2 MALWARE

2.1 Arten und Funktionsweisen

Als *Malware* bezeichnet man Computerprogramme, die unerwünschte, meist auch schädliche Aktionen ausführen.

Grayware ist nicht immer bösartig und wird daher nicht unbedingt als Virus kategorisiert. Sie ist weder ein wirkliches Schadprogramm noch harmlose Software weil alleine durch ihre Aktionen störend wirken kann (zB Pop-up Fenster mit Werbung).

2.1.1 Malware erkennen

Oft wird „Computervirus“ irrtümlich (leider auch von Fachleuten) als Synonym von Malware verwendet, was darauf zurückzuführen ist, dass Viren die ersten Schadprogramme waren, die die Computerleistung beeinträchtigten. In der Zwischenzeit sind Schädlinge mit ganz unterschiedlichen Arbeitsweisen entwickelt worden, sodass eine genaue Differenzierung dieser Programme notwendig wurde. Als Sammelbegriff hat sich das Kunstwort *Malware*, zusammengesetzt aus **mal**icious (bösartig) und Soft**ware** etabliert.

Bezeichnung	***Wirkung***
Virus	Ein einfacher Virus wird durch Aufruf des Programms, in dem er sich eingenistet hat, aktiv. Er verbreitet sich durch Aktivierung der infizierten Datei auch auf andere Dateien und innerhalb des Netzwerkes. Je nachdem, wo der Virus wirkt, unterscheidet man Computer-, Datei-, System-, Makro- und Bootviren.
Wurm	Die Wirkung entspricht dem eines einfachen Virus. Er verbreitet sich allerdings automatisch, beispielsweise über das Adressmaterial für E-Mails. Dazu nutzt er die Sicherheitslücken des Betriebssystems.
Trojaner	Programme, die als nützliche Anwendung in das Computersystem eingeschleust werden, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllen, meist zum Schaden des Anwenders. Mit solchen Programmen kann der *Hacker* Passwörter oder Tastatureingaben herausfinden, um damit einen Zugang in den Computer, aber auch auf Bankkonten des Anwenders erlangen. Je nach Infektionsfunktion werden differenzierte Begriffe verwendet: Backdoor-Trojaner, PWS-Trojaner, Trojan-Downloader …
Hoax	Wörtlich Scherz oder Falschmeldung; meistens erfolgt eine derartige Scherz- oder Falschmeldung mittels E-Mail. Sie gibt bekannt, dass ein Virus unterwegs sei, und fordert den Anwender auf, eine bestimmte Aktion auszuführen. Ein Hoax soll meist nur erschrecken.

Bezeichnung	*Wirkung*
DoS-Attacken	Denial of Service (DoS)-Attacken, die im Internet zur Beeinträchtigung von Webservices führen; zB kann es durch die Versendung einer Vielzahl von E-Mails oder durch Bombardierung mittels Anfragen zur Überlastung von Servern kommen. Dadurch können andere Aktionen nicht mehr hinreichend ausgeführt werden. Die Server sind durch Überlastung nicht mehr erreichbar.
Spyware	Durch Spying (Spionieren) wird das Online-Verhalten von Webnutzern beim Surfen ausspioniert und dieses Wissen an andere weiter gegeben. Aus den Ergebnissen, die in der Regel in Tabellen gespeichert und über E-Mails an den Urheber gesendet werden, können Rückschlüsse auf das Konsumverhalten gezogen und die Werbewirksamkeit durch gezielten Einsatz von abgestimmten Methoden gesteigert werden.
Rootkit	Ein Rootkit ist eine Software, die im Hintergrund versucht, einen Fremdzugriff zu ermöglichen um vertrauenswürdige Daten weiterzusenden. Der Name kommt von Root (engl. für Wurzel; Administratorebene), in dem es installiert wird, um damit zukünftige Logins eines Eindringlings zu verbergen und Prozesse und Dateien zu verstecken. Diese Programme positionieren Malware so gut im System, dass selbst viele Virenscanner sie nicht mehr finden.
Backdoor-Trojaner	Es sind die gefährlichsten und häufigsten Trojaner. Mit einem Backdoor-Trojaner kann der Urheber oder „Master“ des Trojaners mit Hilfe von Fernadministration den Opferrechner angreifen. Im Gegensatz zu den legitimen Fernadministrationsprogrammen können Sie den Backdoor-Trojaner nicht erkennen. Dadurch werden ohne Ihr Wissen Programme installiert, gestartet und genutzt. Wenn Backdoor-Trojaner einmal installiert sind, können sie Dateien verschicken, empfangen, ausführen oder löschen, sie können vertrauliche Daten aus dem Computer entnehmen oder Computeraktivitäten protokollieren.

