CyberEd.io

iSMG INFORMATION SECURITY MEDIA GROUP

Zero Trust Network Access

Written by Dr. Chase Cunningham, Steve King & John Kindervag

Zero Trust Network Access

Our colleague, Dr. Chase Cunningham, the widely acknowledged Doctor of Zero Trust, and current Chief Strategy Officer (CSO) at Ericom Software, has put together a lecture focusing on the origins and history of remote network access, VPNs and the evolution through design and architectural improvements, and finally, to the Zero Trust approach to remote network access, or ZTNA. It will be available on CyberE.io in February after our January launch.

Chase worked with John Kindervag at Forrester Research as a Vice President Principal Analyst where he tracked and covered all aspects of enterprise security, Zero Trust trends, technologies, and frameworks.

While working with John at Forrester, Chase created the Zero Trust eXtended framework, developed their Zero Trust portfolio of accounts and provided strategic guidance on Zero Trust, artificial intelligence, machine learning and security architecture design for security leaders worldwide. Working in various capacities supporting NSA, US Navy, FBI Cyber, and other government mission groups, Chase is a deeply experienced Cybersecurity analyst and we are lucky to have him as a Senior Fellow on our CyberTheory Institute's board.

Back in October, Chase posted an article on LinkedIn that I have included in this post as a way to continue applying market pressure to adopt ZTNA solutions over traditional VPNs.

ZTNA Compared to VPNs

John Kindervag, Dr. Cunningham and I have worked together for over two years combatting the negative media coverage around Zero Trust and offering the organically correct version of Zero Trust to anyone and everyone who will listen. We even created the CyberTheory Institute Decision Council on Zero Trust and surrounded ourselves with an extraordinary team of Zero Trust advocates and senior practitioners who have earned unequivocal credentials in the space through careers that validate their proficiency in Cybersecurity.

We conduct in-depth dinner meetings with extensive discussions around Zero Trust best practices in settings as varied as Mainframes and Operational Technology ICS Networks, with contributions from our senior fellows and thought leaders. We are adamantly pro-Zero Trust and continue to believe that the adoption of a Zero Trust strategy will reduce excessive trust from our networks and lower the incidents of breach from the levels that they enjoy today.

John Kindervag says that “ZTNA is a secure VPN with a Kipling Method Policy statement.” John is correct, but Dr. Cunningham’s view is a tad more expansive and might help folks struggling with nomenclature and technical assumptions to get a clearer picture of what ZTNA is and why it is likely to be of benefit to the enterprise.

Dr. Cunningham’s view: I have nothing against VPNs in general, when after you set aside their implementation quirks, security porosity and latency, they seem fine. In fact, back in 1996, it was applauded as a revolutionary approach to establishing a virtual point-to-point connection through dedicated circuits or tunneling protocols over existing networks. ZTNA however, is so much better, it is hard to warrant much debate. But, here goes, nonetheless.

As we read the cyber news and the Zero Trust market analysis that is published everywhere, we note that there seem to be some misconceptions about the value proposition of a strategy like Zero Trust. We see many posts and analyses talking almost exclusively about the specific technical benefits of a Zero Trust strategic approach. This makes sense because technology helps us achieve the end state we are working to reach, but technology is the "how"; it is not the "why" for Zero Trust.

The "why" for a Zero Trust approach and deciding on the technology that an organization might choose is ultimately about business outcomes, not just technical outcomes.

Traditionally, organizations focused on protecting network access with technologies such as on-premise firewalls and virtual private networks (VPN). Remote users gain access to business networks and resources by logging into a VPN, creating a secure virtual tunnel into the networks. However, problems arise when VPN login credentials fall into the wrong hands or a security risk originates within the organization.

As enterprises now need to support secure remote access at scale, the risks associated with VPN use only surge.

ZTNA Emerges

In the wake of the digital revolution and remote-work policies in response to the pandemic, the number of employees and systems outside the conventional IT perimeter has grown exponentially. Cybercriminals are exploiting this opportunity by blending in with the growing volume of data traffic and launching more sophisticated attacks.

