Schutz vor Malware und Problemlösungen

2.2.1 Die Funktionsweise und die Grenzen von Antiviren-Software verstehen

Antiviren-Software durchsucht Dateien und Programme auf einem Computer nach schädlicher Software (Malware) und entfernt oder blockiert diese. Sie funktioniert meist nach folgenden Methoden:

- **Signaturbasierte Erkennung:** Die Antiviren-Software vergleicht Dateien mit einer Datenbank bekannter Malware-Signaturen. Findet sie Übereinstimmungen, wird die Malware blockiert.
- **Heuristische Analyse:** Dies ermöglicht der Software, neue oder unbekannte Viren zu erkennen, indem sie das Verhalten einer Datei beobachtet.
- **Verhaltensbasierte Erkennung:** Diese Methode prüft die Aktionen eines Programms. Wenn es sich wie ein Virus verhält, wird es blockiert.

Grenzen der Antiviren-Software:

- **Neue Malware:** Antiviren-Programme können Malware, die noch nicht in ihrer Datenbank enthalten ist, schwerer erkennen (Ein Update von Seiten des Herstellers ist notwendig um die neue Malware zu erkennen!).
- **Zero-Day-Angriffe bzw. Zero-Day-Exploits:** Diese treten auf, wenn Angreifer unbekannte Schwachstellen ausnutzen, bevor ein Update verfügbar ist.

Beispiel: Angenommen, ein Nutzer lädt einen Anhang aus einer E-Mail herunter, der ein Virus ist. Die Antiviren-Software erkennt und blockiert ihn aufgrund einer bekannten Signatur. Aber wenn die Malware brandneu ist und die Software noch kein Update hat, könnte der Virus unentdeckt bleiben.

2.2.2 Verstehen, dass Antiviren-Software auf Computern und mobilen Geräten installiert sein soll

Es ist wichtig, dass auf allen Geräten, die mit dem Internet verbunden sind – also nicht nur auf Computern, sondern auch auf Tablets und Smartphones – Antiviren-Software installiert ist. Malware zielt oft auf mobile Geräte ab, um Passwörter, Fotos oder andere persönliche Daten zu stehlen.

Warum auf mobilen Geräten?

- Viele Nutzer speichern wichtige persönliche Daten wie Bankinformationen auf mobilen Geräten.
- Auch auf mobilen Geräten können Viren durch Apps, Nachrichten oder Links auf Websites verbreitet werden.

Beispiel: Ein Benutzer installiert eine App aus einer unsicheren Quelle, die Malware enthält. Wenn die Antiviren-Software aktiv ist, kann sie die App scannen und den Nutzer warnen, bevor Schaden entsteht.

2.2.3 Die Bedeutung von regelmäßigen Software-Updates

Software-Updates sind entscheidend, um die Sicherheit von Geräten zu gewährleisten. Updates enthalten oft Patches für Sicherheitslücken, die von Hackern ausgenutzt werden könnten.

- **Antiviren-Software:** Aktualisierungen sorgen dafür, dass die Software auch neueste Malware erkennt.
- **Web-Browser und Plug-ins:** Diese Programme sind oft Angriffsziel von Malware, da sie direkten Zugriff auf das Internet haben.
- **Anwendungsprogramme:** Auch Anwendungen wie Office-Programme oder PDF-Reader können Schwachstellen aufweisen.
- **Betriebssysteme:** Sicherheitsupdates für das Betriebssystem schützen das gesamte Gerät.

Beispiel: Ein Nutzer ignoriert Updates seiner Antiviren-Software. Ein neues Virus verbreitet sich, und die veraltete Software erkennt ihn nicht, da die neue Signatur nicht heruntergeladen wurde. Regelmäßige Updates hätten dies verhindern können.

2.2.4 Laufwerke, Ordner und Dateien mit Antiviren-Software scannen

Antiviren-Software kann gezielte Scans für Laufwerke, Ordner oder Dateien durchführen. Durch regelmäßige Scans wird sichergestellt, dass das System sauber bleibt.

- **Manuelle Scans:** Benutzer können bestimmte Laufwerke oder Ordner gezielt auf Malware überprüfen.
- **Geplante Scans:** Viele Antiviren-Programme bieten die Möglichkeit, Scans zu bestimmten Zeiten automatisch auszuführen.

Beispiel: Ein Schüler plant einen wöchentlichen Scan für seinen Laptop. So werden automatisch alle Dateien regelmäßig überprüft, und neue Malware wird rechtzeitig erkannt und entfernt.

2.2.5 Risiken durch veraltete und nicht unterstützte Software

Veraltete Software kann Sicherheitslücken enthalten, die durch Updates behoben wurden. Wenn Programme oder Betriebssysteme veraltet sind, wird oft keine Unterstützung (wie Sicherheits-Patches) mehr angeboten, was die Anfälligkeit für Angriffe erhöht.