2.1.2 Selbst verbreitende Malware

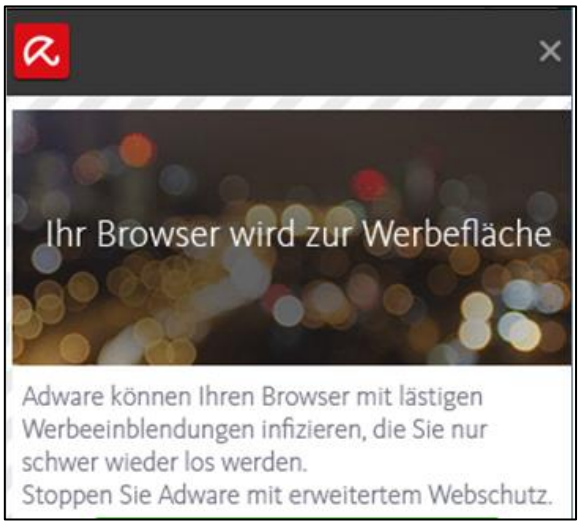
Ein Virus ist ein Programm, das andere Programme „infizieren“ kann. Dabei kann das infizierte Programm so verändert werden, dass dieses eine möglicherweise mutierte Kopie vom Virus-Programm enthält. Infiziert bedeutet, dass sich der Virus in die Befehlskette des ursprünglichen Programms (Wirtsprogramm) einschleust, so dass der Versuch, ein legitimes Programm auszuführen, auch gleich zur Ausführung des Virus führt.

Ein Wurm ist ein Programm, das sich selbst kopiert und verbreitet, ohne sich an ein Wirtsprogramm anzuhängen. Ein Wurm wandert über Netzwerkverbindungen von einem Computer oder mobilen Gerät zum nächsten. Die „Absicht“ der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen. Würmer vermehren sich durch Kopieren und brauchen keine weiteren Befehle, um sich innerhalb eines Firmennetzwerks oder über das Internet zu verbreiten.

2.1.3 Arten von Malware

Adware

Adware ist eine werbeunterstützende Software, mit der Werbebanner automatisch eingeblendet, abgespielt werden oder auch Downloads gestartet werden. Adware-Programme werden oft in Freeware[7] oder Shareware[8] - Programme eingebaut, wo sie sich dann indirekt über die Nutzung des Werbebanners gegenfinanzieren.



Durch das Einblenden von Werbung wird das Lesen der Webseiten beeinträchtigt. Zudem hat Adware häufig einen Code, mit dem persönliche Informationen der Nutzer ohne deren Kenntnis ausspioniert werden.

Ransomware

Ransomware, auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann.

Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter erpressen ihre Opfer, indem sie deutlich machen, dass der Bildschirm oder die Daten nur nach einer Lösegeldzahlung wieder freigegeben werden.

Meistens wird angegeben, dass der User angeblich illegale Aktivitäten vorgenommen hat, die mit einer Strafe von 50 bis 100 Euro abzugelten seien. Ebenso wird versprochen, den Computer nach Zahlung wieder zu entsperren. Dieses erfolgt in der Regel nicht. Aus diesem Grund sollten niemals Zahlungen erfolgen, sondern sofort eine Virenüberprüfung vorgenommen werden.

