Sicherheit von Linuxdesktops

ein Vortrag von Marius Schwarz

im Rahmen des LPD 2017

Sicherheit von Linuxdesktops

Sind Linuxsysteme sicherer als bspw. Windows?

Sicherheit von Linuxdesktops

Fakten

„Jede von Menschen geschriebene Anwendung kann Schwachstellen haben, die ein Angreifer ausnutzen kann.“

„Schwachstellen entstehen auf allen Ebenen durch menschliches Versagen.“

„Je mehr Menschen sich den Programmcode ansehen, desto weniger Schwachstellen werden enthalten sein.“

Sicherheit von Linuxdesktops

Beispiele für Schwachstellen

Der zum Bau des Programms genutzte Compiler, baut anfälligen Programmcode zusammen.

Der Programmierer des Programms, baut in Unkenntnis der Angriffsmöglichkeiten eine Schwachstelle ein, weil das Programm so schnell und einfach geschrieben werden kann.

Der Projektleiter steht unter Zeitdruck und testet die Software nicht ausreichend.

Sicherheit von Linuxdesktops

Angriffsszenarien

Direkter Angriff eines „Dienstes“ von außen:

Angriff auf die Netzwerkkarte
Angriff auf einen Serverdienst

Exploiten einer Schwachstelle von innen:

Angriff auf das Emailprogramm
Angriff auf den Browser
Angriff auf eine Systemkomponente (z.b. Bild)

Angriff auf menschliche Schwächen:

Phishingmails oder Telefonanrufe von Enkeln

Sicherheit von Linuxdesktops

Sicherheitsarchitektur unter Linux

Opensource für Programme

Updateverhalten des Betriebssystems

Security Enhanced Linux – SELinux

Ausführungscontexte

Benutzerkontentrennung

CHROOT-Jails für Programme

QUBES – Container für alle

von Marius Schwarz für LPD 2017 in Braunschweig

Sicherheit von Linuxdesktops

Opensource für Programme

Fast alle wichtigen Programme werden in Teams programmiert.

Dadurch können viele Augen über den geschriebenen Programmcode schauen.

Da sich jeder Mensch den Programmcode ansehen kann, wird einer davon ein Problem erkennen und es entweder zu beheben wissen, oder es für seine Zwecke ausnutzen.

Diese Entscheidung macht den Unterschied zwischen Gut und Böse aus.

Nicht in den Programmcode sehen zu können, schützt nicht vor Angriffen auf die enthaltenen Schwachstellen.

Sicherheit von Linuxdesktops

Updateverhalten des Betriebssystems

Genauso wichtig wie das Erkennen von Schwachstellen, ist der Umgang mit Updates von Programmen.

Alle gängigen Linux Distributionen updaten entweder LIVE, sobald ein Update entdeckt wird, oder wenn der Rechner runtergefahren wird.

Die Linuxdistributoren stellen Updates unmittelbar zur Verfügung, sobald ein (Sicherheits)Patch für eine Schwachstelle vorhanden ist.

Jede Minute könnte Patchday sein, im Gegensatz zu Microsoft,Apple und anderen Softwareherstellern.

Sicherheit von Linuxdesktops

Sicherheit durch Exotismus

Laut der „Fedora Foundation“ nutzen mehrere Millionen Rechner Fedora-Linux als Desktopbetriebssystem.

Linux insgesamt kommt auf einen Anteil von 2.2% *.

Ein automatisierter Angriff per Email lohnt sich nur, wenn man auch überproportional oft auf ein Opferbetriebssystem trifft.

Es ist keine gute Idee sich darauf zu verlassen.

* Quelle: Computer Bild 6.10.2016

Sicherheit von Linuxdesktops

Anzahl der Fehler in einem Betriebssystem

Je mehr Programmcode vorhanden ist, desto mehr Fehler gibt es.

Aufgrund der Aufteilung in viele Entwicklerteams im Linuxumfeld, werden häufiger Meldungen zu Schwachstellen veröffentlicht, die in Closedsource-Programmen wie z.B. Windows „still“ behoben werden.

Es entsteht der falsche Eindruck, daß unter Linux weniger Sicherheit herrschen würde. Es wird gern vergessen, daß jede Veröffentlichung auch mit einem Patch für diese Lücke einhergeht.

Sicherheit von Linuxdesktops

Sind Linuxsysteme sicherer als bspw. Windows?

Sicherheit von Linuxdesktops

Ja, etwas.

Sicherheit von Linuxdesktops

Der Programmcode von Linux wird i.d.R. von mehreren tausend Menschen gesichtet, geprüft und korrigiert.

Sicherheit von Linuxdesktops

Der Programmcode von Linux wird i.d.R. von mehreren tausend Menschen gesichtet, geprüft und korrigiert.

Zudem sind Sie als Linuxbenutzer seltener Zielscheibe von Trojanern per Email.

Sicherheit von Linuxdesktops

Der Programmcode von Linux wird i.d.R. von mehreren tausend Menschen gesichtet, geprüft und korrigiert.

Zudem sind Sie als Linuxbenutzer seltener Zielscheibe von Trojanern per Email.

Außerdem gibt es bei Linux keinen Patchday. Fehler- und Sicherheitsupdates werden so schnell wie möglich verbreitet.