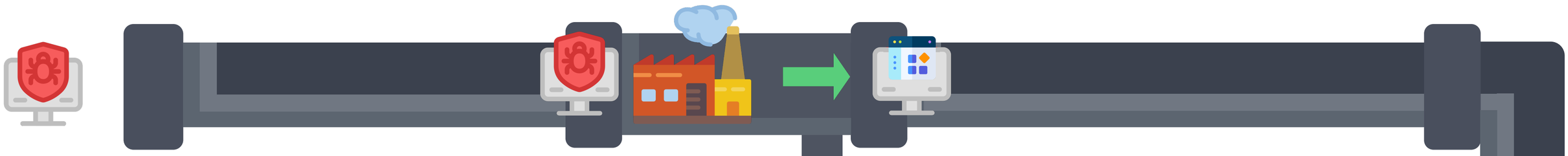
Pipeline zur Erstellung von undetektierbaren Viren



Mein Projekt

Mein Praxisprojekt konzentriert sich auf die Implementierung einer **zweistufigen Pipeline**. In einer Pipeline durchläuft eine **Eingabe** verschiedene Prozessschritte, wo sie modifiziert oder Informationen daraus extrahiert werden, um letztendlich eine **Ausgabe** zurückzugeben. In diesem speziellen Projekt ist die Eingabe ein **Virus**, das von **Antivirenprogrammen** identifiziert wird, während die Ausgabe ein Virus ist, das **NICHT** von Antivirenprogrammen Programmen erkannt wird.

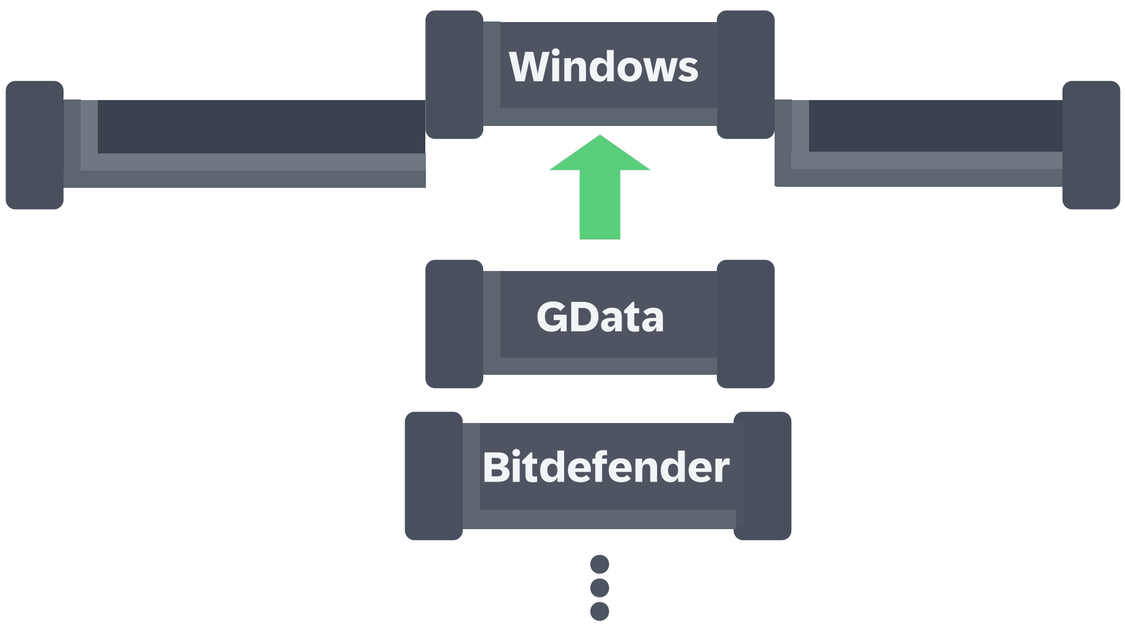
1. Stufe: Verschleiern des Virus

Die erste Stufe verschleiert die Funktion des Virus auf verschiedene Arten. Oft wird der Virus **verschlüsselt**, damit der eigentliche Zweck des Virus nicht erkannt werden kann.
Beispiel:

Print(“Hello”) → Print(decode(“i(2d=”))

Modularität

Die Pipeline ist modular gestaltet, sodass Tools einfach ausgetauscht werden können. Sie ermöglicht bspw. die Prüfung des getarnten Virus durch verschiedene Antivirenprogramme und bietet Sicherheitsteams durch einfache Hinzufüg- und Löschfunktionen hohe **Personalisierbarkeit** für spezifische Angriffsszenarien.

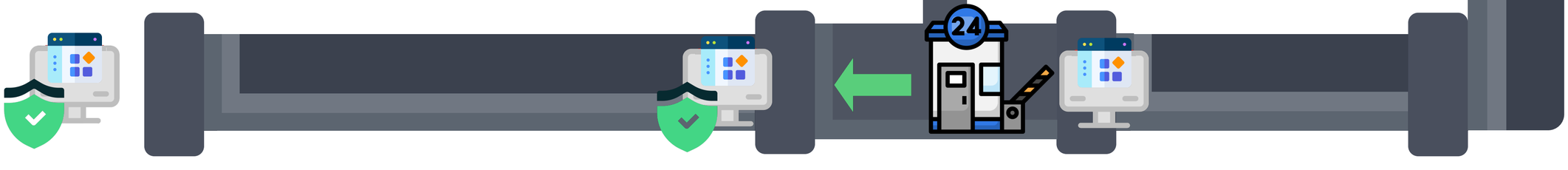


Motivation

Die steigende IT-Infrastruktur-Komplexität birgt gefährliche Schwachstellen, welche schwerwiegende Folgen haben können. Um SAPs **Reaktionsfähigkeit** auf Cyberangriffe zu verbessern, werden solche Angriffe in RedTeam-Engagements simuliert, wobei ein RedTeamer mittels Viren die Zielsysteme kontrolliert. Diese Viren dürfen nicht von Antivirenprogrammen entdeckt werden, da sonst der simulierte Angriff erkannt wird. Daher wird die Funktion der Viren verschleiert und anschließend überprüft ob sie noch von Antivirenprogrammen erkannt werden. Bisher wurden diese Schritte **manuell** ausgeführt, was sehr **ineffizient** und **zeitaufwendig** ist.

2. Stufe: Testen gegen Antiviren Programme

In dieser Stufe wird das verschleierte Virus gegen verschiedene Antivirenprogramme getestet. Der Virus wird dafür in einer Sandbox ausgeführt, um seine **Unentdeckbarkeit** garantieren zu können. Wird es nicht erkannt gibt die Pipeline das Virus zurück.



h_da hochschule darmstadt informatik

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

SAP

Praxisprojekt 2
Informatik Dual
2024

Gruppe B