smARTen begleiten

Das Konzept des smARTen begleiters sieht vor, Lehrbücher mithilfe einer Lernapplikation für DICH interessanter zu gestalten.
Der smARTe Begleiter unterstützt dich aktiv im Lernprozess mithilfe von interaktiven und unterhaltsamen AR-Elementen.
Mit der Lernapp kannst Du dir jederzeit effektiv, leicht und mobil Wissen aneignen – ob Zuhause oder unterwegs, der smARTe begleiter ist TO-GO.

Hier eine kurze Übersicht über die Funktionen des smARTen begleiters:

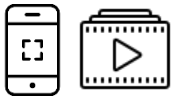
1. STUDY WITH TEXTBOOK

Eigne dir den Sachverhalt mit den smART Lehrbüchern an. Lerne bequem wie gewohnt Deine gewünschte Thematik und markiere oder unterstreiche Dir, die für Dich wichtigen Stichworte, um dir den Inhalt besser zu merken.

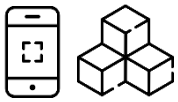
2. SCAN MARKERS

Der smARTe begleiter bietet verschiedene Marker mit verschiedenen Funktionen an, die dir das Lernen einfacher und unterhaltsamer machen:

Triffst Du auf dieses Symbol, ist es Zeit zum Scannen !



Erblickst Du eine Kombination aus diesen Symbolen, wird dir ein lehrreiches Video angezeigt, mit der Du dir den Inhalt noch etwas besser zu verinnerlichen kannst.



Triffst Du auf eine Kombination aus diesen beiden Symbolen und scannst das Bild ein, erscheint ein 3D Modell, mit der Du interagieren kannst.

TEST YOURSELF – Scannst Du das Bild mit diesem Marker, erscheint ein Quiz mit der Du dein gelerntes Wissen anhand von inhaltsrelevanten Fragen und Aufgabenstellungen testen kannst.

Definition einer Maleware im Wikipedia-Stil

Der Begriff „Malware" – ein Zusammenschluss der Wörter „Malicious" (schädlich) und „Software" – wird heute verwendet, um schädliche Programme jeder Art auf Computern oder mobilen Geräten zu beschreiben. Diese Programme werden ohne Zustimmung des Benutzers installiert und können eine Reihe unangenehmer Folgen haben. So können sie beispielsweise die Systemleistung reduzieren, innerhalb Ihres Systems nach persönlichen Daten suchen, Informationen löschen oder sogar den Betrieb computergesteuerter Hardware beeinträchtigen. Hacker entwickeln immer raffiniertere Methoden, um in Systeme einzudringen, und sorgen so für eine wahre Flut auf dem Malware-Markt.

Oft wird der Begriff Computervirus als Überbegriff für sämtliche Malware, die einen Rechner befallen kann, benutzt. Das ist nicht korrekt, da es sich beim Computervirus nur um eine bestimmte Art von Malware handelt und sich der Begriff Virus auf die Infektion unter Nutzung einer Wirtsdatei bezieht.

Sehen wir uns einmal einige der häufigsten Malware-Arten an.

1. Computerviren

Computerviren haben ihren Namen durch die Fähigkeit erhalten, mehrere Dateien auf einem Computer zu „infizieren". Sie verbreiten sich auf andere Geräte, wenn diese infizierten Dateien per E-Mail versendet oder über einen Wechseldatenträger, wie z. B. einen USB-Stick oder (damals noch) eine Diskette, übertragen werden. Laut National Institute of Standards and Technology (NIST) wurde der erste Computervirus namens „Brain" 1986 entwickelt. Zwei Brüder waren es leid, dass Kunden die Software aus ihrem Geschäft illegal kopierten, und entwickelten so den Virus, der den Boot-Sektor der Disketten von Softwaredieben infizieren sollte. So wurde der Virus beim Kopieren der Disketten weitergegeben.

2. Würmer

Im Gegensatz zu Viren sind Würmer nicht auf menschliche Hilfe angewiesen, um sich zu verbreiten: Sie infizieren ein Gerät und nutzen dann Computernetzwerke, um sich auf andere Computer zu verbreiten – ohne Zutun der Benutzer. Indem sie Schwachstellen in den entsprechenden Netzwerken, wie z. B. Sicherheitslücken in E-Mail-Programmen, ausnutzen, können Würmer Tausende Kopien von sich versenden, um so neue Systeme zu infizieren und den Prozess erneut durchzuführen. Während viele Würmer früher lediglich Systemressourcen verbrauchten und so die Leistung reduzierten, enthalten die meisten neuen Würmer sogenannte „Payloads", die dazu dienen, Dateien zu stehlen oder zu löschen.

3. Trojanische Pferde

Diese Programme werden im Allgemeinen nur als „Trojaner" bezeichnet und tarnen sich als legitime Datei oder Software. Einmal heruntergeladen und installiert, nehmen Trojaner Änderungen am Computer vor und führen ohne Wissen oder Zustimmung des Opfers schädliche Aktivitäten durch.

