IT-SECURITY

ACTIONCARD - AQUISITION

Steps for aquire data

Physical surroundings

Steps for aquire data and document surroundings

- **Collection / retention of physical units**
  - Description of the collection method of the suspect's hardware.
  - Date, time and prerequisites.
  - Picture of the setup while collecting the hardware
  - Who was present? (HR, manager, technicians, etc.) Witnesses are important here.
  - Under what conditions was equipment retained? Was the equipment on or off, were there other effects involved? (FX USB or other effects)
  - If there was work on the PC at the time of detention, then it must be described exactly what happened and by whom and the period of time it took place.
  - Where was the device/s stored?
  - Was a memory dump possible?
  - How was the device sealed? We must be able to demonstrate that from detention to readout, there have been no other hands on the equipment. Possibly a picture from the package before transport and after transport
  - Transport of the device how did it happen (was the employee trusted or not)
  - It must be described where the unit has changed hands. Date time, from person to person and signature.
- **The data protection of the device, what happened here?**
  - Was a writeblock device / Software used or not?
  - Data secured to E01 with write protection and which software was used
  - Who secured the data? Time, date and HASH integrity (preferably SHA256 or above)
  - How was data stored and which form of encryption was used?
  - HASH / integrity check must be saved and or performed (depending on the software used)
- **Where is the data secured?**
- **Who has access to data after this?**

Considerations for Triangulating data for the device.

Triangualtion data is data from firewall, siem, shares, antivirus, DNS etc.

- Where is it secured to?
- What types of data are we talking about and what source is it collected from
- What does the data prove?
- Who has collected the data and who has access to the data.
- Data integrity checks must be in place.

It is very important that this is described as well as possible.

REV 1 - 2023

LARS BLOMGAARD - KEA XLEB@KEA.DK