

Much has been made of the robustness of Linux, relative to that of its chief rival, Windows. And while proponents from either side may argue a case convincingly, the fact remains that Windows-based machines are compromised far more often than their counterparts running Linux.

No one is saying that Linux is impervious to attack – just that it is successfully compromised far less frequently. One reason that has been advanced for this state of affairs is the diversity inherent in so many different Linux distributions, each using one of a number of package management systems.

Dr Ntsika Msimang, OpenProject Focus Area Leader at the CSIR's Open Source Centre, says the robustness of Linux is far deeper than the diversity inherent in having a large number of different distributions. "Linux is robust because its evolution follows the tried-and-tested scientific modus operandi. The more brains and eyeballs; the better the product."

MORE HINDRANCE THAN HELP

He believes there is a simple reason why proprietary software is compromised more frequently than open source software (OSS) products. "It is impossible for one company with a limited pool of talent and financial resources to design applications that suit the idiosyncratic needs of billions of people across the globe while at the same time having to anticipate all that could go wrong," he says.

"Scientific inquiry has proven over and over that when talent and resources are aggregated, human beings stand a better chance of improving their current state. I believe that OSS has taken a page from that and the results speak for themselves."

Andre Coetzee, creator of local distribution, Impi Linux, believes the diversity is both a good and bad thing. "Different distributions typically use different C libraries – also known as glibc. This means that a virus, for example, that has been compiled to run on one distribution is probably not going to execute on another if it uses a different version of glibc," he says.

"That's a good thing, but it's also a weakness because it inhibits the portability of applications. However, you can provision an application to execute on almost any glibc by actually including everything

in the installation pack. The difficulty with this is that the executable file becomes huge," he says.

Roy Blume, analyst at BMI-TechKnowledge (BMI-T), believes diversity is more of a hindrance than a help. "You've got 250 plus distributions of Linux and every one of them is slightly unique in its own special little stupid way – and I say that in the nicest possible way. That is the problem with Linux; there is no consistency across the different distributions," he says.

GEEKS DESIGNING FOR GEEKS

Msimang doesn't believe the diversity has much to do with the strength of Linux and says the lack of consistency across distributions probably results from 'geeks' designing for 'geeks' rather than for the average user. "It has more to do with the lack of 'customer' or 'end user' focus than it has to do with making Linux robust," he notes.

At the same time Msimang points to the emergence of user-centric distributions like Ubuntu, Mandriva and Novell (formerly SuSE) as a sign that the Linux market is maturing. "Making things easier for the average 'Joe or Sibongile' does not necessarily compromise the integrity of OSS. Ease of use and security do not have to be mutually exclusive propositions," he adds.

On the subject of making things easier, Coetzee says the Linux Standards Base (LSB) is addressing many of the problems highlighted by Blume.

LSB removes much of the uncertainty of packaging applications for different Linux distributions by mandating a common file structure, the format and location of configuration files, as well as ensuring predictability of certain settings in the administrative, operating system and user space.

Msimang also believes there is strength in the standardisation process that is currently under way. "That is why many OSS advocates are also unequivocal supporters of open standards.

"Consequently, any architecture or software needs to have a built-in proactive development mechanism that affords developers the opportunity to forestall any security breaches or quick recovery once the application has been compromised. It's the OSS development model that provides that mechanism," he concludes. ■

