Sicherheit am PC

Dipl. Ing. (FH) Stephan Mante

Sicherheit am PC

Agenda

1. Schadsoftware
2. Infektionswege
3. Wie kann ich infiziert werden?
4. Anzeichen einer Infektion
5. Windows im Fokus der Angreifer
6. Wie kann ich mich schützen?
7. Datensicherung

Sicherheit am PC

Malware – engl. Sammelbegriff für Schadsoftware

Viren
Nistet sich ein

Spyware
Späht deinen Daten aus

Trojaner
Bleibt unerkannt

Scareware
verunsichert

Würmer
Vermehren sich übers Internet

Adware
Unerwünschte Werbung

Ransomware
Erpresst Lösegeld

Viren

Schadsoftware, die sich an vorhandene Programme anhängt oder neue Programme erzeugt. Viren nisten sich so in das Sytem ein, dass sie unter bestimmten Bedingungen ausgeführt werden (meist beim Start des Systems) ohne dass der Benutzer Kenntnis davon hat.

Viren richten Schaden unterschiedlichster Art mit unterschiedlichsten Erscheinungsformen im System an.

Spyware

Spyware (Ausspähsoftware) sammelt Informationen über den Nutzer und seine Gewohnheiten bei der Nutzung des Computers oder beim Surfen im Internet.
Die gesammelten Informationen werden über das Internet an den Urheber der Spyware übermittelt.

Sie ist Bestandteil eines Programms, was der Nutzer selbst installiert hat, oder was durch einen Einbruch in das System installiert worden ist.

Spyware ist illegal, wenn sie ohne Wissen des Nutzers auf das System gekommen ist.

Würmer (Worm)

Würmer sind Schadsoftware, die sich selbst über das Internet vervielfältigt. Dies geschieht meist durch das versenden von infizierten E-Mails über das Internet an alle E-Mail-Adressen, die sich im Adressbuch befinden.

Dazu installieren die Würmer oft einen eigenen Mailserver, der die Mails verschickt.

Deutliches Anzeichen ist, wenn man vom Internetprovider einen Brief bekommt, dass das System verseucht sei und mit einem Antivirenprogramm zu prüfen wäre.
Bis zur Behebung bleibt das E-Mailsystem dann gesperrt.

Trojaner

Als Trojanisches Pferd (engl. Trojan Horse, kurz Trojaner), bezeichnet man ein Computerprogramm, das gezielt auf fremde Computer eingeschleust wird oder zufällig dorthin gelangt und nicht genannte Funktionen ausführt.

Es ist als nützliches Programm getarnt, indem es bspw. Den Dateinamen eines bekannten Programms aufweist Und neben der versteckten Funktion tatsächlich eine nützliche Funktionalität aufweist, wie z.B. „lustiger_Bildschirmschoner.exe“.

Adware

Adware ist ein Schachtelwort aus **Ad**vertising und Soft**ware** und bezeichnet Software, die dem Benutzer zusätzlich zur eigentlichen Funktion Werbung zeigt bzw. weitere Software installiert, welche Werbung anzeigt.
Adware ist üblicherweise kostenlos und funktionell uneingeschränkt. Oft ist sie auch in kostenlose Software („Freeware“) oder Hilfsprogramme eingebettet und daher schwer zu erkennen. Durch Vermarktung der Werbeflächen werden die Entwicklungskosten gedeckt oder auch Gewinn erzielt. Oft gibt es auch eine Option, gegen Bezahlung eine werbefreie Vollversion zu erhalten.

Beispiel: Opera

Ransomware

Ransomware auch Erpressungstrojaner, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffsder Daten sowie des gesamten Computersystems erwirkt.
Dabei werden private Daten auf einem fremden Computer verschlüsselt, oder der Zugriff auf sie wird verhindert, um für die Entschlüsselung oder Freigabe ein „Lösegeld“ zu fordern. Ihre Bezeichnung setzt sich zusammen aus ransom, dem englischen Wort für Lösegeld, und ware zusammen.

