de data?
- Hoeveel impact heeft het opslaan van de data en het later veiligstellen ervan op de infrastructuur en de personele capaciteit?
- Wie is de eigenaar van de data? (o.a. externe dienstverleners)
- Is er een administrator wachtwoord beschikbaar bij de directie/leidinggegevenden? (kluisprocedure)
- Awareness bij beheerders

Voorbeelden van databronnen

- Desktop/laptops
- E-mail + backup/archief
- Gebruikersprofielen
- Persoonlijke netwerk schijven (homedirectories)
- Bedrijfskritische applicaties
- Logging

Voorbeelden van databronnen

Logging:

- Mailserver (inclusief webmail)
- Spam/antivirus
- Eventlogs
- Proxy
- Firewall(s)
- Routers/switches
- Wifi-gebruik
- Database-transactionlogs
- GSM/vaste telefoon specificaties
- Printers/scanners
- USB-activiteit
- Fysieke toegangsregistratie
- Alarm
- Camerabeelden
- Auditing (mail/files/folders/ rechtenwijzigingen)
- IDS

Forensic Readiness Scan

- Controle op de actuele situatie m.b.t. digital forensic readiness
- Adviesrapport met verbeterpunten

Vragen