Предимства на Linux срещу Windows от гледна точка на Сигурността

Йордан Димов(flipfl0p)

Първо, какво се има предвид под „сигурност“.

1. Наличност: нашите данни и ресурси ще бъдат достъпни когато ни трябват.
2. Цялостност: никой освен нас няма достъп да променя нашите данни
3. Конфиденциалност: никой няма достъп да разглежда нашите данни ако не е оторизиран за това

Потенциални заплахи: кракери, вируси, червеи, троянски коне, злонамерени или случайни инциденти.

От Microsoft казват:

Windows е по-разпространена операционна система от Linux. Затова подлежи на повече и по-чести атаки. Ако Linux имаше толкова потребители колкото Windows, щеше да бъде по-често атакуван.

На практика:

Linux е много по-широко използван като web server платформа в Интернет.

68% - Apache
21% - Microsoft IIS
11% - Други

(статистиката на NetCraft за Септември 2004г.)

Въпреки това:

Всички известни вируси и червеи които са създавали сериозни проблеми в Интернет заразяват единствено IIS сървъра на Microsoft. Примери: CookRed, Nimda, IIS Worm и др.

Писани са червеи и за Apache, но никога не са се разпространявали успешно, защото е много лесно да се отстранят или блокират. Пример: Sloppe

Reboot times – мярка за стабилност

При изследвания е доказано, че машина с ОС на Microsoft се рестартира средно на 60 дни.

Машини с Linux могат да не се рестартират с години.

(като сървъри)

Microsoft казват:

Софтуерът с отворен код е по-несигурен, защото кракерите могат по-лесно да намерят дефекти в него и да го атакуват.

На практика:

За Windows има огромно количество вируси, троянски коне, spyware, adware и тн., които не могат да заразят Linux система по никакъв начин. Когато една машина с Windows XP се свърже в Интернет, отнема средно 16 минути да бъде тя заразена или атакувана.

Всички статисти от предишната точка важат(Apache е opensource а IIS е затворен)

От Microsoft казват:

След като е била намерена уязвимост, отнема повече време да се поправи при Linux отколкото при Windows.

На практика:

Това е фантазия. Всеки, който следи бюлетините за сигурност знае, че поправки(patches) за Linux излизат до ден-два след обявената уязвимост, а за Windows поне месеци а понякога дори години. Пример: URL encoding volation при IIS.

Реалност:

Повечето от вирусите, троянските коне и тн. Заразяват Windows системи чрез Internet Explorer(browse) или Microsoft Outlook(e-mail). При Linux такива проблеми почти не съществуват.

Причини:

I. Windows едва наскоро се превърна в многопотребителска система.

Първоначално, Windows бе проектирана така, че да се използва само от един потребител и да дава на него на всички програми пълен достъп до всички компоненти на системата(CPU, памет и тн.). Понеже критичните части на операционната система не бяха защитени, беше много лесно да се пишат вируси и троянски коне които да правят каквото си поиска авторът им.

Едва при Windows XP започнаха да се правят сериозни опити за отделяне на потребителските от системните пространства. Поради това обаче, програми писани за по-стари версии на Windows не работят под XP. Освен това, XP приема, че отдалечените компютри по мрежата са използвани само от един единствен потребител и им се предоверява.

Windows Server 2003 се доближава най-близо до истинска много потребителност но и там има проблеми.

За разлика от тях, Linux е наследник на Unix която е истинска многопотребителска система още от самото си създаване през 1970-те години

II. Windows е монолитна а не модулна система.

Това означава, че почти всички възможности на Windows се свързват в един единствен основен компонент. За разлика, Linux е строго разделена на слоеве и модули, всеки от които се грижи за строго специфична задача.

Под Windows например е невъзможно да се премахне web browser-ът Internet Explorer, защото е част от ядрото.

Дори когато не искате да го използувате, части от него се стартират всеки път когато използвате MS Outlook, Windows Explorer, Windows Help дори Control Panel и много други приложения. По този начин всяка уязвимост на IE може да се атакува чрез всяко от тези

приложения, дори и никога да не сте използвате IE.

Освен това в една монолитна система като Windows, където всички функции са навързани като котешки червa, всеки сриv в един компонент води до сриv на цялата система.

(стабилност)