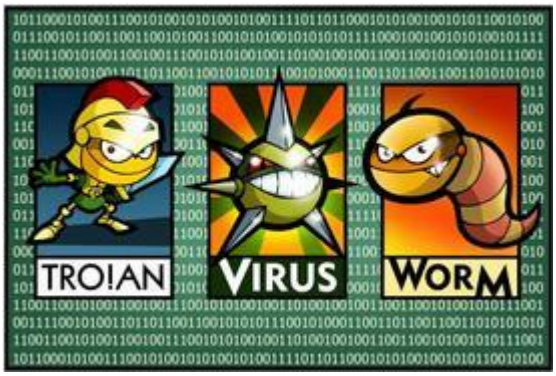
Linux en virussen

Handleiding van Helpmij.nl

Auteur: femke98

Juni 2014



Alle computersystemen kunnen last krijgen van malware en virussen, dus ook een Linux computer. Er zijn gelukkig heel weinig virussen voor Linux beschikbaar, zodat gebruikers doorgaans geen antivirussoftware hoeven te installeren. Toch is het verstandig en aanbevolen dat Linux-gebruikers antivirussoftware installeren op hun Linux-systemen als deze op een netwerk zitten met Windows computers.

Er worden immers bestanden over en weer verstuurd en sommige van deze bestanden worden weer naar andere personen via de mail verzonden.

Sommige gebruikers zullen beweren dat antivirussoftware te veel van het systeem zal eisen, anderen zullen beweren dat het op een Linux computer helemaal niet nodig is. Bedenk echter dat banken tegenwoordig bijna eisen dat op elke computer antivirussoftware is geïnstalleerd. Gelukkig bestaan er voor Linux goede antivirus-programma's en deze zijn zeer eenvoudig te installeren. Om antivirusprogramma's beter te begrijpen, kan het handig zijn om malware zelf te begrijpen.

Vormen van malware:

Malware - Malware is "slechte" software. Malware omvat alle software die een systeem, gegevens of processen / applicaties schaadt. Veel van de malware categorieën overlappen elkaar zoals trojans en spyware.

Trojan - Trojans zijn schadelijke programma's waarmee acties worden uitgevoerd die niet zijn geautoriseerd door de gebruiker. Deze acties kunnen zijn:

- Gegevens verwijderen
- Gegevens blokkeren
- Gegevens wijzigen
- Gegevens kopiëren
- Prestaties van computers of computernetwerken negatief beïnvloeden

In tegenstelling tot computervirussen en wormen kunnen trojans zichzelf niet repliceren.

Spyware - Deze malware verzamelt privégegevens van een gebruiker (financiële informatie, wachtwoorden, gebruikersnamen, etc.) en stuurt deze naar de spyware maker of andere entiteit, die de informatie zal gaan gebruiken. Spyware kunnen trojans zijn en sommige trojans kunnen spyware zijn.

Adware - Adware is de naam voor programma's die zijn ontworpen om advertenties op je computer weer te geven, je zoekopdrachten om te leiden naar reclamewebsites en marketinggerelateerde gegevens over je te verzamelen, bijvoorbeeld welk type websites je bezoekt. Op basis hiervan kunnen dan aangepaste advertenties worden weergegeven. Met adware worden gegevens verzameld met jouw toestemming. Dit moet niet worden verward met Trojaanse spywareprogramma's, waarmee gegevens worden verzameld zonder je toestemming. Omdat de meeste Linux-ontwikkelaars open-source applicaties maken, zijn er niet heel veel Linux-adware programma's te vinden.

Worms - Een computerworm (of kortweg worm) is een zichzelf vermenigvuldigend computerprogramma. Via een netwerk worden kopieën van deze worm doorgestuurd zonder een tussenkomst van een gebruiker. Een worm is geen computervirus want hij heeft geen computerprogramma nodig om zich aan vast te hechten. Men kan stellen dat een worm schade toebrengt aan een netwerk, waar een virus een gerichte aanval op een computer doet.

Veel lezers vragen zich misschien af: "Wat is het verschil tussen een virus en worm? '. Het antwoord is eenvoudig: virussen hechten zich aan programma's en wormen zijn standalone software.

Virussen komen via programma's binnen die gebruikers downloaden en wormen breken in via het netwerk. Als algemene regel kan je stellen dat wanneer een gebruiker het zelf binnen het systeem brengt, dan is het een virus. Komt iets zonder tussenkomst van de gebruiker in de computer, dan is het een worm.

Virussen

Computervirussen zijn een stuk code welke zich kan vermenigvuldigen en in principe altijd schadelijk is voor je pc. Er zijn verschillende soorten computervirussen.

Zombies - Een zombiecomputer (vaak afgekort tot zombie) is een computer die geïnfecteerd is met een Trojaans paard, spyware of virus. Deze kwaadaardige software kan de maker van die software in staat stellen om de geïnfecteerde pc via het internet over te nemen.

Riskware - Riskware is de naam voor legitieme programma's die schade kunnen aanrichten als kwaadwillende gebruikers deze benutten om gegevens te verwijderen, blokkeren, wijzigen of kopiëren, en om storingen te veroorzaken op computers of in netwerken.

Scareware - Software die door middel van bijvoorbeeld popups de gebruikers bang maakt, om deze zo te verleiden tot aankoop van een product. Bekend zijn de pop-ups met de melding dat de pc van de gebruiker vol zit met virussen. Uiteraard zal de in de pop-up genoemde virusscanner deze, tegen betaling, kunnen verwijderen. In de meeste gevallen zijn echter zowel de meldingen als de virusscanner volledig nep, soms bevat de scareware zelf een lading malware.

