CACHE

Implications of India's new VPN rules

Will virtual servers be able to bypass the new CERT-in rules on virtual private networks?

THE GIST

- On April 28, India's cybersecurity agency passed a rule mandating Virtual Private Network (VPN) providers to record and keep their customers' logs for 180 days. It also asked these firms to collect and store customer data for up to five years. It further mandated that any cybercrime recorded must be reported to the CERT-In within six hours of the crime.
- Surfshark VPN stated that taking such radical action that highly impacts the privacy of millions of people in India will most likely be counterproductive and strongly damage the IT sector's growth in the country.
- The Ministry of Electronics and Information Technology said that the rules are applicable to "any entity whatsoever", regardless of whether they have a physical presence in India or not, as long as they deliver services to Indian users.

ABHISHEK CHATTERJEE
NABEEL AHMED

The story so far: On April 28, India's cybersecurity agency passed a rule mandating Virtual Private Network (VPN) providers to record and keep their customers' logs for 180 days. It also asked these firms to collect and store customer data for up to five years. It further mandated that any cybercrime recorded must be reported to the CERT-In (Computer Emergency Response Team) within six hours of the crime. The new directives, if passed, will be effective from June 28. In response to the CERT-In rules, Nord VPN, one of the world's largest VPN providers, has said it is moving its servers out of the country. Two other firms, Express VPN and Surfshark, said they will shut down their physical servers in India and cater to users in India through virtual servers located in Singapore and the U.K.

Who all will be affected by the new rules?

CERT-In directions are applicable to data centres, virtual private server (VPS) providers, cloud service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and government organisations. Firms that provide Internet proxy-like services through VPN technologies also come under the ambit of the new rule. Corporate entities are not under the scanner.

What is a virtual server, and what are its uses?

A virtual server is a simulated server environment built on an actual physical server. It recreates the functionality of a dedicated physical server. The virtual twin functions like a physical server that runs software and uses resources of the physical server. Multiple virtual servers can run on a single physical server.

Virtualising servers helps reallocate resources for changing workloads. Converting one physical server into multiple virtual servers allows organisations to use processing power and resources more efficiently by running multiple operating systems and applications on one partitioned server. Running multiple operating systems and applications on a single physical machine reduces cost as it consumes less space and hardware. Virtualisation also reduces cost as maintaining a virtual server infrastructure is low compared to physical server infrastructure. Virtual servers are also said to offer higher security than a physical server infrastructure as the operating system and applications are enclosed in a virtual machine. This helps contain security attacks and malicious behaviour inside the virtual machine.

Express VPN and Surfshark have said that they will shut down their physical servers in India and cater to users in India through virtual servers located in Singapore and the U.K.

Virtual servers are also useful in testing and debugging applications in different operating systems and versions without having to manually install and run them in several physical machines. Software developers can create, run, and test new software applications on a virtual server without taking processing power away from other users.

Can server relocation and virtualisation help VPN providers circumvent the new rules?

The FAQs published by the Ministry of Electronics and Information Technology (MeiTY) regarding the cybersecurity directions offers some clarity on relocation and virtualisation. It says the rules are applicable to "any entity whatsoever" in the matter of cyber incidents and cyber security incidents, regardless of whether they have a physical presence in India or not, as long as they deliver services to Indian users. The service providers who do not have a physical presence in India but offer services to the users in the country, have to designate a point of contact to liaise with CERT-In. Also, logs may be stored outside India as long as the obligation to produce logs to CERT-In is adhered to by the entities in a reasonable time.

VPN companies, like Surfshark, on the other hand believe that by removing their physical servers to countries outside India they will comply with the laws applicable to their activities, the company said to *The Hindu*.

How will the law impact India's IT sector?

In response to *The Hindu*'s queries on the impact of removal of physical servers from the country on jobs, SurfsharkVPN said "It would be difficult to estimate the exact number of individuals impacted in terms of employment because we were renting servers from Indian providers."

VPN suppliers leaving India is not good for its burgeoning IT sector. Taking such radical action that highly impacts the privacy of millions of people in India will most likely be counterproductive and strongly damage the IT sector's growth in the country, the company said in a release last week.

It estimated that 254.9 million Indians have had their accounts breached since 2004 and raised its concern that collecting excessive amounts of data within Indian jurisdiction without robust protection mechanisms could lead to even more breaches.

The Netherlands-based company further said that they have never received a similar directive on storing customer logs from any other governments in the world.

Does China have similiar rules regarding VPN usage?

Though not all VPNs are officially banned in China, only government-approved VPNs are officially permitted to function, Syed Ali Akhtar, Fellow at the National Law University, Delhi told *The Hindu*.

Visitors and Chinese citizens use VPNs to circumvent China's Great Firewall, which has blocked access to many websites, keywords and even IP addresses.

Government-approved VPNs have to register with the Chinese government and have to comply with data requests during investigations. However, cases of tourists being penalised for using non- government approved VPNs have not been reported, Akhtar said.