**Miras Nussupov, Zhanbaj Uzdenbaev**

**(Taldykorgan, Kazakhstan)**

**REASONS TO CHOOSE LINUX IN TERMS OF SECURITY**

Undertakings contribute a ton of time, exertion and cash in keeping their systems secure. The most security-cognizant may have a security activities focus. They obviously utilize firewalls and antivirus instruments. They most likely invest a considerable measure of energy checking their systems, searching for obvious inconsistencies that could show a rupture.

In any case, what number of have given much idea to one of the foundations of their advanced activities: the working systems sent on the workforce's PCs? Was security even a factor when the work area OS was chosen? This brings up an issue that each IT individual ought to have the capacity to reply: Which working system is the most secure for general organization?

One reason undertakings won't not have assessed the security of the OS they conveyed to the workforce is that they settled on the decision years prior. Backpedal sufficiently far and every working system were sensibly protected, in light of the fact that the matter of hacking into them and taking information or introducing malware was in its earliest stages. What's more, once an OS decision is made, it's difficult to think about a change. Scarcely any IT associations would need the migraine of moving an internationally scattered workforce to an altogether new OS.

Unquestionably the dangers defying endeavor systems have changed over the most recent couple of years. Assaults have turned out to be significantly more complex. The solitary youngster programmer that once overwhelmed the general population creative energy has been supplanted by efficient systems of crooks and shadowy, government-financed associations with huge registering assets.

The OS you convey to your clients makes a distinction for your security position, yet it isn't a certain protect. For a certain something, a break nowadays will probably come to fruition in light of the fact that an assailant examined your clients, not your systems. Conveying a safe working system is a vital beginning stage, however without client instruction, solid firewalls and consistent cautiousness, even the most secure systems can be attacked. Also, obviously there's dependably the danger of client downloaded programming, augmentations, utilities, modules and other programming that seems amiable yet turns into a way for malware to show up on the system.

What's more, regardless of which stage you pick, a standout amongst other approaches to keep your system secure is to guarantee that you apply programming refreshes immediately. Once a fix is in the wild, all things considered, the programmers can figure out it and locate another endeavor they can use in their next flood of assaults.

In case you're a security supervisor, it is to a great degree likely that the inquiries raised by this article could be rethought like so: Would we be more secure in the event that we moved far from Microsoft Windows? To state that Windows rules the undertaking market is to downplay the case.

On the off chance that your systems fall inside that 88%, you're most likely mindful that Microsoft has kept on amplifying security in the Windows system. Among its upgrades have been modifying its working system codebase, including its own particular antivirus programming system, enhancing firewalls and executing a sandbox engineering, where programs can't get to the memory space of the OS or different applications.

However, the ubiquity of Windows is an issue in itself. The security of a working system can depend to a huge degree on the extent of its introduced base. For malware creators, Windows gives a gigantic playing field. Focusing on it gives them the most blast for their endeavors [1].

On the off chance that the most well known OS is continually going to be the greatest target, at that point can utilizing a less prominent alternative guarantee security? That thought is another interpretation of the old — and altogether defamed — idea of "security through indefinite quality," which held that keeping the internal workings of programming restrictive and along these lines mystery was the most ideal approach to protect against assaults.

Joe Moore of Wolf Solutions gives Apple more credit, saying that "off the rack, macOS X has an incredible reputation with regards to security, to some extent since it isn't as broadly focused as Windows and to some degree since Apple completes an entirely great job of remaining over security issues." [2]

You likely knew this from the earliest starting point: The unmistakable accord among specialists is that Linux is the most secure working system. Be that as it may, while it's the OS of decision for servers, ventures conveying it on the work area are rare.

What's more, on the off chance that you decided that Linux was the approach, you would even now need to choose which dissemination of the Linux system to pick, and things get more confused there. Clients will need a UI that appears to be well-known, and you will need the most secure OS.

Obviously, an essential differentiator is that Linux is open source. The way that coders can read and remark upon each other's work may appear like a security bad dream, however it really ends up being a vital motivation behind why Linux is so secure, says Igor Bidenko, CISO of Simplex Solutions. "Linux is the most secure OS, as its source is open. Anybody can survey it and ensure there are no bugs or secondary passages."

Wilkinson expounds that "Linux and Unix-based working systems have less exploitable security blemishes known to the data security world. Linux code is inspected by the tech group, which fits security: By having that much oversight, there are less vulnerabilities, bugs and dangers."

That is an inconspicuous and maybe irrational clarification, yet by having handfuls, or some of the time hundreds, of individuals read through each line of code in the working system, the code is in reality more hearty and the possibility of defects slipping into the wild is lessened.

Another factor referred to by PC World is Linux's better client benefits show: Windows clients "are for the most part given chairman access of course, which implies they essentially approach everything on the system," as indicated by Noyes' article. Linux, interestingly, incredibly confines "root" [3].

Dormancy is an intense power. Despite the fact that there is clear accord that Linux is the most secure decision for the work area, there has been no charge to dump Windows and Mac machines for it. In any case, a little however critical increment in Linux reception would presumably bring about more secure processing for everybody, on the grounds that in piece of the overall industry misfortune is one certain approach to stand out enough to be noticed. As such, if enough clients change to Linux on the work area, Windows and Mac PCs are probably going to end up more secure stages.

**References:**

1. The 10 most common Windows security vulnerabilities [Electronic resource]// - URL: https://searchenterprisedesktop.techtarget.com/tip/The-10-most-common-Windows-security-vulnerabilities - (date of treatment: 25.04.2018)
2. Apple Security Flaws Give Some Researchers Concern [Electronic resource]// - URL: https://www.wired.com/story/apples-security-macos-high-sierra-ios-11/- (date of treatment: 27.04.2018)
3. The state of Linux security in 2017 - Linux Audit [Electronic resource]// - URL: https://linux-audit.com/the-state-of-linux-security-2017/- (date of treatment: 29.04.2018)

**Scientific adviser:**

Candidate of Technical Sciences Uzdenbaev Zhanbaj Shujnshalievich.