Aufgabe Hardware: Einführung in die forensische IT-Ermittlung

Stellt Euch vor, Ihr seid frischgebackene IT-Detektivinnen und -Detektive, die an einem Tatort tätig werden müssen. Bisher habt Ihr Euch vorwiegend mit grundlegenden Hardware-Komponenten wie Bussen, Caches, Prozessoren, Speicher und Peripheriegeräten vertraut gemacht. Nun sollt Ihr erstmals in die Welt der IT-Forensik eintauchen.

In einem kleinen Unternehmen ist ein schwerwiegender IT-Sicherheitsvorfall aufgetreten. Die Geschäftsführung vermutet, dass ein Mitarbeiter unbefugt auf einen Büro-Desktop-PC zugegriffen und vertrauliche Daten manipuliert hat. Das System ist noch eingeschaltet, aber niemand weiß, ob bereits Spuren verwischt oder Hardwarekomponenten entfernt oder ausgetauscht wurden. Da Ihr als forensische Einsteigerinnen und Einsteiger gerade erst die Basiskomponenten eines Computers kennengelernt habt, sollt Ihr nun anhand dieses Szenarios erste Schritte der Spurensicherung erarbeiten.

Eure Aufgabe:
Ihr betretet den Tatort: Ein kleiner Büroraum mit einem einzigen Desktop-PC. Neben dem Rechner befinden sich externe Speichermedien (z. B. eine externe Festplatte, ein USB-Stick), ein Drucker, eventuell ein Netzwerkanschluss (auch wenn Ihr bislang über Netzwerke wenig wisst) sowie einige herumliegende Werkzeuge (Schraubendreher, Kabel, etc.). Eure Aufgabe ist es, ein Konzept zur forensischen Beweissicherung zu entwickeln, bei dem Ihr insbesondere die Euch bekannten Hardwarekomponenten mit einbezieht. Ihr sollt keine fertigen Lösungen präsentieren, sondern Euch gedanklich herantasten, welche konkreten Schritte sinnvoll wären, um den Status Quo zu dokumentieren, Spuren zu sichern und Veränderungen am System zu verhindern.

Szenario:

1. **Die Vermutung:** Ein Mitarbeiter könnte heimlich Daten von einer internen Festplatte auf einen externen Datenträger kopiert haben. Möglicherweise hat er Programme oder Skripte installiert, um bestimmte Sensorwerte auf dem Mainboard oder das BIOS des Rechners zu manipulieren. Die Geschäftsführung wünscht nun eine lückenlose Dokumentation, damit eine interne IT-Forensik-Abteilung oder, falls nötig, die Strafverfolgungsbehörden den Vorfall aufklären können.

2. **Vorgaben:**

    - Ihr habt keinerlei Anweisungen erhalten, wie man forensisch korrekt vorgeht.
    - Ihr dürft den Rechner nicht einfach abschalten, ohne abzuwägen, welche Konsequenzen dies für flüchtige Daten (z. B. im RAM) hat.

- Jede Veränderung am System könnte die Beweise verfälschen.
- Euer Wissen über Hardware ist begrenzt auf die Komponenten, die Ihr bislang kennengelernt habt. Das Netzwerkkabel liegt zwar bereit, aber Eure Kenntnisse über Netzwerkanalyse oder -verkehr sind noch rudimentär. Trotzdem solltet Ihr bedenken, dass auch hier Hinweise liegen könnten.

Aufgabenstellungen (Anleitung für eigene Recherchen):

1. **Erstmaßnahmen am Tatort:**
    - Überlegt, wie Ihr den physischen Zustand des Computers dokumentiert. Welche Hardwarekomponenten identifiziert Ihr zuerst?
    - Welche Werkzeuge oder Hilfsmittel würdet Ihr benötigen, um den Ist-Zustand eindeutig festzuhalten (z. B. fotografische Dokumentation, Siegel, Handschuhe, Schreibmaterial)?

2. **Flüchtige und permanente Speicher:**
    - Denkt darüber nach, welche Daten flüchtig sind (z. B. RAM-Inhalte) und warum deren Sicherung möglicherweise priorisiert werden sollte.
    - Welche Komponenten können permanente Daten enthalten, die später analysiert werden könnten (Festplatte, eventuell SSD, externe Speichermedien, ...)?
    - Wie könntet Ihr sicherstellen, dass keine Manipulation der Hardwarekomponenten stattfindet (z. B. durch Versiegeln von Gehäusen oder Anschlüssen)?

3. **Abbildung des kompletten Systems:**
    - Welche Schritte würdet Ihr unternehmen, um ein "Ebenbild" der aktuellen Systemzustände anzufertigen (Stichworte: Klonen von Festplatten, Hashing von Kopien, Dokumentation der BIOS-Einstellungen)?
    - Auf welchen Ebenen (physische Hardware, Speicher, Firmware) könnten Spuren liegen, und welche davon solltet Ihr zuerst sichern?

4. **Sorgfältiger Umgang mit Schnittstellen:**
    - Überlegt, welche Schnittstellen (USB-Ports, SATA-Kabel, Speicherkarten-Slots) in Eurem Szenario eine Rolle spielen. Welche Beweise könnten an externen Geräten hängen?
    - Wie könntet Ihr sicherstellen, dass ein USB-Stick oder eine externe Festplatte authentisch ist und nicht zwischenzeitlich ausgetauscht wurde?

5. **Integrität und Nachvollziehbarkeit:**
    - Welche Methoden gibt es, um die Integrität der sichergestellten Beweise zu prüfen (z. B. Einsatz von Hash-Funktionen)?
    - Wie könntet Ihr sicherstellen, dass die forensische Kette (Chain of Custody) gewahrt bleibt, also lückenlos dokumentiert ist, wer wann welche Komponenten in die Hand genommen hat?

Eure Recherche:
Nehmt Euch Zeit, um in den nächsten Stunden ein Konzept zu entwickeln, das diese Punkte adressiert. Ihr müsst keine perfekten Antworten liefern, aber nach der Zeit solltet Ihr in der Lage sein, einen strukturierten Ansatz zu präsentieren:

- Definiert einzelne Schritte in zeitlicher Reihenfolge (z. B. zuerst Dokumentation, dann RAM-Sicherung, dann Festplatten-Klon, etc.).
- Überlegt, welche Tools oder Techniken Ihr recherchieren müsstet, um diese Aufgaben korrekt auszuführen.
- Reflektiert, wo Ihr noch Wissenslücken habt, und macht Euch Notizen, welche Begriffe oder Methoden Ihr nachträglich vertiefen möchtet.

Tragt eure Informationen bitte in Form von PRÄSENTATIONSFOLIEN zusammen (gerne auch mit Inkludierung von Excallidraw-Visualierungen) und bereitet euch darauf vor, kommenden Montag dazu einen Vortrag zu halten. Wenn ihr am Montag noch Zeit für die Vorbereitung eures Vortrags braucht, bekommt ihr die natürlich.

Viel Erfolg und schon mal ein angenehmes Wochenende euch!