verinext

TECH BRIEF

SECURITY AT THE EDGE: WELCOME TO THE CYBER-JUNGLE

It's a jungle out there in the world of cybersecurity. Organizations used to be able to contain their IT equipment and services within four walls. They could erect a strong perimeter and mount a reasonably successful defensive battle against attacks. These days, networks are distributed, active in clouds, and have sprawling virtual supply chains as well as an army of remote or hybrid workers. The network perimeter is gone. Traditional security strategies are no longer enough. New approaches are required.

In some ways it is akin to how battle tactics have shifted over the centuries. Back in the day, two armies met head-on along one clearly defined zone of conflict. In modern warfare, a superior force may mount an invasion. But keeping the conquered territory is a different matter. Both the U.S. and Russia struggled for years to hold Afghanistan against a highly distributed, nimble and hard-to-detect insurgency and guerrilla opponent.

With the prevalence of remote work and distributed networks, modern enterprises face a similar dilemma. How do they defend themselves against such an elusive adversary? They have so many vulnerable endpoints operating across a hodge podge of home networking and poorly protected internet of VPN connections that they don't know where the enemy may strike next. And strike they will. A few years ago, businesses might hope that they could avoid a breach. These days, it is a case of when, not if.

THE CYBERSECURITY PICTURE GETS SCARIER

It is a sad reflection on the state of security that many organizations are blissfully unaware that cybercriminals are already operating inside their walls – and have been doing so for months. The average data breach in the U.S. goes undetected for a staggering 206 days.

The massive leap in artificial intelligence (AI) capabilities has inevitably filtered into cybercriminal circles. The bad guys are harnessing this technology to make malware that is smarter and more effective. Take the recent announcement about Beep malware. It is a form of botnet implant malware that can operate at a massive scale and infect a large number of targets in a short time. But that is only part of the challenge. Beep employs exhaustive anti-analysis and detection-evasion techniques that make it extremely challenging to spot. And once inside, it enables adversaries to deploy ransomware and other nasty malware payloads onto compromised systems remotely.

The Verizon Data Breach Investigations Report (DBIR) also noted that ransomware continues its seemingly unassailable rise. Its presence in successful breaches grew by another 13% in 2022. Pre-COVID, ransomware played a part in only 4% of breaches and now it's present in about a quarter of all times where a hacker is able to enter a network.

DEVICE MADNESS MAKES HYBRID WORK EVEN MORE PRONE TO ATTACK

To make matters worse, the average employee now has more devices than ever in their possession. If they had only one device to manage, security professionals might have an easier time of it. But according to Enterprise Strategy Group (ESG), 50% of employees have five corporate and personal devices and another 20% have more than five devices. The sheer quantity of machines poses a serious problem for enterprise security. It is quite likely that one or more of these devices is not managed by IT. These users may have to enter passwords and get authorized to access the network. Nevertheless, they are typically operating in a home environment. Who knows how secure the Wi-Fi is and how many of their family members are using their devices to visit dodgy websites and download apps that could already be compromised.

If that wasn't bad enough, IT has its own internal headaches as well. ESG numbers show that only 6% of organizations use fewer than five management tools. 27% use 5-10, 33% have 11-15, 26% have 16-20 and 9% use an astonishing 20 or more. The analyst firm reports that having many tools makes the enterprise less secure. Those with 15 or more actually suffer by far the most breaches.

HYBRID IS HERE TO STAY

Some say there is an easy fix for all this. Bring remote workloads back in house and force employees to work in the office. If such a radical move were to happen, it would certainly simplify life for enterprise cybersecurity. But the cloud is not only here to stay, and it is growing. For every workload repatriated from the cloud, there are a dozen new ones went to the cloud. Even more, hybrid is here to stay; workers have demonstrated reluctance to return to the downtown 9-5 commuter grind.

According to Wakefield Research, 47% of employees would look for a new job if their employer didn't offer a flexible working model. They want at least some time to work from home if not the entire work week. Mercer's Global Talent Trends Study points out that around 80% of C-level executives believe it is crucial for companies to be more open and easier to relate to. That means listening to employees and not being too dictatorial about where they should work. Millions of jobs permanently became remote during the pandemic years and most aren't likely to come back. The long-expected return to the office looks like it may never happen.

EDGE SECURITY MUST STEP UP

The solution for cybersecurity reliance, then, does not lie in hopes of a sudden shift in the commuter zeitgeist. It entails adapting to this new employee paradigm by adopting a security framework that can do an efficient job of edge security. The key elements are Secure Access Service Edge (SASE), Secure Service Edge (SSE), Zero Trust Network Access (ZTNA) and Network-as-a-Service (NaaS).

- **SASE is a class of products that converge networking service brokering, identity service brokering and security as a service into one solution.** These tools make security for edge environments more effective by creating a single fabric for networking services with a single control point.

- **SSE can be considered a subset of SASE that focuses more on securely enabling end-user access.** It delivers stronger edge security capabilities to remote workers without getting too involved in network connectivity infrastructure. You can read more about the differences between SASE and SSE in this article in our blog. SSE secures access to the web, cloud services and private applications via access control, data security, threat protection and security monitoring features. It can also enforce acceptable-use control through network-based and API-based integration. In most instances, SSE delivers as a cloud service, but it can also include on-premises and agent-based components. It has emerged as one of the best ways to protect remote workers from cyber threats and malicious attacks by governing their access control and monitoring for unusual activity.

- **ZTNA is more of a security philosophy or approach rather than being a specific technology.** It seeks to institute a comprehensive and flexible trust model that eliminates the principle of implicit trust from inside and outside of the network perimeter. Rather than trusting a device or user based purely on password entry, it demands additional proof to verify the person or device is genuine and has not been compromised. Multi-factor Authentication (MFA), biometrics and other technologies fall under the zero-trust umbrella. Individuals are not automatically trusted just because they are on the network. They must prove who they are and then given limited access to only the systems they need. SSE tools and servicing now incorporate large portions of the ZTNA market, according to Gartner.

- **NaaS is a way to deliver networking services such as SSE, SASE, ZTNA and others via the cloud with the heavy lifting done by a service provider instead of being retained in-house.** This can become an optimal solution for IT teams that must cover their security bases but don't have the internal resources to support the need.

SSE is seen by many as the best way to secure remote endpoints without becoming embroiled in networking and security complexity. According to Cybersecurity Insiders, 67% of organizations plan to start their SASE strategy with a Security Service Edge platform. 65% want to adopt SSE within the next 24 months. 47% plan to begin SSE implementation with ZTNA deployment and 48% say their primary SSE use case is securing access for remote and hybrid employees. They view SSE as the solution to excessive user privilege whereby too many users have access to mission-critical systems and even administrative permissions, placing the organization at risk.

If comprehensive security and risk management is a priority for your organization to protect your data and your brand, Verinext has the expertise and solutions you need. We can help you elevate your security posture with the layered approach you require from the datacenter to the edge. We are the experts in SSE, and NaaS, to fortify your business against security risk, preventing devastating loss of capital, brand equity and customers so you can operate with confidence.

Learn About Verinext Security Solutions

verinext.com/solutions/security