- **Inkompatibilität:** Neue Programme und Dateien funktionieren eventuell nicht mit alter Software.
- **Sicherheitslücken:** Hacker nutzen bekannte Schwachstellen aus, um Malware einzuschleusen.

Beispiel: Ein Unternehmen verwendet Windows XP, das keine Sicherheits-Updates mehr erhält. Ein Angreifer nutzt eine bekannte Schwachstelle in diesem System aus, um Malware zu installieren. Ein aktuelles Betriebssystem hätte unter Umständen diesen Angriff verhindern können.

2.3 Problemlösung und -behebung

2.3.1 Den Begriff Quarantäne verstehen

Quarantäne ist ein Bereich der Antiviren-Software, in dem verdächtige Dateien sicher aufbewahrt werden. Diese Dateien sind isoliert und können das System nicht schädigen. Quarantäne wird verwendet, wenn sich die Software nicht sicher ist, ob eine Datei wirklich infiziert ist. Wir kennen das Quarantäneverhalten noch aus der COVID Zeit, als Lockdowns für infizierte Personen verhängt wurden.

Beispiel: Ein Nutzer lädt eine Datei herunter, die verdächtig erscheint. Die Antiviren-Software verschiebt die Datei in Quarantäne, bis der Nutzer entscheiden kann, ob sie gelöscht oder wiederhergestellt werden soll.

2.3.2 Infizierte oder verdächtige Dateien unter Quarantäne stellen oder löschen

Die Antiviren-Software bietet die Option, infizierte Dateien entweder in Quarantäne zu verschieben oder vollständig zu löschen.

- **In Quarantäne verschieben:** Die Datei bleibt isoliert und kann später geprüft werden.
- **Löschen:** Wenn die Datei definitiv schädlich ist, sollte sie gelöscht werden, um die Bedrohung zu beseitigen.

Beispiel: Ein Nutzer entdeckt einen infizierten Anhang in einer E-Mail und die Antiviren-Software fragt, ob sie die Datei in Quarantäne verschieben oder löschen soll. Da die Datei infiziert ist, wählt er das Löschen, um kein Risiko einzugehen.

2.3.3 Malware-Angriffe mithilfe von Online-Ressourcen bekämpfen

Viele Anbieter bieten Online-Ressourcen an, um Malware-Angriffe zu identifizieren und zu bekämpfen. Dazu gehören:

- **Websites von Antiviren-Anbietern:** Sie bieten aktuelle Informationen über bekannte Bedrohungen und Lösungen.
- **Betriebssystemanbieter:** Microsoft, Apple und andere bieten Sicherheitsinformationen und Tools, um das System sicher zu halten.
- **Behörden und Organisationen:** Websites wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellen Sicherheitswarnungen und Handlungsempfehlungen zur Verfügung.

Beispiel: Ein Schüler vermutet, dass sein Computer mit Malware infiziert ist. Er besucht die Website seines Antiviren-Software-Anbieters und lädt ein spezielles Tool zur Malware-Entfernung herunter, welches das Problem behebt.

2.3.4 Online-Ressourcen zur Malware-Bekämpfung: VirusTotal.com

VirusTotal.com ist ein nützliches Online-Tool, das Dateien und URLs kostenlos auf Malware überprüft. Es scannt die Datei oder URL mithilfe von über 70 Antiviren-Scannern und mehreren Analyse-Tools, um verdächtige Inhalte zu erkennen. Dies bietet eine zusätzliche Schutzebene, insbesondere wenn die eigene Antiviren-Software nichts gefunden hat.

Funktionsweise von VirusTotal.com:

1. **Datei-Upload:** Nutzer können eine verdächtige Datei hochladen, und VirusTotal scannt diese mit verschiedenen Antiviren-Programmen.
2. **URL-Prüfung:** Man kann auch URLs eingeben, um Websites auf schädliche Inhalte zu prüfen.
3. **Ergebnisse ansehen:** Die Seite zeigt detaillierte Ergebnisse, darunter eine Liste der Antiviren-Scanner, die die Datei oder URL geprüft haben, und welche sie als sicher oder gefährlich einstufen.

Beispiel: Ein Schüler erhält eine E-Mail mit einem verdächtigen Anhang. Bevor er ihn öffnet, lädt er die Datei auf VirusTotal.com hoch, um sicherzustellen, dass sie keine Malware enthält. Mehrere Scanner melden die Datei als gefährlich, woraufhin der Schüler die Datei nicht öffnet und seinen Lehrer informiert.

Hinweis: VirusTotal ist kein Ersatz für eine lokal installierte Antiviren-Software, sondern eine Ergänzung für Fälle, in denen die eigene Software keine Bedrohung erkennt.