Linux hilft Windows - Virenbekämpfung mit Freier Software

Edgar 'Fast Edi' Hoffmann

Community FreieSoftwareOG

kontakt@freiesoftwareog.org

2. Juli 2015

Linux vs. Windows Sicherheitskonzepte

Computerviren, Würmer, Trojaner, Botnetze etc. richten Schaden an - sowohl auf dem eigenen Computer als auch in Unternehmen, durch den Ausfall von Diensten, Servern oder Datenverlust.

Fast alle Schadprogramme (engl. Malware) richten sich dabei gegen Windows bzw. Windowssysteme.
Dies liegt zum einen daran, dass Windows noch immer das - mit Abstand - verbreitetste Betriebssystem für Desktop-Rechner / Endanwender ist.

Linux vs. Windows Sicherheitskonzepte

Ein zweiter, genau so wichtiger Punkt ist die natürliche Diskrepanz zwischen Sicherheit und Komfort - beides zusammen geht nicht oder endet oft in einem (faulen) Kompromiss.

Zwar kündigt Microsoft immer wieder an, die Computerwelt sicherer zu machen, allerdings ist es nach wie vor so, dass es dringend angeraten ist, einen Windows-PC mit einer (inzwischen integrierten) Firewall und einem Viren-/Spywarescanner auszustatten, vor allem dann, wenn man regelmäßig im Internet surft.

Firewalls und insbesondere Virenscanner sind heute ein eigener, umfangreicher Bereich bei kommerzieller Software.

Linux vs. Windows
Sicherheitskonzepte

Es geht aber auch ohne solche Programme, wenn man ein geeignetes Betriebssystem nutzt, das vergleichsweise weit weniger anfällig gegen Malware ist:

GNU/Linux

≫*Es gibt keinen vernünftigen Grund, warum Computer zunächst unsicher konzipiert und dann vom Benutzer abgedichtet werden müssen.*≪

Linux vs. Windows
Ist Linux vollkommen sicher?

≫*Nein. Es ist weit davon entfernt, wenn auch nicht so weit wie andere...*≪

Es gibt immer mal wieder Sicherheitslücken in Linux, manche davon schwerwiegend.

Sie werden allerdings üblicherweise innerhalb kürzester Zeit nach Bekanntwerden behoben

Außerdem sind die möglichen praktischen Auswirkungen von Sicherheitslücken aufgrund des konsequent eingehaltenen Sicherheitskonzeptes vergleichsweise gering, insbesondere auf Desktop-Rechnern.

Allerdings sollte ein Benutzer die angebotenen Online-Updates auch ernst nehmen.

Linux vs. Windows
Ist Linux vollkommen sicher?

Im Server-Bereich sind auch Linux-Server immer wieder Ziel von Hacker-Attacken.

Der Angriff erfolgt hier im Regelfall aber nicht auf Linux bzw. den Kernel, sondern auf die darauf laufende Programme, die Dienste (in welcher Form auch immer) im Internet bereit stellen.

Populär sind dabei Attacken wie Cross Site Scripting, SQL Injection oder die Ausnutzung von Lücken in unsauber programmierten PHP-Anwendungen.

Schadprogramme
Begriffserklärung

- Schadfunktionen sind gewöhnlich getarnt oder die Software läuft gänzlich unbemerkt im Hintergrund
  - Manipulation oder das Löschen von Dateien
  - technische Kompromittierung von Sicherheitssoftware bzw. Sicherheitseinrichtungen (Firewalls oder Antivirenprogramme)
  - ungefragtes Sammeln von Daten zu Marketing-Zwecken
  - ordnungsgemäße Deinstallation mit generell gebräuchlichen Mitteln schlägt fehl

Schadprogramme
Begriffserklärung

Mittlerweile kursieren sehr viele Schadprogramme, auch Malware genannt (meist für Windows), die man gemeinhin grob unterteilt in

- Viren
- Trojaner
- Würmer
- Spyware/Adware (Grayware)
- Scareware/Rogueware
- Ransomware

Viren
Begriffserklärung

Der Begriff Virus ist älter und häufig nicht klar abgegrenzt.
So ist z.B. die Rede von Virenschutz, womit aber viel allgemeiner der Schutz vor Schadsoftware jeglicher Art gemeint ist.

Ein typischer Virus verbreitet sich, während die heute gängigen Schadprogramme die Struktur von Trojanischen Pferden zeigen, deren primärer Zweck nicht die Verbreitung, sondern die Fernsteuerbarkeit ist.

Trojaner
Begriffserklärung

Ein Trojanisches Pferd (kurz Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder eine Backdoor.

Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Würmer
Begriffserklärung

Ein Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netze wie das Internet und versucht, in andere Computer einzudringen.

Spyware/Adware (Grayware)
Begriffserklärung

Grayware wird teils als eigene Kategorie benutzt, um Software wie Spyware und Adware oder andere Varianten, die Systemfunktionen nicht direkt beeinträchtigen, von eindeutig schädlichen Formen abzugrenzen.

Spyware und Adware forschen den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller oder andere Quellen, um diese entweder zu verkaufen oder um gezielt Werbung zu platzieren.

Spyware/Adware (Grayware)
Begriffserklärung

Diese Form von Malware wird häufig zusammen mit anderer, nützlicher Software installiert, ohne den Anwender zu fragen, und bleibt auch häufig nach deren Deinstallation weiter tätig.

- Als Spyware bezeichnet man Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten
- Adware wird Software genannt, die – häufig zusammen mit gewünschten Installationen oder Webabrufen – ohne Nachfrage und ohne Nutzen für den Anwender Funktionen startet, die der Werbung oder auch Marktforschung dienen

Scareware/Rogueware Begriffserklärung

Scareware oder auch Rogueware ist darauf angelegt, den Benutzer zu verunsichern und ihn dazu zu verleiten, schädliche Software zu installieren oder für ein unnützes Produkt zu bezahlen.

Beispielsweise werden gefälschte Warnmeldungen über angeblichen Virenbefall des Computers angezeigt, den eine käuflich zu erwerbende Software zu entfernen vorgibt.

Manche Versionen werden kostenpflichtig angeboten, andere Versionen installieren weitere Schadprogramme während des Täuschungsvorgangs

Ransomware
Begriffserklärung

Ransomware blockiert den Zugriff auf das Betriebssystem bzw. verschlüsselt potenziell wichtige Dateien und fordert den Benutzer zur Zahlung von Lösegeld auf – meist über Coupon-Bezahlsysteme wie Ukash oder Paysafecard.

Beispiel: Der sogenannte BKA-Trojaner

Schadprogramme
Mobile Bedrohungen

In den letzten Jahren hat die quasi rasende Verbreitung von Smartphones/Tablets die Aufmerksamkeit der Schadsoftware-Szene vermehrt auf sich gezogen.
Laut Kaspersky Security Bulletin 2013/2014 sind 62% der schädlichen Anwendungen Teile mobiler Botnetze.

Im 4. Quartal 2014 entdeckten Kaspersky Labs 103.072 neue mobile Schadprogramme und 1.527 mobile Banktrojaner.

Alle Techniken und Mechanismen zur Infektion und Verschleierung von schädlicher Aktivität werden sehr schnell vom PC auf die mobile Plattform Android übertragen.
Offenheit und Popularität dieses Betriebssystems begünstigen diese Tendenz.

Schadprogramme
Mobile Bedrohungen

Die meisten mobilen schädlichen Anwendungen sind auf den Diebstahl von Geld und erst in zweiter Linie auf den Diebstahl von persönlichen Informationen ausgerichtet.

Bei der Mehrheit der mobilen Schadprogramme handelt es sich um Bots mit umfassender Funktionalität.
In nächster Zeit wird ein Handel mit mobilen Botnetzen einsetzen.

Ganz eindeutig ist eine „Bankenausrichtung“in der Entwicklung mobiler Schadprogramme zu beobachten.
Die Virenautoren verfolgen die Entwicklung der Online-Banking-Dienste sehr genau.
Bei erfolgreicher Infektion eines Smartphones wird sofort überprüft, ob das Telefon mit einer Kreditkarte in Verbindung steht.

Schadprogramme
Prognosen

Trojanische Pferde in E-Mail-Dateianhängen werden immer seltener, während die Angriffe über das Web etwa mittels Drive-by-Download zunehmen.
Außerdem kommt der Einsatz von Rootkit-Techniken zum Verstecken der Schädlinge immer häufiger vor.

Laut dem Kalifornischen Malware-Spezialisten Kindsight Security waren 2012 in Deutschland durchschnittlich 13% der privaten Rechner durch Malware infiziert.

Viren - (K)Ein Thema für Linuxer?

Können sich Linux-Nutzer generell sicher fühlen?

> ≫*Nur, weil sie von den Cyber-Kriminellen bisher kaum beachtet wurden. Aber das kann sich ändern.*≪*(Jewgeni Kasperski, 2008)*

Eigentlich ist unter Linux kein Virenscanner nötig, da bestehende Sicherheitskonzepte ausreichen.

