AIRGAP

Unsecured VPNs Can be a Hot Mess

The shift to remote work created by the pandemic has exposed the shortcomings of virtual private networks and has led to a growing number of organizations embracing a "zero trust" model.

The NSA and CISA have issued recommendations with respect to choosing and hardening VPNs to prevent nation-state APTs from weaponizing flaws & CVEs that have the potential to infiltrate protected networks. These organizations recently recommended that enterprises "harden" their VPNs against hackers in light of the onslaught of cyberattacks.

VPNs became essential for the preservation of global business continuity during the pandemic, with the encrypted connections enabling remote employees to access enterprise networks. 87% of enterprises relied on VPNs as primary access points as they migrated to remote work globally, according to a survey of 630 IT security leaders by software firm NetMotion. The survey also found that the financial sector was the second-most active category for VPN usage, trailing only the legal industry by a narrow margin.

At the same time, there has been a surge in cyber-crime, exposing the shortcomings of VPNs and other types of perimeter security technology meant to insulate private enterprise networks from the public Internet. The NSA has identified numerous vulnerabilities and exposures in leading VPN products. One such attack resulted in the temporary shutdown of an organization's industrial processes after a ransomware group encrypted its control servers.

"We exposed many new flaws in the traditional VPN solutions in the last 18 months," said Ritesh Agrawal, CEO and Co-Founder of Airgap Networks, a cybersecurity vendor focused on ransomware prevention and mitigation. VPNs work by assigning a system-approved IP address to credentialed users, empowering them with total network access. *"[VPNs] were never designed as a primary means of enterprise access – and any such use is out of specification, obviously,"* Agrawal said.

> "Vulnerabilities in VPN servers are like welcome mats to nation-state advanced persistent threat (APT) actors. Often, they **weaponize VPN vulnerabilities** to break into protected networks."

AIRGAP

The problem with VPNs and other conventional perimeter security frameworks is that suspicious-activity filters inherently trust that a credentialed user is a legitimate sign-in.

As the SolarWinds breach in December 2020 revealed, single sign-on credentials can be hijacked in the cloud by sophisticated attackers to penetrate the perimeter and plunder enterprise networks.

Enter Zero Trust

VPNs are the doorways to private, sensitive internal networks and are exposed to the world for bad actors to compromise. Consequently, the failures of perimeter security technology have led to the wider adoption of the "zero trust" model. Zero trust means *"no network user, packet, interface or device – whether internal or external to the network – should be trusted,"* John Kindervag, creator of the strategy, wrote in The Wall Street Journal this year.

"Some people mistakenly think zero trust is about making a system trusted, but it really involves eliminating the concept of trust from cybersecurity strategy," said Kindervag, senior VP of cybersecurity strategy at ON2IT.

The National Institute of Standards and Technology describes zero trust as a set of principles that takes a *"holistic view that considers all potential risks to a given mission or business process"* and how those risks can be mitigated. There is no single *"specific infrastructure implementation or architecture, but it depends on the workflow"* being analyzed and the resources that are used in performing it, NIST said.

Dynamic Thinking

Zero trust products and services ensure that "applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities," according to Gartner, a market researcher. "The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack."

Lateral movements are most often the technique that a cyber-attacker leverages, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. "Once the attacker has breached an organization's digital boundaries or perimeter, the attackers are free to roam around internally and cause as much damage as they wish." said Agrawal. "It could take weeks or months before they are caught in the act and that's enough time for any attacker to wreak havoc."

One example of a Zero Trust technology and emerging VPN alternative is a software-defined perimeter (SDP), which safeguards networks by establishing "1-1 connections between users and the resources that they need," according to NetMotion. With SDPs, "users only get access to the application they requested and nothing more – preventing any kind of lateral movement, because connections are to the resource and not the whole network," NetMotion said.