intersoft consulting

Data protection, IT security and IT forensics: We keep you on track

Women in Forensics

Agenda

1. Who we are
2. IR/Incident Response Process
3. Memory Forensics
4. Scenario

Who we are

Svenja Mischur

Head of the IT Forensics department

M.Eng. IT Security and Forensics

Since 2016

intersoft consulting services AG

- Consulting in data protection, IT security and IT forensics
- Founded: 2006
- Locations : Hamburg, Berlin, Cologne, Frankfurt am Main, Stuttgart, Munich
- Chairman of the Board : Thorsten Logemann
  Board of Directors : Dr. Nils Chris[illegible]

Who we are

intersoft consulting

Christian

Co-Founder und CTO

Trufflepig Forensics

- Developing Software for Digital Forensics and Incident Response
- 1st Product: Trufflepig Nexus, a high-performance memory forensics software solution
- Founded: 2020

SPONSORED BY THE Federal Ministry of Education and Research

Allianz für Cyber-Sicherheit Teilnehmer

Mitglied im bitkom

Secur|Ty made in Germany Trust Seal www.teletrust.de/itsmig

GRÜNDER WETTBEWERB DIGITALE INNOVATIONEN

Agenda

1 Who we are

2 IR/Incident Response Process

3 Memory Forensics

4 Scenario

IR – Incident Response

intersoft consulting

Incident

- Classification required, whether an incident has occurred at all
- Major challenge for companies

