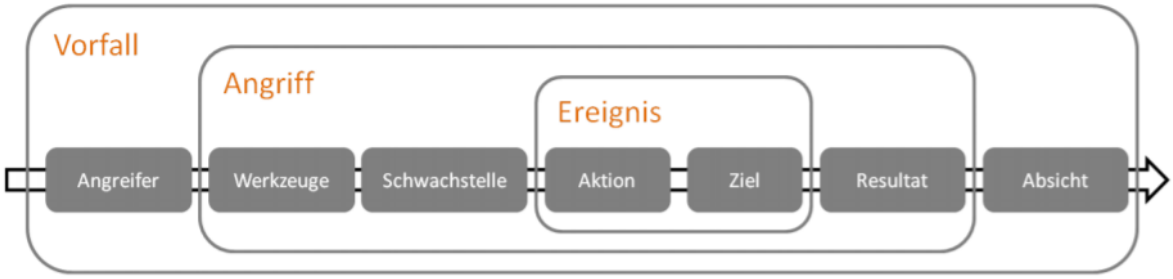
IT-Forensik

Der Begriff Forensik ist den meisten Menschen aus dem Bereich der Gerichtsmedizin bekannt. In diesem Fall bezeichnet die forensische Analyse die Aufklärung eines Vorgangs durch die Ermittlung von physikalischen oder biologischen Spuren. Diese Spuren sind Beweismittel, die Informationen über den Tathergang belegen oder die Annahme eines Vorfalls bestätigen.

Auf die IT-Forensik übertragen, bedeutet dies also die Aufklärung von Vorfällen im digitalen Bereich. Man sucht also nach digitalen Spuren, die genau wie in den anderen Gebieten der Forensik, Hinweise auf einen Tathergang liefern sollen. Eine IT-forensische Untersuchung findet immer statt, sobald ein kriminalistischer Vorfall stattgefunden hat oder angenommen wird. Neben der Aufklärung von Straftaten kann die IT-Forensik auch zum Einsatz kommen, um Störungen oder Fehlfunktionen der IT zu analysieren und aufzuklären. Eine Betriebsstörung oder zufälliger Ausfall ohne Außeneinwirkung bedingen jedoch nicht immer einer forensischen Untersuchung. Diese Vorfalls-Bearbeitung ist ein Teil des Notfallmanagements. Das Notfallmanagement schließt neben der Vorfalls-Bearbeitung auch den Wiederanlauf und die Wiederherstellung ein. Ziel der IT-Forensik ist es, exakt festzustellen, welche Aktionen auf einem IT-System stattgefunden haben und wer Verursacher oder Verantwortlicher hierfür ist.

Allgemein lässt sich die IT-Forensik in die Post-mortem-Analyse und in die Live-Forensik bzgl. des Zeitpunktes der Untersuchung einordnen.
Dabei wird bei der Post-mortem-Analyse (auch bekannt als Offline-Forensik) der Vorfall nachträglich aufgeklärt. Dies geschieht im Wesentlichen durch die Untersuchung von Datenträgerabbildern (so genannten Images) auf nichtflüchtige Spuren (zumindest in einem bestimmten Zeitraum) von Vorfällen. Das Hauptaugenmerk liegt dabei auf der Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien von Massenspeichern.
Bei der Live-Forensik (auch bekannt als Online-Forensik) hingegen beginnt die Untersuchung bereits während der Laufzeit des Vorfalls. Hier wird vordringlich versucht, so genannte flüchtige Daten zu gewinnen und zu untersuchen. Diese beinhalten unter anderem den Hauptspeicherinhalt, Informationen über bestehende Netzwerkverbindungen und gestartete Prozesse.

Um die Vorfälle zu klassifizieren und eine einheitliche und verständliche Definition des Vorfalls zu gewährleisten, wurde die CERT-Taxonomie eingeführt. Diese Taxonomie klassifiziert den Vorfall in drei Bereiche, die ineinandergreifen: Vorfall, Angriff und Ereignis.



Ein IT-forensischer Vorfall kann somit nur dann stattfinden, wenn auch ein Angreifer und eine Absicht vorliegen. Der Angriff, der von eben diesem Angreifer ausgeführt wird, bedingt neben Werkzeugen auch einer Schwachstelle im IT-System, um ein entsprechendes Resultat zu erzielen. In der Mitte steht das Ereignis, welches eine Aktion mit einem bestimmten Ziel beinhaltet.

Aufgabenstellung:

Beantworten Sie folgende Fragen!

Beschreiben Sie den Begriff IT-Forensik!

Untersuchung und Dokumentation von Daten und Systemen

Erläutern Sie das Ziel von IT-Forensik!

Einen Bericht zu haben, der im Gericht genutzt werden kann oder genutzt werden kann damit in Zukunft dieses Problem so nicht mehr auftritt

Exakt feststellen welche Aktionen auf dem IT-Systemen gemacht wurden und von wem

Nennen Sie Situationen, in denen IT-Forensik eingesetzt werden sollte!

Cyberangriff

Datendiebstahlversuche nachzuweisen

Erläutern Sie die Unterschiede zwischen einer Live- und Offline-Forensik!

Live-Forensik findest während des Vorfalls statt um Flüchtige Daten zu erfassen, während Offline-Forensik im nachhinein statt findet

Beschreiben Sie die CERT-Taxonomie!

Gliedert einen Vorfall in 3 Bereiche: Vorfall, Angriff, Ereignis