Botnet

Ein Botnet oder Botnetz ist eine Gruppe von Bots[9]. Die Bots laufen auf vernetzten Rechnern und nutzen die Ressourcen des lokalen Rechners ebenso wie die Verbindung zu den im Netz verfügbaren Computern.

Man unterscheidet „gutartige“ Bots und „bösartige“ Bots. Letztere werden beispielsweise zum Sammeln von E-Mail-Adressen für Werbezwecke, für das mas-

---

[7] **Freeware**; Programme, die zur kostenlosen Nutzung bereit gestellt werden.

[8] **Shareware**; Vertriebsform für Software. Software wird zum Test auf eine gewisse Zeit kostenlos zur Verfügung gestellt und kann danach nach Bezahlung einer Lizenzgebühr dauerhaft genutzt werden.

[9] Unter einem **Bot** versteht man ein Programm, das selbstständig Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein.

senhafte, unautorisierte Kopieren von Webinhalten bis hin zum systematischen Ausspionieren von Softwarelücken von Servern mit dem Ziel eingesetzt, in diese Server einzubrechen.

Spyware

Diese Art von heimtückischer Software wird vor allem beim Download eines vermeintlich kostenlosen Angebots auf Ihrem Computer installiert. Dort können die Surfgewohnheiten festgehalten werden oder die Eingabe von Passwörtern und Kontonummern ausspioniert werden. Auch Angaben über die benutzte Software, von heruntergeladenen Dateien oder die Konfiguration der Hardware sind für den Eindringling wertvolle Informationen.

Merkmale, die auf Spyware schließen lassen

Die folgende Liste enthält Anzeichen, die darauf hindeuten, dass sich auf Ihrem Computer möglicherweise Spyware befindet:

- Schwache Systemleistung, besonders während des Surfens im Internet.
- Der Computer reagiert häufiger nicht mehr.
- Der Computer braucht länger, bis der Windows-Desktop angezeigt wird.
- Der Browser schließt sich unerwartet oder reagiert nicht.
- Wenn Sie auf einer Suchseite eine Suche ausführen, werden Ergebnisse auf einer anderen Website angezeigt.
- Wenn Sie auf einen Link klicken, öffnet sich der Link nicht oder es wird eine vollkommen andere Website angezeigt.
- Die Startseite des Browsers ändert sich und kann nicht zurückgesetzt werden.
- Popup-Werbefenster werden angezeigt, obwohl der Browser nicht geöffnet ist, oder sie erscheinen auf Webseiten, die in der Regel keine Popup-Fenster enthalten.
- In Ihrem Browser werden zusätzliche Symbolleisten angezeigt.
- Ihren Favoriten werden automatisch Webseiten hinzugefügt.
- Ihrem Desktop werden automatisch Symbole hinzugefügt.

Vorbeugen vor Spyware und Hijacking-Software

Meistens wird Spyware und Hijacking-Software installiert, wenn Sie eine auf einer Webseite angezeigte Sicherheitswarnung per Mausklick „bestätigen“. Das Fenster mit der Sicherheitswarnung enthält ungefähr folgenden Text:

Möchten Sie <Name des kostenlosen Programms> installieren und ausführen. Angemeldet am <Datum und Uhrzeit> von <Name des Softwareherstellers oder des werbenden Unternehmens>.

Wenn Sie in dem Fenster mit der Sicherheitswarnung auf die Schaltfläche zum Bestätigen klicken, wird ein Skript oder Steuerelement im System integriert. Das Skript oder Steuerelement ändert das Verhalten Ihres Webbrowsers und passt es gemäß den Anforderungen des werbenden Unternehmens an.

