



2 MALWARE (SCHADSOFTWARE)

2.1 Arten und Funktionsweisen

Als Malware bezeichnet man Computerprogramme, die unerwünschte, meist auch schädliche Aktionen ausführen. Die Gefahr immer neu entwickelte Computerschädlinge nicht zu erkennen, erfordert es, sich laufend mit veröffentlichten Warnungen zu beschäftigen. Aktualisieren Sie Ihr Antivirenprogramm, lesen Sie die Warnungen Ihrer Geschäftspartner (Banken, Behörden, Lieferanten...) Vor allem aber: seien Sie misstrauisch gegenüber allzu freundlichen Kontaktangeboten.

2.1.1 Den Begriff Malware verstehen; verschiedene Arten von Malware kennen: Adware, Fileless Malware, Virus, Wurm, Trojaner, Bots, Ransomware, Spyware, Keylogging, Cryptojacking

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 **malicious** (böartig) und **Software** etabliert.

Bezeichnung	Wirkung
Adware	Sammelbezeichnung für Programme, die in Computersysteme eindringen und unerwünschte Werbung einblenden. Sie produziert aufdringliche Popups, Banner und Browser-Werbung, stört beim Surfen und verlangsamt den Browser.
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.
Fileless Malware	Dateilose Schadsoftware: Hier handelt es sich um eine Art von Cyberangriff, bei der Schadcode direkt im Arbeitsspeicher (RAM) ausgeführt wird. Dadurch sind keine Dateien auf der Festplatte auffindbar. Sie nutzt vertrauenswürdige, bereits vorhandene Systemwerkzeuge wie PowerShell oder WMI, um Angriffe durchzuführen. Da keine verdächtigen Dateien auf dem Datenträger abgelegt werden, ist diese Form der Malware oft unsichtbar für klassische Antivirenprogramme.
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.



Bezeichnung	Wirkung
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 <i>Hacker</i> 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 ...
Bots	Bots können nützlich bei automatischen Routineaufgaben, im Kundenservice oder beim Sammeln von Informationen sein. Zudem werden sie aber auch zum Verbreiten von Desinformationen und Diebstahl von Zugangsdaten eingesetzt, erzeugen Fake-Accounts und führen Cyberangriffe aus.
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 weitergegeben. 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 Virens Scanner 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.



Bezeichnung	Wirkung
Ransomware	Bei einem Ransomware-Angriff werden die Daten auf einem IT -System verschlüsselt und eine Entschlüsselung erst gegen Zahlung eines Lösegeldes (engl. Ransom) in Aussicht gestellt. Immer öfter wird zusätzlich mit der Veröffentlichung der zuvor entwendeten Daten gedroht, um das Opfer zusätzlich unter Druck zu setzen.
Keylogging	Keylogger sind Programme, die als Hintergrundprozess auf einem Computer oder anderen Gerät laufen und die Tastatureingaben des Nutzers aufzeichnen.
Cryptojacking	Beim Cryptojacking (auch bössartiges Cryptomining genannt) greifen Cyberkriminelle, sogenannte Cryptojacker, unerlaubt auf Computer oder Mobilgeräte zu und nutzen deren gekaperte Rechenleistung, um illegal Kryptowährung zu schürfen. Diese Form der Cyberkriminalität zielt im Gegensatz zu Malware auf die Nutzung der Rechenleistung des Endgerätes ab.

2.1.2 Wissen, wie sich KI (Künstliche Intelligenz) Malware von traditioneller Malware durch Fähigkeiten wie Anpassung, Lernen und Umgehung unterscheidet

Malware ist schädliche Software. Sie soll Computer, Smartphones oder Netzwerke angreifen und Daten stehlen, löschen oder Geräte beschädigen.

Traditionelle Malware arbeitet nach festen Regeln. Sie macht immer das Gleiche. Ein Virenschutz kann sie daher leichter erkennen, weil ihr Verhalten bekannt ist.

KI-Malware (Malware mit Künstlicher Intelligenz) ist moderner und gefährlicher. Sie kann sich an neue Situationen anpassen und aus Erfahrungen lernen.