Einige Firmen bieten dennoch Virenscanner für Linux an, die beispielsweise auf Dateiservern sinnvoll sind, die auch von Windows-Clients genutzt werden.

Linux-Viren

- Linux / Hutizu-A / Backdoor.Linux.Hutizu.a (Trojaner)
- Hand of Thief (Trojaner)
- Lupper / Plupii.C / Lupper.worm.b / Lupper-I und Mare.d. (Wurm)
- OSF.8759 (Virus, Infiziert ELF-Binärdateien auf Linux-Systemen)
- ...

Linux-Programme zur Virenbekämpfung

- ClamAV
- AVG free
- Avast
- Comodo
- Kaspersky
- BitDefender
- F-Prot

Live-Systeme
Schadprogrammbekämpfung

- Kaspersky Rescue Disk
- AVG Antivir
- Avira Rescue System
- Desinfec't
- Acronis Antimalware

Schadprogramme
Fazit

Die größte Gefahr sitzt in der Praxis vor dem Bildschirm:
Auch das beste Betriebssystem kann nicht verhindern, dass ein unvorsichtiger Anwender seine Bankdaten per unverschlüsselter E-Mail versendet oder gar an einen Phisher verrät.

Auch die Installation von Programmen, die nicht aus den geprüften, offiziellen Paketquellen stammen, kann böse enden.

Schadprogramme
Fazit

Einerseits entfallen unter Linux diffuse Gefahren wie Würmer, Viren, Spyware & Co. (weitestgehend)

Dennoch ist es eine Sache gesunden Menschenverstands, bei sensiblen Daten prinzipiell wachsam zu sein.
Und sich die folgenden Grundsätze immer wieder vor Augen zu halten:

- 100% Sicherheit gibt es nicht!
- Sicherheit ist ein Konzept, keine Hard- oder Softwarelösung
- Sicherheit ist immer auch ein stückweit unbequem
- ein Computer ist so sicher wie ein Benutzer im Umgang mit demselben

Exkurs
Brauche ich eine »Personal Firewall«?

Sicherheitsprogramme unter Windows sind zwar unverzichtbar, betreiben aber zu einem großen Teil auch Augenwischerei:

Virenscanner und Firewalls versuchen durch Symbole oder Meldungsfenster auf sich aufmerksam zu machen, damit der Anwender sich gut geschützt fühlt.

Dummerweise kann auch ein Schädling den Virenscanner oder die Firewall deaktivieren oder verändern, wenn er einmal ins System gekommen ist.

Schließlich hat ein Benutzer mit Administrator-Rechten völlige Freiheit - auch die, den Computer zu infizieren.

Exkurs
Brauche ich eine »Personal Firewall«?

Eine sogenannte Personal Firewall hat unter Windows zwei Aufgaben:

- Sie blockiert Zugriffe aus dem Internet auf Dienste, die aus irgendwelchen Gründen auf dem Rechner laufen.

GNU/Linux Standardinstallationen bietet im Internet erst gar keine Dienste an, also gibt es auch nichts, was man blockieren müsste.

Im Gegenteil: Auch eine Firewall ist ja nur ein Stück Software und kann selbst Sicherheitslücken enthalten. Umso besser, wenn man auf sie verzichten kann.

Exkurs
Brauche ich eine »Personal Firewall«?

- Sie blockiert unerwünschte Zugriffe auf das Internet für Programme, die man absichtlich oder unabsichtlich (Viren, Trojaner) auf seinem Computer installiert hat

Eine versehentliche Softwareinstallation ist durch das konsequent eingehaltene Sicherheitskonzept nicht möglich, und wenn die sicheren, überprüften Paketquellen genutzt werden, ist eine Firewall nicht nötig.

Darüberhinaus laufen auf modernen Routern ohnehin schon recht effektive Firewalls.

duckundweg

Live-Demo der aktuellen Desinfec't

Links zur Präsentation

http://www.clamav.net/ http://free.avg.com/de-de/homepage
http://www.avadas.de/freeware/avast-free-antivirus-fuer-linux.html
http://www.comodo.com/products/free-products.php
http://www.kaspersky.com/de/
https://de.wikipedia.org/wiki/Liste_von_Linux-Malware

Weitere Informationen bekommen Sie hier:

http://www.FreieSoftwareOG.org
und
Kontakt@FreieSoftwareOG.org

oder kommen Sie doch einfach zu unserem regelmäßigen Treffen,
jeden 1. Mittwoch im Monat ab 20:00 Uhr.
(Treffpunkt und Thema laut Webseite)

FreieSoftwareOG.org