Cos eye more options post CrowdStrike: Quick Heal

Pune: Entities operating critical infrastructure will think of diversification for sourcing their cybersecurity needs, drawing from their learnings from the recent CrowdStrike incident, Quick Heal CEO Vishal Salvi told TOI.

“The lapse was more of an error. But it could have been somebody who can create this and actually launch a cyberattack. It can be an intentional activity.That is something we need to worry about and people will start asking questions whether we want to put everything in one basket or diversify,” he said in an interaction.

On its end, Microsoft has already said that it will not give access to the kernel to third parties.

For any operating system, there is a core software called the kernel and all applications will sit on top of the kernel. Typically, applications are in user space and the operating system is in the core kernel.

Any compromise on user space will affect that particular application and nothing will happen to the operating system and device. But if something happens to the kernel, the entire operating system will crash, which is what happened in CrowdStrike, he said.

Commenting on long-term solutions, Salvi said that it is a continuous process. These incidents have happened in the past and the lessons are to be learnt from each one as to what kind of accountability can be put on the third-party cybersecurity companies. After the incident, all the cybersecurity providers, including Quick Heal, are looking into what can be done to prevent such instances, he said The SolarWinds malware attack, which led to data loss and compromise for several companies and the govt in the US, led to the creation of stricter compliance measures.