Damit dies nicht passiert, klicken Sie in einem Fenster mit einer Sicherheitswarnung, das auf nicht vertrauenswürdigen Webseiten angezeigt wird, niemals auf die Schaltfläche zum Bestätigen. Schließen Sie diese Fenster, indem Sie auf **NEIN** oder gleichzeitig auf die Tasten Alt und F4 drücken.

Keylogger

Als Keylogger bezeichnet man Hard- oder Software zur Aufzeichnung von Tastatureingaben. Das Ziel dieser Methode ist, alle Aktivitäten am Computer zu kontrollieren. So kann auch ein unerlaubter Zugriff auf Daten nachvollzogen werden, welche E-Mails geschrieben wurden oder auf welche Internetseiten von diesem Computer zugegriffen wurde.

Der Nachteil aber ist, dass diese Aufzeichnungen auch unbemerkt an einen Angreifer übermittelt werden können und so eine immense Gefahr darstellen. Der Angreifer kann dann aus diesen Informationen für ihn wichtige Daten, wie zB Anmeldeinformationen oder Kreditkartennummern filtern.

Einen Schutz vor dem Zugriff eines Hardware-Keyloggers bietet die Verwendung einer virtuellen Tastatur (Bildschirmtastatur). Gegen Software-Keylogger hilft nur die Verwendung von Anti-Spyware-Programmen und Virenscanner.

Dialer

Mit so genannten Dialer-Programmen (Einwahlprogramme) kann eine Verbindung über das Telefonnetz hergestellt werden. Wird diese Methode jedoch dazu verwendet, auf eine kostenintensive Mehrwertnummer umgeleitet zu werden, so entstehen für den Geschädigten enorme Telefonrechnungen. Ein solches Programm muss in der Regel heruntergeladen, d.h. angeklickt und am Computer gespeichert und anschließend ausgeführt werden. Dialer gibt es oft auf Webseiten mit erotischem Inhalt oder auch auf Seiten, die andere Services (denkbar sind zB Seiten für Klingeltöne oder Logos, Hausaufgaben, Referate) anbieten.

Um sich zu schützen, kann man bei seiner Telefongesellschaft eine Sperrung aller 0939- Nummern (in Deutschland 0190 bzw. 0900-9) für den eigenen Anschluss beantragen.

Benutzer, die sich ausschließlich über DSL[10] mit dem Internet verbinden, sind nicht von Dialern betroffen. Dafür besteht die Gefahr, über das Mobilfunknetz mit einer Mehrwertnummer verbunden zu werden.

Beachten Sie Aufforderung, die Ihnen bei Besuch einer Website zur Eingabe einer Handynummer erscheint und meiden Sie die Aktivierung.

2.2 Schutz

Wenn man sich vorstellt, dass nur ein geringer Teil der bisher beschriebenen Gefahren auch in unseren Computern oder unseren Smartphones lauern können, so wird uns bewusst, wie wichtig Maßnahmen sind, diese Gefahren abzuwehren. Am besten ist es, diese Schadsoftware erst gar nicht in unsere Geräte eindringen lassen. Hier hilft Antiviren-Software.

[10] **Digital Subscriber Line.** Übertragungsstandards bei denen Daten mit hohen Übertragungsraten über einfache Kupferleitungen gesendet und empfangen werden können; im privaten Bereich meist ADSL.

Schutz vor dem Eindringen von Malware und vor deren Aktivierung am Computer bieten Antivirusprogramme. Diese durchforsten (scannen) Programmcodes, erkennen dabei Malware und beseitigen diese.

2.2.1 Funktionsweise von Antiviren-Software

Ein Virenscanner oder Antivirusprogramm ist eine spezielle Software, die bekannte Computerviren, Computerwürmer und Trojaner aufspüren, blockieren und auch löschen kann.