KI-Malware hat mehrere besondere Fähigkeiten

- **Anpassung:** Sie kann ihr Verhalten ändern, wenn sie merkt, dass ein Computer gut geschützt ist.
- **Lernen:** Sie kann aus früheren Angriffen Informationen sammeln und zukünftige Angriffe verbessern.
- **Evasion** (Ausweichen): Sie versucht, Virenschutzprogramme und andere Sicherheitsmaßnahmen zu umgehen. Zum Beispiel kann sie ihren Programmcode verändern oder sich unauffällig verhalten, damit sie nicht entdeckt wird.

Deshalb sind regelmäßige Software-Updates, ein aktueller Virenschutz und vorsichtiges Verhalten im Internet besonders wichtig. Auch das Misstrauen gegenüber unbekannten E-Mails, Links und Dateianhängen hilft dabei, Angriffe durch traditionelle Malware und KI-Malware zu verhindern.

2.1.3 Arten von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm

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.

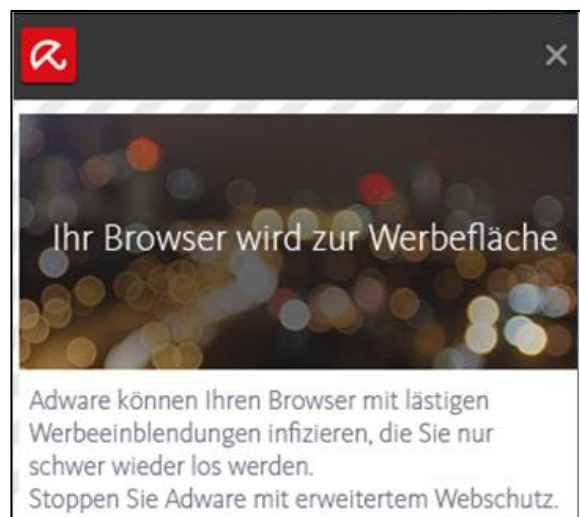
Ein Wurm ist ein Programm, das sich selbst kopiert und verbreitet, ohne sich an ein Wirtsprogramm anzuhängen. Ein Wurm wandert über Netzwerkverbindungen von einem Computer oder mobilen Gerät zum nächsten. Die „Absicht“ der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen.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

2.1.4 Arten von Malware und ihre Funktionsweise für Datendiebstahl, Betrug oder Erpressung kennen, wie: Adware, Ransomware, Spyware, Bots, Keylogger

Adware

Adware ist eine werbeunterstützende Software, mit der Werbefbanner automatisch eingeblendet, abgespielt werden oder auch Downloads gestartet werden. Adware-Programme werden oft in Freeware⁴ oder Shareware⁵-Programme eingebaut, wo sie sich dann indirekt über die Nutzung des Werbefbanners 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 nennt man Schadsoftware, die einen Computer bereits beim Startvorgang unterbricht. Sie verhindert den Zugriff auf Ihren Rechner bzw. Netzwerk oder

⁴ **Freeware**; Programme, die zur kostenlosen Nutzung bereit gestellt werden.

⁵ **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.



verschlüsselt Dateien. Oft wird auf dem Sperrbildschirm vorgegeben, von der Polizei oder einer vergleichbaren Behörde zu sein.

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.

Ransomware-Angriffe können kostspielige Unterbrechungen des Betriebs und den Verlust kritischer Informationen und Daten verursachen. Es sollten solche Zugriffe den Behörden angezeigt werden.

Botnet

Ein Botnet oder Botnetz ist eine Gruppe von Bots⁶. 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 „böartige“ Bots. Letztere werden beispielsweise zum Sammeln von E-Mail-Adressen für Werbezwecke, für das massenhafte, 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.

⁶ Unter einem **Bot** versteht man ein Programm, das selbstständig Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein.



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 Surfs 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 Virens Scanner.

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.

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 Verstehen, dass Antiviren-Software und Anti-Malware-Software auf Computern und mobilen Geräten installiert sein soll; ihre Funktionsweise und Grenzen verstehen

Ein Virens Scanner 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 Virens Scanner 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 Virens Scanner Neutralisierungsmaßnahmen ein, um die infizierte Datei zu beseitigen oder zu säubern.

Wie arbeiten Virens Scanner?