Bekanntester Vertreter ist **Locky** mit 5000 Infezierungen pro Tag in Deutschland

Sicherheit am PC

Infektionswege

Direkter Angriff

- Der Rechner wird direkt aus dem Internet oder lokalem Netzwerk angegriffen
- Oft werden Schwachstellen eines Dienstes ausgenutzt

Indirekter Angriff

- Unbeabsichtigtes Herunterladen von Schadsoftware über den Internet Browser (drive-by-download)
- Zusendung von Schadsoftware per E-Mail
- Abgreifen von Passwörtern, sog. Phishing-Angriffe
- Über ein USB-Stick wird auto. Schadsoftware auf dem Rechner installiert
- Zugangsdaten werden über einen fingierten Telefonanruf erbeutet (Social Hacking)

Sicherheit am PC

Wie kann ich infiziert werden?

- Beim Besuch von Internetseiten mit verseuchtem Inhalt
- Beim Installieren von Software aus unklarer Herkunft
- Beim Öffnen von verseucher E-Mail; hier reichen schon eine html-E.Mails ohne Anhang aus
- Durch direkten Angriff aus dem Internet
- Durch Einbinden verseuchter externer Speichermedien (USB-Stick, Festplatte)
- Wenn ich der Aufforderung zum Download und Installation Folge leiste