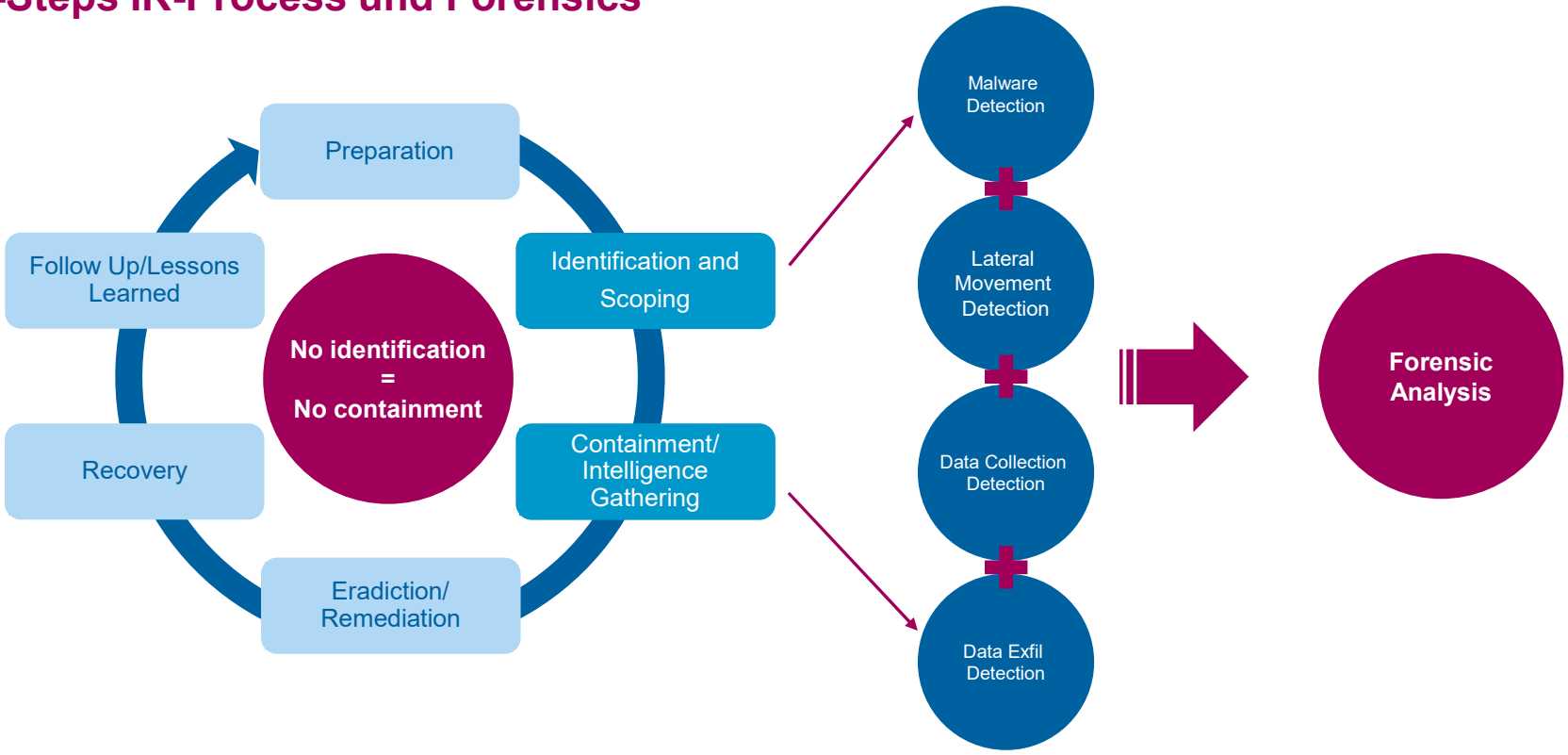
Response

- Reaction to the incident
- If an event is an incident, a reaction must follow

Incident Response Process

intersoft consulting

6-Steps IR-Process und Forensics



Agenda

1 Who we are

2 IR/Incident Response Process

➔ 3 Memory Forensics

4 Scenario

The role of memory in the forensic analysis

intersoft consulting

- Collecting memory is important for capturing the volatile data of a system
- What is in the memory:
  - Processes
  - open files, registry keys and devices
  - Encryption Keys and passwords
  - Network connections
  - Configuration Parameters
  - Memory-only exploits/ rootkit technology

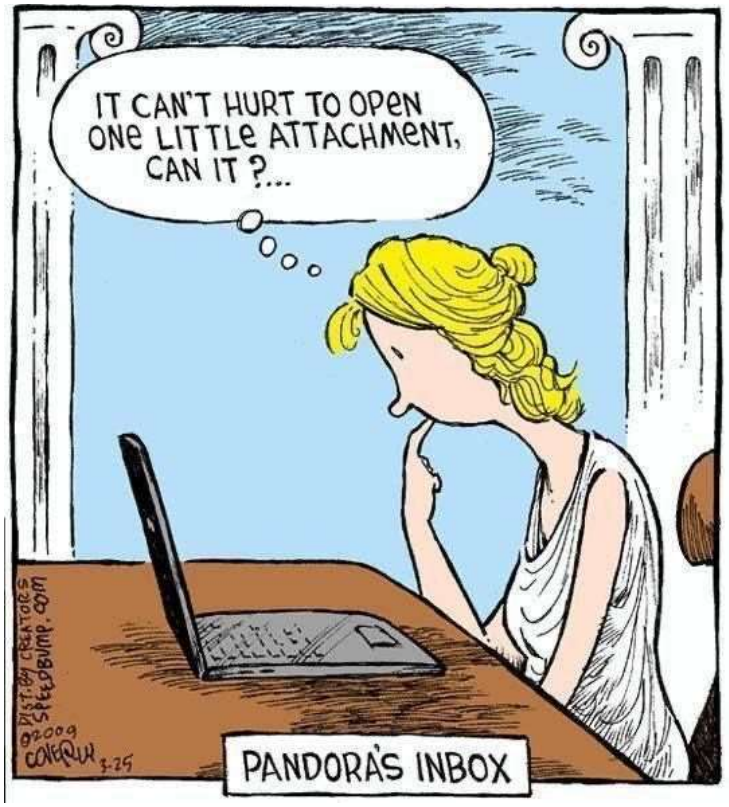
Agenda

1. Who we are
2. DFIR/Incident Response Process
3. Memory Forensics
4. Scenario

Current situation

intersoft consulting

- Incident Response requested by customer
- Attacker got credentials through a Brute Force Attack
- Attacker got control over the Domain Controller through an open SMB Share



Quelle: https://twitter.com/netzpalaver/status/1302243677604118528

Important questions

intersoft consulting

- Is the attacker still in the network? how to remove?
  - Blocking malicious IP addresses
  - Changing passwords
- Which devices are affected?
  - Rapid re-infection possible through forgotten devices
- What actions were performed by the attacker? Are important data affected?
- How did the attacker gain access to the system?
- Is there a backup?
- Have all steps been documented and hafe affected persons been informed?

What we will perform later

intersoft consulting

Together we will work on an incident response case and reconstruct what happened. We will also see how important memory forensics are in incident response cases and what information can be gathered here. Furthermore, we will give tips on how you can practice with open source tools.

- Image creation and Image mounting
- Windows Registry and other important windows artifacts for the case
- Different tools that are used to reconstruct what happened

intersoft consulting

Data protection, IT security and IT forensics: We keep you on track

Thank you for your attention

Svenja Mischur
Managing Consultant IT-Forensik
M.Eng. IT-Security und Forensics, Detective Inspector

smischur@intersoft-consulting.de
040 / 790 235 489

Follow us on Twitter:
twitter.com/Dr_Datenschutz

Subscribe our Data protection Newsletter:
www.datenschutzbeauftragter-info.de/newsletter