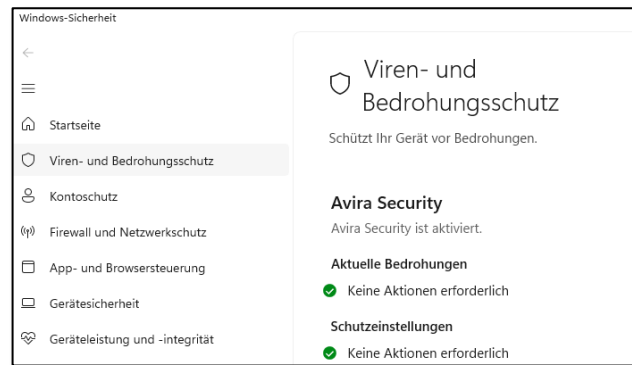
Die meisten Programme bieten 2 Methoden der Virensuche.

- **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.

Programme zur Malwareabwehr sollen auf allen Geräten installiert sein, die Daten speichern oder transferieren. Der Markt für Virens Scanner-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 durchaus 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.



Welche Leistungen bieten Antivirusprogramme neben Virenschutz noch?

VPN (siehe dazu Punkt 3.1.1 ab Seite 53) schützt vor Auskundschaftung und Nachverfolgung Ihrer Internet-Surf-Gewohnheiten.

Norton VPN. Ihre Komplettlösung für Online-Sicherheit.

- Genießen Sie eine schnellere, zuverlässigere und sicherere VPN-Software.
- Mehr Anonymität und Sicherheit beim Surfen.
- Leistungsstarker Virenschutz.
- Erstellen, Speichern und müheloses Anwenden starker Passwörter.

Beispiel aus der Website von norton.com

In Firmen sind oft unterschiedliche Arbeitsgruppen und Aufgabenbereiche abzusichern. Viele Anbieter stellen dafür speziell zusammengestellte Programmpakete zur Verfügung.

kaspersky

Privatanwender Unternehmen Partner Über uns

EUR Q Mein Konto

Produkte Services Branchen Lösungen

Kleine und mittelständische Unternehmen

Kaspersky Small Office Security **BESTSELLER**

Kaspersky Next EDR Foundations

Alle Produkte für kleine Unternehmen

Kaspersky Next EDR Optimum

Endpoint

Kaspersky Next EDR Foundations **Neu**

Kaspersky Next EDR Optimum **Neu**

Kaspersky Next EDR Expert

Kaspersky Private Security Network

Kaspersky Embedded Systems Security

SIEM & XDR

Kaspersky Next XDR Expert **Neu**

Network

Kaspersky Anti Targeted Attack

Kaspersky Security for Mail Server

Kaspersky Security for Internet Gateway

Cloud-Umgebung

Kaspersky Hybrid Cloud Security

Kaspersky Container Security

Threat Intelligence

- KSOS Portal
- Testversionen und Downloads
- KMU-Lizenz verlängern
- Partner finden
- Geschäftskonto
- Kaspersky TIP

Beispiel aus der Website von kaspersky.com



2.2.2 Die Bedeutung von regelmäßigen Software-Updates für Antiviren-Software, Anti-Malware-Software, Web-Browser, Plug-ins, Anwendungsprogramme, Betriebssysteme verstehen

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-In⁷. Die meisten Softwarehersteller bieten daher für Ihre Produkte ständig Updates⁸ an, die man auch wirklich installieren soll.

Vergewissern Sie sich, ob Ihr Browser (MS Edge, Firefox, Google Chrome, Safari etc.) auf dem letzten Stand ist.

Beachten Sie die Informationen von Java⁹-Updates.

Ständig tauchen neue Viren, Würmer und Trojaner auf. Daher wird die Datenbank mit den Virussignaturen¹⁰ 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.



2.2.3 Laufwerke, Ordner und Dateien mit Antiviren-Software und Anti-Malware-Software scannen; Zeitplan für Scans mit Antiviren-Software festlegen

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.

Anti-Malware-Software schützt Ihre Geräte vor Viren, Trojanern, Ransomware und Spyware. Während klassische Antivirenprogramme primär bekannte Bedrohungen abwehren, sind spezialisierte Anti-Malware-Tools darauf ausgelegt, tiefsitzende, neuartige und unerwünschte Programme (Adware) aufzuspüren.

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

⁷ **Plug-In** (auch Plugin) Bezeichnung für ein Zusatzmodul, das die Leistung eines Programms erweitert.