Um die schädliche Software zu erkennen, besitzt jeder Virenscanner eine Datenbank mit ihm bekannten Viren und anderer schädlicher Software. Gefundene Programmcodes werden mit den Einträgen der Datenbank verglichen. Wenn eine Datei oder ein Teil einer Datei mit einem Beispiel aus dieser Datenbank übereinstimmt, leitet der Virenscanner Neutralisierungsmaßnahmen ein, um die infizierte Datei zu beseitigen oder zu säubern.

Wie arbeiten Virenscanner?

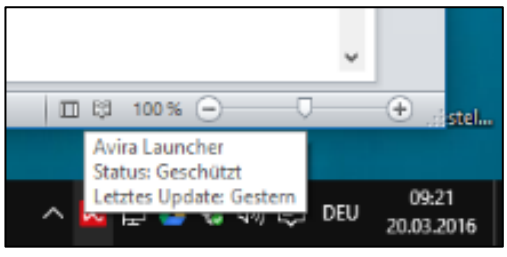
Die meisten Programme bieten 2 Methoden der Virensuche.

- **On Access** Ein Hintergrundüberwachungsprogramm (Guard) überprüft laufend alle Dateien, die vom System gelesen, geschrieben oder bearbeitet werden.
- **On Demand** Durch den User wird der Scan manuell gestartet. Danach werden Dateien, Ordnern oder Datenträgern gezielt durchsucht.

2.2.2 Antiviren-Software auf Computer installieren

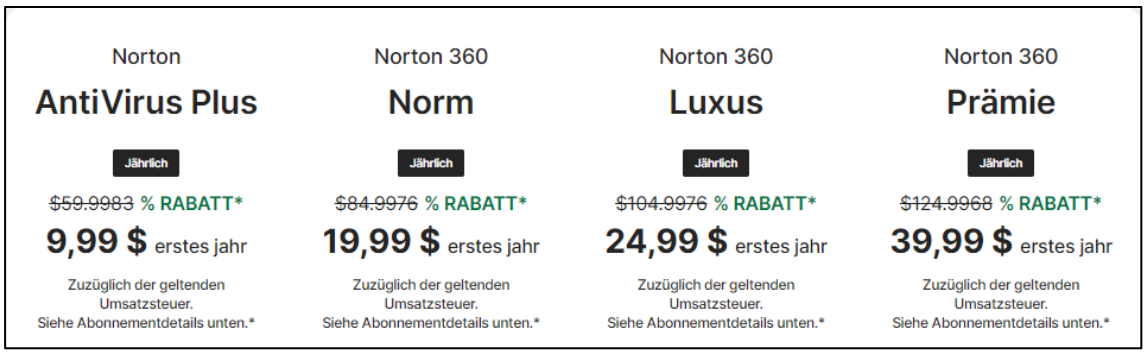
Programme zur Malwareabwehr sollen auf allen Geräten installiert sein, die Daten speichern oder transferieren. Der Markt für Virenscann-Software ist groß. So gibt es Programme, die kostenlos zur Verfügung gestellt werden (meist jedoch nur für den nicht gewerblichen also privaten Gebrauch) und Programme, deren Nutzung kostenpflichtig ist. Ein Vergleich über die Leistungsfähigkeit der angebotenen Software ist sinnvoll. In jedem Fall aber sollten Sie auf allen Ihren Geräten Antiviren-Software installieren.

Zudem ist es überaus wichtig, regelmäßig ein Update durchzuführen, da die Gefahr einer Malware-Infektion groß ist und täglich größer wird. Viele Antiviren-Software-Anbieter führen deshalb eine automatische Aktualisierung durch – aber noch besser ist es, dies selbst zu überprüfen.

