**Fragenkatalog Viren**

1. Aus welchen Komponenten besteht ein Virus?

2. Erkläre die Begriffe Bootsektor, POST und BIOS.

3. Was sind Bootsektorviren?

4. Was sind Makroviren?

5. Welche Tarnmechanismen gibt es bei Viren. Erstellen sie eine kurze Erklärung je Möglichkeit.

6. Woher kommt der Begriff Malware.

7. Was sind Würmer? Worin unterscheiden sich Würmer und Viren.

8. Was ist ein Trojaner?

9. Was sind Interruptvektoren (IRQ), wie hängen diese mit Stealth Viren zusammen.

10. Was sind polymorphe Viren?

Erstellen sie pro Frage eine kurze Erklärung bzw. wo möglich eine kleine Skizze.

1. Ein Virus besteht aus einer Infektion (die Verbreitung des Virus), einer Payload (der Nutzlast/Schaden) und einer Tarnung
2. Bootsektor: Der Code im Bootsektor enthält weitere Anweisungen, wie und wo die Startdateien des Betriebssystems zu laden sind.

POST: Power-on-self-test 🡪 führt zu einer Fehlererkennung des BIOS

BIOS: wird unmittelbar nach dem Einschalten des PCs durchgeführt. Die Aufgabe des BIOS ist es den PC funktionsfähig zu machen und ein Betriebssystem einzuleiten.

1. Ein Bootsektorvirus nutzt die Tatsache aus, dass jeder Computer einmal starten muss. Ein Bootsektorvirus versucht vor dem Start des eigentlichen Betriebssystems vom befallenen Rechner ausgeführt zu werden.
2. Makros werden zusammen mit der entsprechenden Dokumentdatei gespeichert. Sie enthalten Funktionen, die dem Benutzer der Anwendungssoftware die Arbeit mit dem Dokument erleichtern, z.B. Serienbriefe. Microsoft unterstützt Makros und zwar so, dass sie beim Öffnen eines Dokuments „mitgestartet“ werden. Makroviren nutzen diese Tatsache aus, indem sie beim Öffnen eines z.B. Word-Dokuments, das infiziert ist, starten und die Infektionsroutine sucht nach weiteren Dokumenten und fügt dort den Virus als neuer Autostart-Makro ein.
3. Slackviren tarnen sich, indem sie die Tatsache ausnutzen, dass z.B. NTFS Cluster anlegt bei Dateien, die eine bestimmte KB-Größe enthalten. So ist die Datei nicht so groß, wie allerdings angezeigt wird. Eine 40.000 Bytes große Datei belegt z.B. 65.536 Bytes. Die verlorenen 25.536 Bytes werden **Slackspace** genannt. Ein Slackvirus tarnt sich so, dass er Dateien sucht, die einen größeren Slackspace haben als der Virus selbst. Dort schreibt er sich dann rein und der User sieht keinen Unterschied.

Overlayviren versuchen sich zu tarnen, indem sie sich in die Programmdatei hineinschreiben, weil viele Virenscanner nur das Dateiende von Programmen untersuchen, können sie nicht entdeckt werden.

1. Malware kommt aus dem lateinischen: malus (schlecht) oder aus dem englischen: malicious (bösartig)
2. Würmer verbreiten sich selbstständig und sind eine Art Virus. Nicht jeder (kein) Virus verbreitet sich selbstständig (Unterschied).
3. Ein Trojaner ist in erster Hinsicht kein Virus im eigentlichen Sinn, weil es sich hierbei um ganz normale Software handelt. Der Trojaner hat allerdings eine dem User nicht bekannt unerwünschte Zusatzfunktion. Diese Zusatzfunktion kann von Trojaner zu Trojaner verschieden sein.
4. Die Software-IRQs stellen grundlegende PC-Funktionalitäten zur Verfügung, auf denen Programmierer auch ohne Vorhandensein eines Betriebssystems aufbauen können. Ein Stealth-Virus leitet von der Funktion der Software-IRQ auf sich um.
5. Polymorphe Viren ändern von Infektion zu Infektion den eigenen Code, behalten aber die Funktion bei, indem sie für jedes Segment eine Alternative zur Verfügung haben.