4. Adware

Eines der am weitesten verbreiteten Online-Ärgernisse ist Adware. Diese Programme zeigen automatisch Werbeanzeigen auf dem Host-Computer an. Bekannte Arten von Adware sind beispielsweise Pop-up-Werbeanzeigen auf Webseiten oder in vermeintlich kostenlosen Anwendungen integrierte Werbung. Zwar ist viele Adware verhältnismäßig harmlos, jedoch gibt es Varianten, die Tracking-Tools nutzen, um Ihren Standort oder Ihren Browserverlauf zu ermitteln und gezielte Werbeanzeigen auf Ihrem Bildschirm anzuzeigen. BetaNews berichtet sogar von einer neuen Form von Adware, die Ihre Antiviren-Software deaktivieren kann. Da Adware mit Kenntnis und Zustimmung des Benutzers installiert wird, kann sie nicht als „Malware" bezeichnet werden. Deshalb wird sie häufig als „potenziell unerwünschte Programme" bezeichnet.

5. Spyware

Spyware (kurz für „Spionagesoftware") tut genau das, was ihr Name vermuten lässt: Sie spioniert Ihren Computer aus. Sie erfasst Daten, wie z. B. Ihre Tastenanschläge, Surfgewohnheiten und sogar Anmeldedaten, die dann an Dritte gesendet werden – für gewöhnlich Cyberkriminelle. Sie kann auch bestimmte Sicherheitseinstellungen auf Ihrem Computer ändern oder Ihre Netzwerkverbindungen beeinträchtigen. Laut TechEye bieten neue Arten von Spyware Unternehmen sogar die Möglichkeit,

das Verhalten ihrer Benutzer über verschiedene Geräte hinweg nachzuverfolgen – und das ohne ihre Zustimmung.

6. Ransomware

Ransomware infiziert Ihren Computer, verschlüsselt vertrauliche Daten, wie z. B. persönliche Dokumente und Fotos, und verlangt ein Lösegeld für ihre Entschlüsselung. Wenn Sie die Zahlung verweigern, werden die Daten gelöscht. Manche Ransomware-Varianten blockieren auch gleich den gesamten Zugriff auf den Computer. In den Lösegeldforderungen wird möglicherweise behauptet, es handele sich um legitime Strafverfolgungsbehörden, die Sie bei illegalen Aktivitäten erwischt haben. Im Juni 2015 erhielt das Internet Crime Complaint Center des FBI Beschwerden von Benutzern, die durch eine gewöhnliche Ransomware namens CryptoWall insgesamt einen Schaden von 18 Millionen US-Dollar erlitten hatten.

7. Bots

Bei Bots handelt es sich um Programme, die automatisch bestimmte Aktionen durchführen sollen. Sie dienen vielen legitimen Zwecken, können jedoch auch als eine Art von Malware zweckentfremdet werden. Einmal auf einem Computer angelangt, können Bots das Gerät dazu bringen, bestimmte Befehle auszuführen – ohne Wissen oder gar Zustimmung des Benutzers. Hacker können auch versuchen, mehrere Computer mit dem gleichen Bot zu infizieren, um so ein sogenanntes „Botnet" (kurz für „Roboternetzwerk") zu schaffen, das für die Remote-Steuerung der infizierten Computer genutzt werden kann. Mithilfe eines Botnet stehlen Cyberkriminelle vertrauliche Daten, spionieren die Aktivitäten ihrer Opfer aus, verbreiten automatisch Spam oder führen verheerende DDoS-Angriffe auf Computernetzwerke durch.

8. Rootkits

Rootkits ermöglichen den Remote-Zugriff auf einen Computer zur Fernsteuerung durch Dritte. Diese Programme sind äußerst nützlich für IT-Experten, die Netzwerkprobleme an entfernten Standorten beheben müssen. Sie können jedoch auch schnell zur Gefahr werden: Sind sie einmal installiert, ermöglichen es Rootkits den Angreifern, die vollständige Kontrolle über das Gerät zu übernehmen, um Daten zu stehlen oder andere Malware zu installieren. Rootkits arbeiten unbemerkt und verschleiern ihre Existenz. Die Erkennung dieser Art schädlichen Codes erfordert die manuelle Überwachung auf ungewöhnliches Verhalten sowie die regelmäßige Installation neuer Patches für Betriebssystem und andere Software, um potenzielle Infektionsvektoren zu beseitigen.

9. Bugs

Sogenannte „Bugs", also kleine Fehler im Softwarecode, stellen keine Art von Malware dar, sondern einfach Fehler der Programmierer. Auch sie können sich jedoch schädlich auf Ihren Computer auswirken, beispielsweise in Form von Abstürzen oder einer Verringerung der Systemleistung. Sicherheitsfehler jedoch bieten Angreifern Möglichkeiten, die Verteidigung zu umgehen und das Gerät zu infizieren. Durch Sicherheitskontrollen versuchen Entwickler, solche Fehler zu beseitigen. Es ist jedoch zwingend erforderlich, die entsprechenden Software-Patches auch zu installieren.