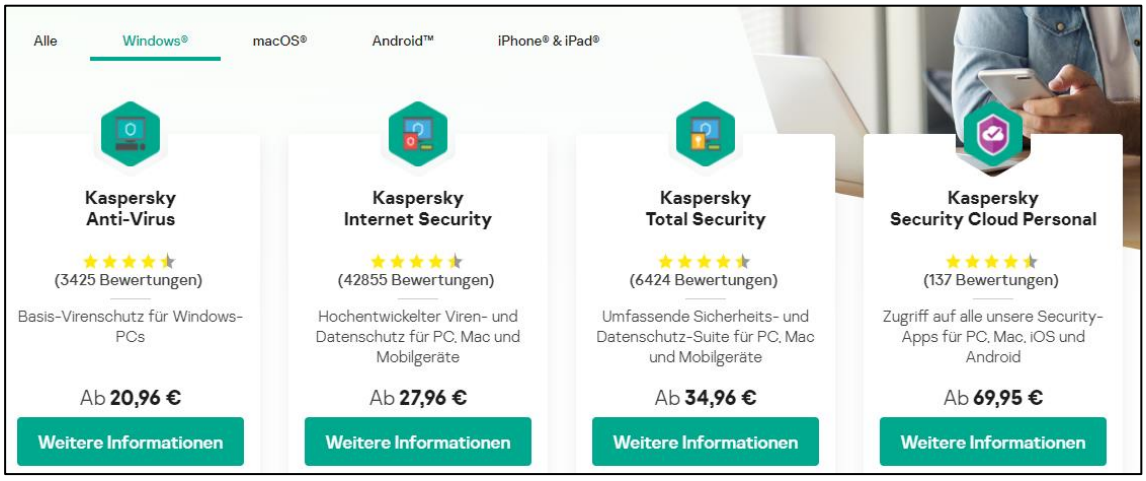


Manche Programme sind kostenfrei – Sicherheit kostet aber auch Geld

Beispiel aus der Website von TOTAL AV (März 2022)



Beispiel aus der Website von norton.com (März 2022)



Beispiel aus der Website von kaspersky.com (März 2022)

2.2.3 Regelmäßige Software-Updates

In Punkt 2.1.1 werden die typischen Schadprogramme aufgezeigt. Wie immer diese auf Ihren Computer oder Ihre mobilen Geräte gelangen, sie nisten sich in das Betriebssystem ein, wirken bei der Verwendung des Browsers oder über ein

Anwendungsprogramm oder über ein Plug-In[11]. Die meisten Softwarehersteller bieten daher für Ihre Produkte ständig Updates[12] an, die man auch wirklich installieren soll.

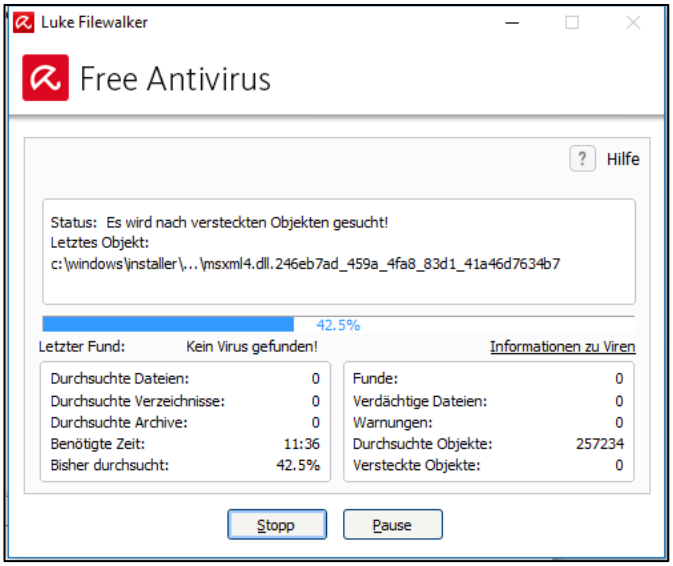
Vergewissern Sie sich, ob Ihre Browser (Microsoft Edge, Firefox, GoogleChrome, Safari etc.) auf dem letzten Stand sind.

Beachten Sie die Informationen von Java-Updates.