Samengevat, scareware laat computergebruikers schrikken zodat zij na het betalen van geld of het installeren van malware zichzelf denken te beschermen tegen een niet-bestaande dreiging.

Ransomware - Ransomware betekent letterlijk: gijzelingssoftware. Hiermee blokkeren criminelen uw computer. Deze digitale afpersers doen zich vaak voor als de politie. U zou zich schuldig hebben gemaakt aan strafbare feiten en daarom een boete moeten betalen. Niets is minder waar: het bericht is niet afkomstig van de politie en uw computer blijft ook na betaling geblokkeerd.

Antivirus Software / virusscanners

Dit zijn computerprogramma's die schadelijke software zoals virussen en wormen opsporen, voorkomen en actie ondernemen om deze te verwijderen of onschadelijk te maken. Afhankelijk van de instellingen van het programma kan de malware direct worden verwijderd of de gebruiker kan worden gevraagd wat te doen met de kwaadaardige software.

ClamAV - De meest populaire Linux-antivirussoftware is ClamAV. ClamAV is een command-line antivirus-programma dat gratis en open-source is onder de GPL licentie. De updates zijn ook gratis. Het webadres van ClamAV is www.clamav.net. Gebruikers kunnen naar de website om het programma te downloaden of ze kunnen het volgende commando in de terminal gebruiken (kopieër en plak):


```
sudo apt-get install clamav clamav-daemon clamav-freshclam
```

ClamAV's definities worden bijgewerkt via freshclam. Typ "sudo freshclam" om de definities van de virusscanner bij te werken.

ClamTK - clamtk is een grafische gebruikersinterface voor ClamAV. ClamTK is gelicenseerd onder de GPL-licentie. Om ClamTK installeren, ga je naar http://www.clamtk.sourceforge.net en download de software of gebruik het volgende commando in de terminal (kopieër en plak):

```
sudo apt-get install clamtk
```

Avast - Avast is een gratis antivirus software. Avast is geen open-source en gebruikt doorgaan veel RAM-geheugen. Veel gebruikers vinden dat Avast meer bescherming biedt dan ClamAV. De betaalde versie van Avast biedt tal van functies die in ClamAV ontbreken. Bezoek http://www.avast.com/nl-nl/index en download de applicatie.

AVG - Anti-Virus Guard is een gratis antivirusbescherming welke kan worden gedownload via deze link: http://free.avg.com/us-en/download.prd-alf

Comodo - Comodo is een gepatenteerde scanner die kan worden gedownload van: https://www.comodo.com/home/internet-security/antivirus-for-linux.php

Kaspersky - Kaspersky is een eigen scanner die kan worden gevonden via deze link: http://www.kaspersky.com/product-updates/linux-file-server-antivirus

Bescherming en repareren:

De beste manier om een systeem te beschermen is door alleen programma's te downloaden en te installeren van vertrouwde sites en ontwikkelaars. Programma's uit de officiële repository van je distro zijn altijd te vertrouwen.

Er zijn twee manieren om malware te verwijderen. De eerste methode omvat het gebruik van een virusscanner die de malware probeert te vinden en te verwijderen. De tweede manier is om de uitvoerbare bestanden handmatig te scannen, zeker wanneer deze programma's niet van officiële repositories komen. Denk hierbij aan PPA's die nog weleens gebruikt worden. (Een ppa is een Personal Package Archive. Dit zijn online-softwarebronnen die gebruikt worden om de nieuwste versies van softwarepakketten, digitale projecten en andere toepassingen te verzorgen.)

De beste manier om beschadigde uitvoerbare bestanden te herstellen, is de geïnfecteerde of beschadigde software opnieuw te installeren. Om jezelf te beschermen tegen malware is het belangrijk om te weten dat malware alleen in een uitvoerbaar of executable bestand kan zitten. Zo kan een PNG, MP3 en FLV-bestanden geen virussen bevatten, omdat ze geen programmabestanden zijn. De gebruiker opent een programma om deze bestanden te bekijken of te beluisteren. Let wel wanneer je via p2p netwerken MP3 of PNG bestanden ophaalt, dat deze geen .exe erachter hebben staan, want dan zijn het wel executable bestanden en dus uitvoerbaar.

Bovendien, vergeet niet dat de meeste screensavers executables zijn, zodat malware zich kan verbergen in screensavers.

Hoewel er voor Linux zeer weinig virussen in omloop zijn, is het verstandig om alle computers en servers te voorzien van een bescherming tegen malware. Weten hoe malware werkt en hoe je computers moet/kan beveiligen zal helpen bij de bescherming van deze systemen.

Maar wat nog belangrijker is: hou je hoofd erbij! Ook al denk je met een Linux computer safe te zitten, de banken zullen waarschijnlijk anders reageren als je geld opeens weg is. En dan heb je een groot probleem. Bekijk de uitzending van Radar maar eens waarin je goed kan zien dat banken nog altijd de schuld bij de klant neerleggen en dat deze hun onschuld moeten bewijzen. Terwijl het toch eigenlijk andersom zou moeten zijn!!

Bekijk de uitzending van Radar HIER. Tegelijkertijd kan je op deze pagina van de website het een en ander lezen over de eisen die banken stellen. Het is maar dat je het weet!!