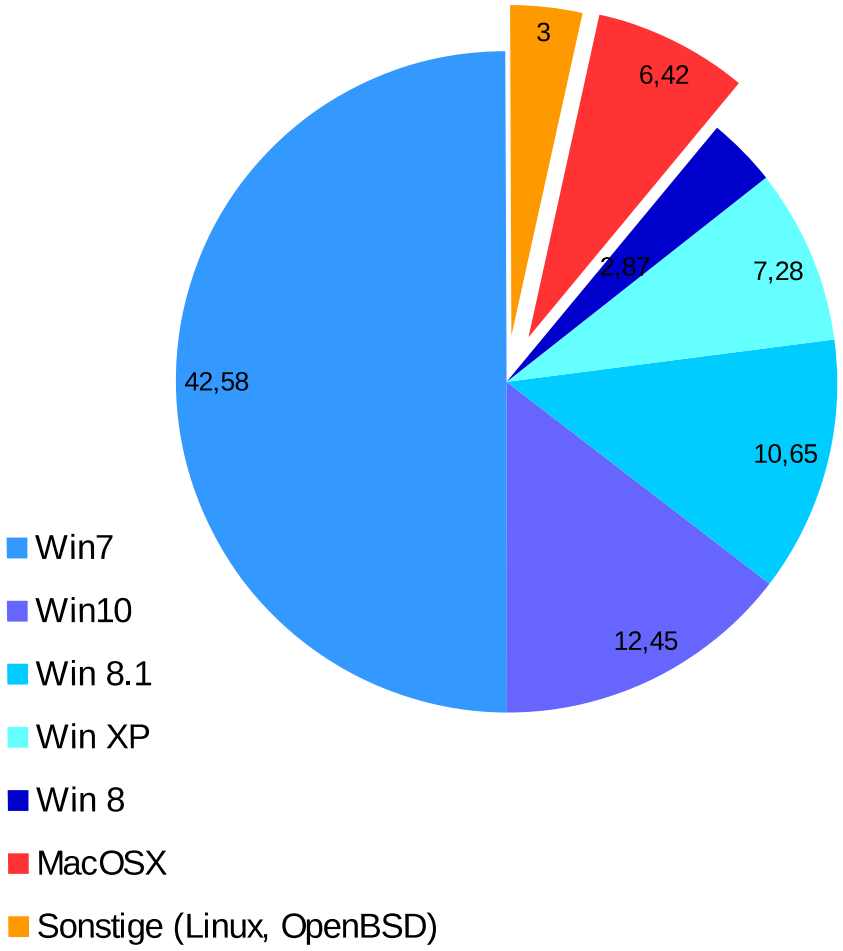
Sicherheit am PC

Anzeichen einer Infektion

- Rechner wird langsam
- Das Starten bzw. Runterfahren dauert sehr lange
- Der Internetbrowser zeigt nach dem Start eine unbekannte Internetseite
- Es werden im Internetbrowser falsche Internetseiten aufgerufen
- Der Rechner belegt die Internetbandbreite übermäßig
- Es werden Pop-Up Fenster unkontrolliert angezeigt
- Es tauchen neue Leisten im Internetbrowser auf
- Verschlüsselte Internetseiten (http**s**://) lassen sich nicht mehr öffnen
- ….

Sicherheit am PC

Verteilung der Betriebssysteme



Bedeutung

Je größer die Verbreitung einer Betriebssystem-Plattform ist, um so größer ist auch die Gefahr einer Infektion.

Die Programmierer einer Schadsoftware sind daran interessiert, mit möglichst geringem Aufwand eine möglichst große Wirkung zu erzielen.

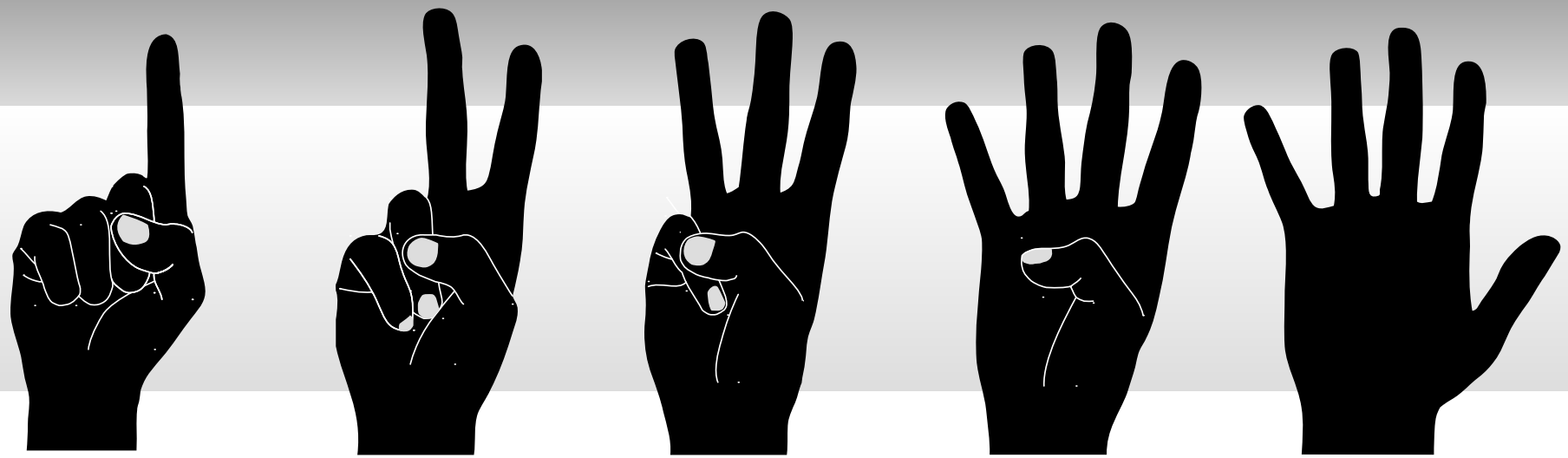
Schadsoftware ist meist nur auf einer Plattform lauffähig und kann deshalb auf einer anderen keinen Schaden anrichten.

Quelle: http://de.statista.com

Wie kann ich meinen Rechner schützen?