Ständig tauchen neue Viren, Würmer und Trojaner auf. Daher wird die Datenbank mit den Virussignaturen[13] auch ständig aktualisiert. Fast alle Anbieter von Antivirusprogrammen bieten automatische Aktualisierungen (Updates) an. Nutzen Sie dieses Angebot. Es liegt in Ihrem Interesse, dass Sie immer gegen die aktuell bekannten Viren gewappnet sind.

2.2.4 Laufwerke, Ordner und Dateien mit Antiviren-Software scannen

Auf jedem Computer sollte ein Antivirus-Programm installiert sein. Für den privaten Gebrauch werden auch verschiedene kostenlose Programme angeboten. Bei manchen Programmen kann eine zeitlich begrenzte Testinstallation vorgenommen werden.



Planen Sie, in welchen Zeitabständen ein kompletter Virusscan stattfinden soll. Das könnte zB bei jedem Neustart des Computers erfolgen. Natürlich dauert das eine Weile und daher kann es sinnvoll sein, einzelne Laufwerke oder externe Datenträger nur von Zeit zu Zeit komplett zu scannen. Ordner, in denen Programme abgelegt sind, sollten öfters überprüft werden. In jedem Fall sollten bei einem Download von Dateien oder beim Abrufen Ihrer E-Mails diese Dateien immer einem Virusscan unterzogen werden.

In einem Netzwerk sind die Server meist so konfiguriert, dass On-Demand-Virenscans außerhalb der Geschäftszeiten durchgeführt werden. Damit können zeitraubende Unterbrechungen ausgeschlossen werden.

---

[11] **Plug-In** (auch Plugin) Bezeichnung für ein Zusatzmodul, das die Leistung eines Programms erweitert.

[12] **Update** = Aktualisierung von Software; kostenlos; behebt erkannte Fehler oder Sicherheitslücken.

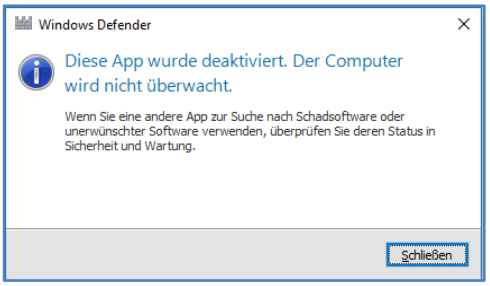
[13] **Virussignatur**: Erkennungsmuster eines Virus, das zur Identifikation verwendet wird.

2.2.5 Risiko bei veralteter und nicht mehr unterstützter Software

Stellen Sie sich vor, Sie hätten im Oktober 2012 einen Laptop mit einem vorinstallierten Betriebssystem *Windows 8*, mit einem *Internet-Explorer* und einer *Testversion* des Antivirusprogramms Norton Security gekauft und in Betrieb genommen. Wenn Sie in der Zwischenzeit weder die Updates von Windows abgerufen hätten noch die Norton-Software über den Testzeitraum hinaus verlängert hätten, wo wäre da noch Sicherheit? Software-Produkte altern im Laufe der schnelllebigen Computerentwicklung und werden nicht mehr durch Updates unterstützt – wie dies zB beim Browser Internet Explorer oder Windows 8 der Fall ist. Das Antivirusprogramm von damals ist ebenfalls längst überaltert und für eine Aktualisierung nicht mehr geeignet. Abgesehen davon war während all der Jahre Ihr Computer allen Malware-Angriffen ausgesetzt. Und wer weiß: vielleicht haben böse Eindringlinge sich bereits Ihrer persönlichen Daten bedient.

Beachten Sie beim Kauf einer neuen Software, dass diese mit Ihrem Betriebssystem und anderen bereits installieren Produkten kompatibel, d.h. gemeinsam funktionstüchtig, ist, und Hard- und Software technisch harmonieren und miteinander betrieben werden können. Besteht Inkompatibilität, so passen diese nicht zusammen und können nicht kombiniert werden.

