NordVPN Lists Five Measures to Supercharge Its Security

NordVPN Signs a Strategic Partnership with Versprite — a Leading Cybersecurity Consulting Firm

October 29, 2019. In the aftermath of a security incident involving NordVPN and a third-party data center, the company is taking action to enhance its security. One of the first moves is a long-term strategic partnership with VerSprite — one of the leading cybersecurity consulting firms.

The partnership will include threat and vulnerability management, penetration testing, compliance management and assessment services. VerSprite will also help to form an independent cybersecurity advisory committee, which will consist of selected experts and oversee NordVPN's security practices.

"We are planning to use not only our own knowledge, but to also take advice from the best cybersecurity experts and implement the best cybersecurity practices there are," says Laura Tyrell, Head of Public Relations at NordVPN. "And this is the first of many steps we are going to take in order to bring the security of our service to a whole new level."

According to NordVPN, they are ready to take action in five different fields to become more secure than ever. Here's the list of the planned measures:

1. Partnership with the top cybersecurity consulting firm VerSprite. Penetration testers are a key part of NordVPN's security efforts. Their job is to prod the infrastructure for weaknesses and mitigate the vulnerabilities. That's why NordVPN is engaging in a long-term strategic partnership with VerSprite, a leading cybersecurity consulting firm.

VerSprite will work with NordVPN's in-house team of penetration testers to challenge the infrastructure and ensure the security of customers. The main tasks covered in the new agreement include comprehensive penetration testing, intrusion handling, and source code analysis. VerSprite will also help to form an independent cybersecurity advisory committee.

2. Bug bounty program. Over the next few weeks, NordVPN is going to introduce a bug bounty program. Bug bounties reward cybersecurity experts for catching potential vulnerabilities and reporting to the developers so they can fix them. Bounty hunters will get a well-earned payout, and NordVPN users will get a service they know is scoured for bugs by thousands of people every day to make it as secure as possible.

3. Infrastructure security audit. NordVPN is planning to complete a full-scale third-party independent security audit in 2020. The audit will cover the infrastructure hardware, VPN software, backend architecture, backend source code, and internal procedures. The chosen vendor for the security audit will be announced in the upcoming weeks.

4. Vendor security assessment and higher security standards. NordVPN is planning to build a network of collocated servers. While still located in a data center, collocated servers are wholly owned exclusively by NordVPN. NordVPN is currently finishing its infrastructure review so that they can eliminate any exploitable vulnerabilities left by third-party server providers. NordVPN is committed to ensuring that their exclusively owned data centers maintain the highest security standards.

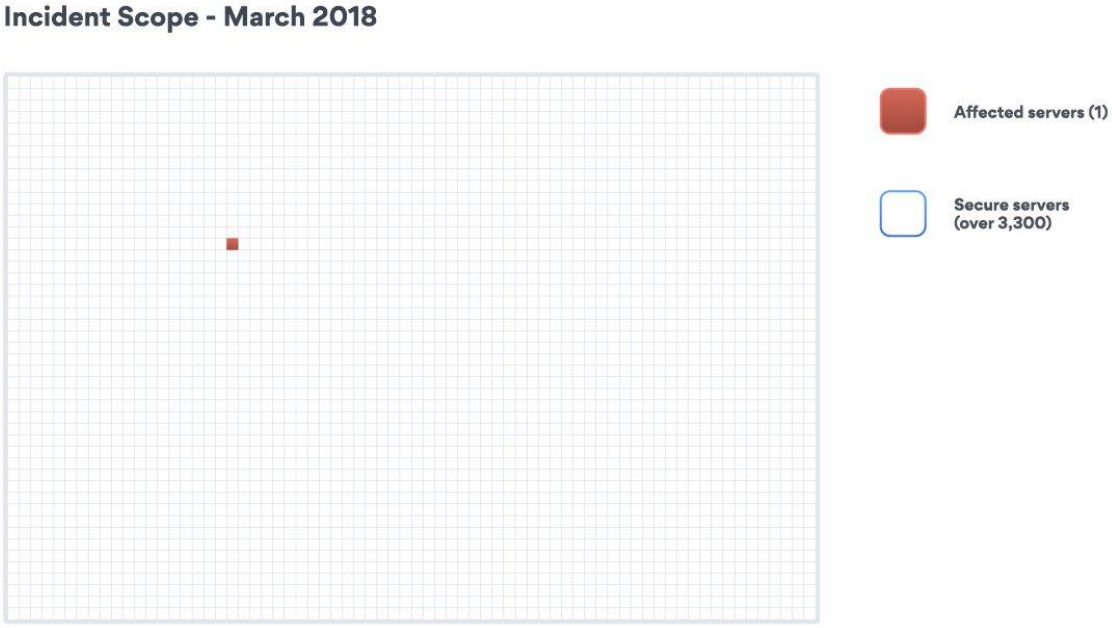
5. Diskless servers. NordVPN is planning to upgrade their entire infrastructure (currently featuring over 5100 servers) to RAM servers. This will allow to create a centrally controlled network where nothing is stored locally — not even an operating system. Everything the servers need to run will be provided by NordVPN's secure central infrastructure. If anyone seizes one of these servers, they'll find an empty piece of hardware with no data or configuration files on it.

"The changes we've outlined will make you significantly safer every time you use our service. Every part of NordVPN will become faster, stronger, and more secure – from our infrastructure and code to our teams and our partners," says Laura Tyrell. "That's our promise – we owe it to you."

What happened last week

Last week, it was announced that 1 of more than 5000 NordVPN's servers was accessed by an unauthorized third party. The hacker managed to access this single server located in Finland because of mistakes made by the data center owner, of which NordVPN was not aware.

However, NordVPN is sure that no customer data was affected or accessed by the malicious actor, as the server did not contain any user activity logs, usernames, or passwords. NordVPN's service as a whole was not hacked, the code was not hacked, the VPN tunnel was not breached, and the NordVPN apps stayed unaffected.



ABOUT NORDVPN

NordVPN is the world's most advanced VPN service provider, used by over 12 million internet users worldwide. NordVPN provides double VPN encryption, malware blocking, and Onion Over VPN. The product is very user-friendly, offers one of the best prices on the market, has over 5,000 servers in 60 countries worldwide, and is P2P friendly. One of the key features of NordVPN is zero-log policy. For more information: nordvpn.com.