Die 5 wichtigsten Sicherheitsregeln

Up-to-date	Anti-Viren-Software	Awareness	Backup	Adblocker
Spielen Sie zeitnah Anti-Viren- und Programm- bzw. Betriebssystems-Updates ein.	Verwenden Sie unbedingt eine Anti-Viren-Software, auch auf einem Mac!	Seien Sie kritisch beim Öffnen von unbekannten E-Mails. Klicken Sie nicht auf integrierte Links, bzw. öffnen Sie niemals deren Anhänge.	Machen Sie regelmäßig Backups von ihren wichtigen Daten und bewahren Sie diese getrennt vom Rechner auf.	Verwenden Sie im Internetbrowser einen Adblocker um sich vor gefährlicher Werbung zu schützen.

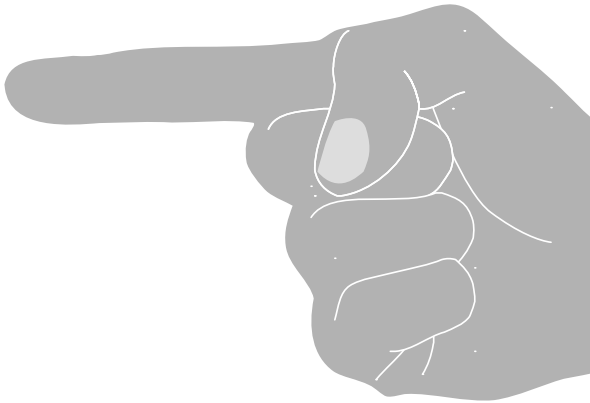


Datensicherheit und Sicherheit

Awareness (dt. Bewusstheit)

Benutzerverhalten

- Fremdsprachliche E-Mail und E-Mail von unbekannten Absendern löschen, ggf. beim Absender nachfragen.
- Seien Sie kritisch gegenüber Rechnungen und anderen Dokumenten, mit denen Sie nicht rechnen.
- Updates immer auf der Webseite des Herstellers durchführen. (filehippo.com, ninite.com)
- Nur die Software installieren, die man unbedingt benötigt
- Im Windows-Explorer Deaktivierung des Punktes „Erweiterungen bei bekannten Dateitypen ausblenden“
  z.B. würde die Datei “Bild.jpg.exe” sonst -> Bild.jpg
- Nicht unter administrativen Rechten arbeiten (Kontotyp = Standard)



Backup

Motivation

Nach einem Festplattendefekt oder Virenbefall ist es vorteilhaft eine Datensicherung durchgeführt zu haben. Sollten Sie eine Datei versehentlich gelöscht haben, stellen Sie diese selektiv aus der letzten Datensicherung wieder her. Nach einem Totalausfall des Rechners stellen Sie alle Daten auf einem neuen Computer aus dem Windows-Backup wieder her.

Um eine optimale Datensicherheit zu gewährleisten, sollten Sie das richtige Backup-Medium auswählen. Ich empfehle, die Sicherungs-datenträger an einem sicheren Ort aufzubewahren.

Sicherheit am PC

Datensicherungsarten:

„Normale Datensicherung“

- Dateibezogenes Backup auf einem externen Datenträger
- Nur die eigenen (persönlichen) Dateien (Dokumente, Bilder usw.)

Systemabbild

- Der gesamte Festplatteninhalt wird als Image auf DVD oder externem Datenträger gespeichert
- Die Rücksicherung einzelner Dateien ist nicht möglich

Schattenkopie

- Über einen Wiederherstellungspunkt können Systemdateien wieder hergestellt werden.
- Wird max. 90 Tage vorgehalten
- ShadowExplorer einsetzen (http://www.shadowexplorer.com)

Backup

Datensicherung mit Windows-Bordmitteln:

Windows 7
http://www.netzwelt.de/news/131181_2-anleitung-backup-windows-7-bordmitteln.html

Windows 8
http://praxistipps.chip.de/windows-8-backup-mit-bordmitteln_24065

Windows 10
http://praxistipps.chip.de/windows-10-backup-erstellen-so-gehts-richtig_39656