|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** Datendiebstahl von Festplatte(physisch) | **Hauptverantwortlicher**: Simeon Weigel |
| **Ziel des Angriffs**: Datendiebstahl | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure : Frau Müller , Herr Zimmermann **Fallbeschreibung**:  Frau Müller möchte ihren alten USB-Stick auf eBay verkaufen. Aus Angst, das jemand ihre persönlichen Daten lesen kann, löscht Sie ihre Daten. (Exemplarisch eine *Textdatei*: LoginnamePasswort). | |
| *1 . Ausgangssituation:* | |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *2. Nach Löschen der Datei* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Frau Müller verkauft ihren USB-Stick an Herrn Zimmermann auf ebay. Herr Zimmermann hat böse Absichten und möchte sich den Daten von Frau Müller annehmen. Dazu verwendet er das Freewareprogramm *Recuva*, mit dem sich gelöschte Daten widerherstellen lassen. |
| *3. Widerherstellen der Datei mit Recuva* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *4. Inhalt der Datei nach Widerherstellung* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Der Angreifer kann nun alle vertrauliche Daten von Frau Müller einsehen. |
| **Kommentare**: Ein mögliches Szenario wäre zudem, das man seinen USB-Stick entsorgt und ein Angreifer sich diesen annimmt. |
| Schutzmaßnahmen |
| Um sich gegen so einen physischen Angriff zu schützen, kann man seinen USB-Stick sicher überschreiben. Zum Beispiel mit dem Programm: Abylon Shredder. Mit diesem wird der Speicherplatz überschrieben und der Angreifer kann somit Dateien nicht widerherstellen. |
| *5. Sicheres Löschen der Datei* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *6. Das Programm recuva erkennt die Datei noch……* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *6. Die Datei kann jedoch nicht mehr so widerhergestellt werden, wie sie ursprünglich war* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Ein Encodieren der Zeichen ist auf keinen Fall möglich. |
| **Kommentare**:  Das Programm Abylon Shredder besitzt 5 verschiedene Sicherheitslevel:  0: normales Löschen – Verknüpfungen entfernen  1: 2x überschreiben mit binären Nullen  2: 3x überschreiben mit Nullen und Zufallszahlen  3: 7x überschreiben nach DoDII-Methode  4: 13x überschreiben DoDII und Zufallszahlen  5: 35x überschreiben (Peter Gutman Methode)  Diese Möglichkeit schützt nicht davor, wenn man vertrauliche Daten in Dateinamen schreibt. |

Zusätzlich:

Eingehen auf Verfahren der Speicherung von Daten?!(Technik genauer beschreiben?!)Warum ist es dann sicher etc.