IT Forensik

Sichere Löschung von Festplatten und Datenspeichern

Mara Schulke
Matrikelnr. 20215853, SS22 B.Sc. IT Security, THB

19. Juni 2022

Übersicht

Wieso ist eine sichere Löschung so wichtig?

- verhinderung von Datendiebstahl
- rechtliche Vorgaben
- Hardware wiederverwendbar machen

Gefahren durch falsche Löschung

- Häufige Gerätewechsel bei mangelnder Aufbereitung des Speichermediums bergen die Gefahr dass ein Angreifer diese nach Verkauf / Entsorgung rekonstruieren kann
- Selbst normale Endanwender können mittels Software wie z.B. EaseUS schlecht gelöschte Speichermedien wiederherstellen

Wie funktioniert die Rekonstruktion von Datenseichern?

- Rekonstruktion ist möglich wenn Daten nicht physisch gelöscht wurden
  - Formatierung entfernt Daten nur oberflächlich da i.d.R. nur die Zugriffstabellen angepasst werden und nicht die Register geleert werden.
- Durch durchsuchen der Register einer Festplatten mit entfernter Zugriffstabelle lassen sich softwareseitig Datenrekonstruieren
- Bei Beschädigten oder mittels SMR gesicherten Festplatten ist eine softwareseitige Rekonstruktion oft nicht mehr möglich, hier gibt es allerdings noch die Möglichkeit über physischen Zugriff auf die Festplatte Informationen wiederherzustellen (bspw. von spezialisierten Unternhemen unter Reinraum-Bedingungen)

Methoden zur sicheren Speicherlöschung

- Physische Zerstörung des Datenträgers
- Überschreiben der Daten innherlab des Datenträgers

Überschreiben gesicherter Bereiche

- Um vollständige Sicherheit zu gewährleisten müss sämtliche Bereiche eines Datenträgers überschrieben werden
- Zu typischen gesicherten Bereichen zählen die HPA (Host protected area) und das DCO (device configuration overlay)
- Programme zur Datenlöschung die vom Betriebssystem des Nutzers ausgeführt werden haben oft keinen uneingeschränkten Zugriff da das Betriebssyystem während der Löschung noch Teile des Datenträgers verwendet

Übersicht etablierter Standards

- Cryptographic Erasure (Crypto Erase)
  - Keine Runden
  - Löscht den kryptografischen Schlüssel mit der die zu löschenden Daten hardwareseitig verschlüsselt wurden
  - Funktioniert nicht mit jeder Hardware
- Peter Gutmann's Algorithm
  - Veröffentlicht: 1996
  - 1 bis 35 Runden
  - Muster: Kombination aus allen anderen Standards
- Bruce Scheier's Algorithm
  - Veröffentlicht: 1996
  - 7 Runden
  - Muster: 1, 0, 5x pseudozufällige Sequenz
- U.S. Navy Staff Office Publication NAVSO P-5239-26, 1993
  - Veröffentlicht: 1993
  - 3 Runden
  - Muster: Zeichen, Komplement, Zufallswert

Übersicht etablierter Standards

- BSI-2011-VS
  - Veröffentlicht: 2011
  - 4 Runden
  - Verschlüsselung mit AES-128-CBC mit anschließender löschung des Schlüssls
- DoD 5220.22-M (E)
  - Veröffentlicht: 1995
  - 3 Runden
  - Muster: 0, 1, Zufallswerte
- DoD 5220.22-M (C)
  - 1 Runden
  - Muster: aperiodische Zufallswerte
- DoD 5220.22-M (ECE)
  - Veröffentlicht: 2001
  - 7 Runde
  - Muster: DoD 5220.22-M (E), DoD 5220.22-M (C), DoD 5220.22-M (E)

Übersicht etablierter Standards

- U.S. Air Force System Security Instruction 5020
  - Veröffentlicht: 1993
  - 3 Runden
  - Muster: 1, 0, zufälliges Zeichen
- HMG Infosec Standard 5, Lower Standard
  - 1 Runden
  - Muster: Zufällige Zeichenkette
- HMG Infosec Standard 5, Higher Standard
  - 3 Runde
  - Muster: 0, 1, Zufallswert

Vor- und Nachteile kryptografiebasiereter Datenlöschung

Vorteile:

- Konstanter Aufwand (d.h. unabhängig von der Festplattengröße)
- Impliziert Festplattenverschlüsselung, förderlich für die allgemeine Sicherheit
- Resistent gegen alle bekannten und zukünftigen Datenwiederherstellungsverfahren

Nachteile:

- Sicherheit der Daten ist abhängig davon dass die Verschlüsselung nicht gebrochen wird

Etablierte Programme zur Datenlöschung

-

Quellen

-
-
-
-
-
-