Wenn Sie versuchen, mehrere Antivirenprogramme auf einem Computer zu installieren, kann es dabei zu Störaktionen kommen. Manchmal passiert es in solch einem Fall, dass ein Antivirusprogramm das andere – aufgrund der darin enthaltenen Virensignatur-Datenbank – für einen Virus hält.



Windows Defender von Microsoft ist im Windows-Betriebssystem integriert. Es hat allerdings die Eigenschaft, sich selbst zu deaktivieren, wenn ein anderes Antivirusprogramm installiert ist.

2.3 Problemlösung und -behebung

2.3.1 Quarantäne und die Auswirkung auf infizierte oder verdächtige Dateien

Wenn ein Virenscanner schädliche Dateien findet, gibt er in den meisten Fällen eine Warnung an den User weiter, mit der Frage, was jetzt geschehen soll. Die Möglichkeiten reichen von Auslagern der befallenen Datei in einen Quarantäne-Bereich über einen Reparaturversuch bis zum endgültigen Löschen der infizierten Datei.

Quarantäne ist ein Ordner, der im Antivirus-Programmordner angelegt wird. In diesem werden verdächtigte Dateien verschoben und können, solange das Antivirusprogramm aktiv ist, keinen Schaden anrichten.

2.3.2 Umgang mit infizierten oder verdächtigen Dateien

Wann Quarantäne – Wann Löschen

Wo liegt nun der Unterschied zwischen Quarantäne und Löschen? Die Option mit Quarantäne ist bei falschen Virus-Meldungen sinnvoll.

In Quarantäne gehören Dateien, bei denen nicht genau bekannt ist, ob diese wirklich „infiziert" sind und ob man diese Datei für den Betrieb des Computers nicht doch braucht. So wäre es zB fatal, wenn das Antivirus-Programm ein kritisches Programm wie Explorer.exe falsch markiert und daraufhin die Datei sofort gelöscht werden würde. In diesem Fall ist das Verschieben der markierten Datei in die Quarantäne die bessere Entscheidung. Dort ist die gefundene Datei vom Rest des Computers abgeschottet und kann keinen Schaden anrichten. Ist danach die Funktionalität des Computers nicht mehr gegeben, so kann die Datei wieder aus der Quarantäne zurückgeholt werden. Treten jedoch keinerlei Probleme auf, kann die Datei aus der Quarantäne unwiderruflich gelöscht werden.

Beispiel: Dateipfad vom Quarantäne-Ordner – QB, den Kaspersky

2.3.3 Malware-Angriff mithilfe von Online-Ressourcen identifizieren

Wie bereits in Punkt 2.2.3 aufgezeigt wird, sollten durch laufende Aktualisierung der Betriebssystem- und Anwendersoftware drohende Gefahren hintangehalten werden. Die Programmanbieter veröffentlichen immer wieder Updates, die entdeckte Sicherheitslücken schließen. Oft werden diese Neuerungen automatisch auf Ihren Computer eingespielt oder zumindest in Form einer Informationsmeldung bekannt gegeben. Trotzdem sollte man von Zeit zu Zeit die Webseiten der Anbieter bereits installierter Programme durchforsten, um gegebenenfalls bestehende Warnungen dieser Anbieter nicht zu versäumen.

Beobachten Sie daher die Webseiten

- Ihres Betriebssystem- oder ToolAnbieters *(Microsoft, Apple, Linux, Java, …)*
- der Anwenderprogramme (MSOffice, OpenOffice, Joomla,…)
- des Browsers (Microsoft Edge, Firefox, Opera, Chrome, …)
- Ihrer Antivirus-Software (McAfee, AVG, Avira, Kaspersky, Norton, G Data, …)
- von E-Payment, E-Commerce und E-Government (Banken, mPAY24, Paypal, Amazon, Ebay, finanzonline, ELDA, …)