Mythen und Fakten - Um Computerviren ranken sich viele Mythen

Jede Fehlermeldung zeigt eine Vireninfektion an. Das stimmt nicht: Fehlermeldungen können auch durch Hardware- oder Softwarefehler auftreten.

Viren und Würmer verbreiten sich nur mit Zutun des Benutzers. Das ist falsch. Es muss zwar Code ausgeführt werden, damit ein Virus einen Computer infizieren kann, hierfür ist jedoch keine Benutzerinteraktion erforderlich. So kann beispielsweise ein Netzwerkwurm Geräte automatisch infizieren, wenn bestimmte Schwachstellen auf dem entsprechenden Computer vorhanden sind.

E-Mail-Anhänge von bekannten Absendern sind sicher. Das ist nicht wahr: Schließlich können auch bekannte Absender mit einem Virus infiziert sein und die Infektion verbreiten. Selbst wenn Sie den Absender kennen, öffnen Sie keine Anhänge, bei denen Sie sich nicht absolut sicher sind.

Antiviren-Lösungen halten alle Bedrohungen auf. Zwar tun Virenschutz-Anbieter ihr Bestes, um auf dem neuesten Stand der Malware-Entwicklung zu bleiben, jedoch ist auch eine umfassende Lösung für Internetsicherheit erforderlich, die mit ihren Technologien Bedrohungen frühzeitig blockieren kann. Und selbst dann lässt sich 100-prozentiger Schutz nicht garantieren. Deshalb ist es wichtig, beim Surfen auf gewisse Dinge zu achten, um das Risiko eines Angriffs zu reduzieren.

Viren können einen physischen Schaden anrichten. Und was passiert, wenn schädlicher Code dazu führt, dass Ihr Computer überhitzt oder dass wichtige Chips beschädigt werden? Virenschutz-Anbieter haben diesen Mythos schon viele Male widerlegt: Solche Schäden sind einfach nicht möglich.

Sind Handys von Maleware geschützt?

Bei iPhones werden Apps ausschließlich über den „App Store" geladen. Bevor dort neue Apps freigegeben werden, kontrolliert Apple diese auf Viren, Trojaner und Würmer. iPhone-Besitzer fangen sich daher nur sehr selten einen Virus ein.
Google geht bei Android-Smartphones mit dem „Google Play Store" ähnlich vor. Installierte Apps werden regelmäßig mit dem Virenscanner „Google Play Protect" auf schädliche Software geprüft.

Wird ein Virus gefunden, kann Google die App auch aus der Ferne von eurem Smartphone löschen.

Allerdings lassen sich auf Android-Handys auch Apps von anderen Webseiten installieren – mittels sogenannter APK-Dateien. Google hat dann keinen Einfluss darauf, ob die entsprechende APK-Datei virenfrei ist. Nutzer, die sich APK-Dateien zum Installieren von Apps von anderen Webseiten herunterladen, sollten der Webseite also vertrauen können. Außerdem hängen einige Smartphone-Hersteller mit Android- und Sicherheitsupdates hinterer, wodurch die Gefahr für Viren ebenfalls steigt.

Ist der Nutzer nicht vorsichtig, kann er sich Viren auch über E-Mails, SMS, MMS und Downloads einfangen. Ist man in einem öffentlichen WLAN eingeloggt, kann dort ebenfalls schädliche Software übertragen werden.

Anzeichen für einen Handy-Virus

Ein Virus kann das gesamte Smartphone kontrollieren und/oder auch private Daten zugreifen und etwa E-Mails oder Passwörter mitlesen. Das wäre besonders beim „Mobile Banking" auf dem Handy gefährlich. Anzeichen für einen eingefangenen Virus sind:

- Das Smartphone zeigt plötzlich Werbung (auch außerhalb des Browsers).
- Ihr werdet aufgefordert Lösegeld zu zahlen, damit ihr wieder auf eure Daten zugreifen könnt (Ransomware).
- Der Akku wird plötzlich schneller leer als üblich
- Euer Smartphone installiert selbstständig dubiose Apps
- Euer Smartphone reagiert nicht richtig mehr auf eure Eingaben

Startet ein Android-Smartphone im sicheren Modus, um herauszufinden, ob ihr einen Virus habt. Sind nun beispielsweise die Werbeeinblendungen verschwunden, ist das Smartphone wahrscheinlich von einem Virus befallen.

Quellen:

- https://www.kaspersky.de/resource-center/threats/computer-viruses-and-malware-facts-and-faqs
- https://www.giga.de/tipp/virus-auf-handy-entfernen-das-koennt-ihr-tun/

(Bilder)

- https://de.123rf.com/photo_30113816_malware-oder-computer-virus-warnzeichen-vektor-illustration.html
- https://de.cleanpng.com/png-vhrrhu/
- https://www.pngegg.com/de/png-wupgs
- https://de.dreamstime.com/lizenzfreies-stockbild-computervirus-image35868036