⁸ **Update** = Aktualisierung von Software; kostenlos; behebt erkannte Fehler oder Sicherheitslücken.

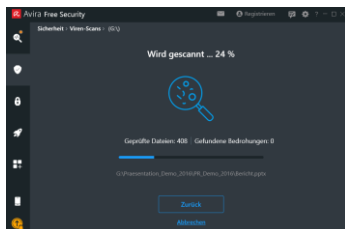
⁹ **Java** = Programmiersprache und Computing-Plattform. Sie stellt mittlerweile eine Basis für den Großteil der digitalen Welt von heute bereit und dient als zuverlässige Plattform für viele Services und Anwendungen. Auch neue, innovative und zukunftsgerichtete Produkte und digitale Services basieren nach wie vor auf Java.

¹⁰ **Virussignatur**: Erkennungsmuster eines Virus, das zur Identifikation verwendet wird.



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.



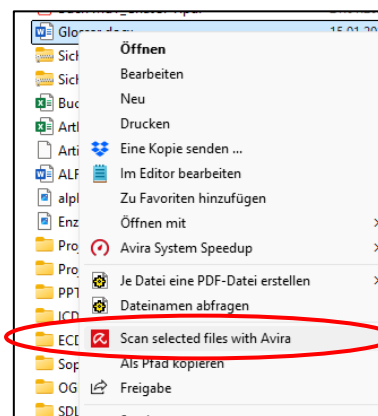
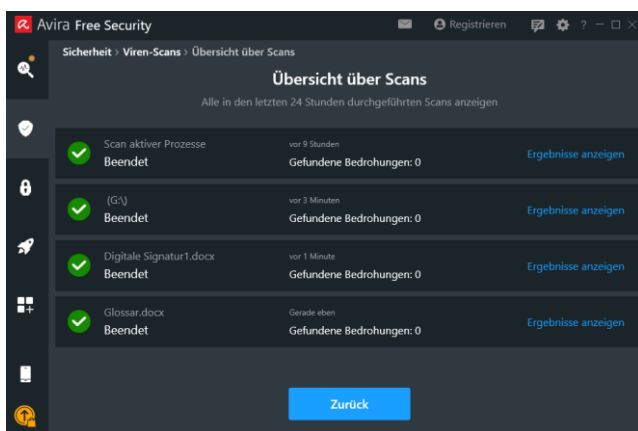
Meist meldet sich Ihr Virenschutzprogramm automatisch, sobald Sie zB einen USB-Stick an Ihren Computer anschließen, und beginnt mit dem Scan des Datenträgers.

Nach Beendigung des Scans erhalten Sie eine Übersicht der geprüften Dateien und ev. gefundener Bedrohungen.



Einzelne Dateien überprüfen Sie bequem im *Explorer*, indem Sie für die Datei das Kontextmenü aufrufen und über **WEITER OPTIONEN ANZEIGEN** den Befehl zum Scan aufrufen.

Auch hier erhalten Sie eine Übersicht der gescannten Daten.



Außerdem bekommen Sie jederzeit einen Überblick über aktuelle Bedrohungen in den Windowseinstellungen: **DATENSCHUTZ UND SICHERHEIT/ WINDOWS-SICHERHEIT /VIREN- UND BEDROHUNGSSCHUTZ.**

Hier stehen Ihnen weitere Scanoptionen zur Verfügung.

☒ Schnellüberprüfung
Überprüft Ordner im System, in dem häufig Bedrohungen gefunden werden.

☐ Vollständige Überprüfung
Alle Dateien und ausgeführten Programme auf der Festplatte werden überprüft. Diese Überprüfung kann mehrere Stunden dauern.

☐ Benutzerdefinierte Überprüfung
Wählen Sie aus, welche Dateien und Speicherorte überprüft werden sollen.

☐ Microsoft Defender Antivirus (Offlineüberprüfung)
Bestimmte Schadsoftware lässt sich u. U. besonders schwierig vom PC entfernen. Microsoft Defender Antivirus (Offline-Überprüfung) kann helfen, derartige Software mithilfe neuester Bedrohungsdefinitionen zu finden und zu entfernen. Durch den Vorgang, der etwa 15 Minuten dauert, wird der PC neu gestartet.

Jetzt überprüfen