The Zero Trust security model is designed from the ground up to prevent and mitigate the damage of such data breaches by necessitating even authorized users, devices and systems to prove they are authorized before gaining any access. Through microsegmentation, it empowers IT teams to arrange resources in discrete zones, containing potential attacks and preventing them from spreading laterally throughout the network. Sensitive data and information are secured through the use of granular, role-based access policies.

The expansion of the data footprint is also a factor that necessitates Zero Trust. The castle-and-moat model was designed for a time when an organization's resources resided locally on-premise. But today, most enterprises' resources lie scattered across multiple cloud platforms and data centers, diffusing the traditional perimeter. We no longer have data lakes. We now have data oceans. The legacy approach to cybersecurity has become ineffective in these hybrid cloud environments.

Costs Are Skyrocketing

According to an IBM breach report, the cost of the response and fallout of a breach is up by about 10% year over year. But there is another not so well noted "cost" of a breach that seems to slide by most market posts, that is, the cost of that response, and the after-action costs that get passed on to the breached companies' consumers. These costs average to about a 60% increase in the prices of goods and services. Why does that matter? Customers don't like to think that they are the ones who are paying for a company's failure to secure their systems.

Research shows that up to 30% of customers in the retail, finance and healthcare industries will stop doing business with companies that have been breached. And similar research shows that 85% of customers will tell others about their experience, damaging the brand value and positioning of a breached organization. Lastly, roughly 34% of customers will vent their feelings about their experience on social media.

The Ponemon Institute's Cost of a Data Breach Report states that lost business was the greatest expense associated with a data breach. This accounts for nearly 40% of the cost of a data breach attributed directly to customer attrition. In addition, the added cost of acquiring new customers due to diminished reputation contribute significantly to increased customer turnover. A breached business suffers across the board and history tells us 95% of all breaches can be avoided. Replacing VPN systems with a Zero Trust Network Access solution is a great first step to eliminate that threat.

In spite of threat and breach data that offers evidence of this very real danger on a daily basis, most companies still under-utilize best security practices and under-spend on proven technology solutions. Most companies insist that cybersecurity is unaffordable, and cling to the notion that it won't happen to them. Others who do spend on Cybersecurity, do so in a traditional layered defense model adding incremental protection as new threats surface.

In any other market, would a company continue to engage in failed business practices if thousands of evidentiary-based proofs argues that the current practice has categorically failed?

Doing What We've Always Done Will Not Change The Outcome

Most of us work in some form of market-related work, we sell things. What would any organization do if they looked across the market in which they sell and saw that the dominant approach to sales was failing writ large? They would change their approach, or the business would fail just like the others. Security is no different from any other market. If we ignore the realities of space and think that we are somehow different even if we are doing the same thing that others who failed did, then aren't we delusional? This is pretty simple, choose to take a different approach or expect the same outcome.

Are there technologies that can help us get to the desired end state faster? Absolutely. Just as with any other market space some technologies can help us reach an end state if we use them intelligently and in line with our overarching strategic goals. Much like accounting software has revolutionized small business operations, or Salesforce has changed the game globally by streamlining the sales process, a few key technologies are critical to a successful Zero Trust strategy.

The Zero Trust strategy requires an organization to continuously verify an entity's identity and treat all access requests as if they originate from a compromised, unprotected network. To do this a few things must technically happen.

The technologies employed must be able to do the following four things at a minimum:

1. Continuously validate access and requests to resources: there must be an ability to process authorization dynamically rather than access being solely based on a singular input from a policy engine. Those requests must be reliant on a time horizon. In other words, there is no unfettered access, and there is no access without a dynamic set of criteria being met before any asset is made available.

2. Least-privileged access: access is restricted based on identity and a variety of telemetry that powers contextual decision-making for the policy engine. The technology does not take any single input and then allows access. Multiple steps are necessary for access to be granted and intelligent telemetry is leveraged across requests in real time.

3. Network level vs Application level access: VPNs use network level access and take a blanket approach to that network. Once authenticated, fraudulent or not, that access is provided to "all" resources that might be available to that user. Additionally the privilege level of many VPN's is excessively powerful and introduces risk for an infrastructure. ZTNA, on the other hand, adopts the opposite approach, providing no access unless an asset – an application, data, or service – is expressly permitted for that user. Anything not specific to the policy is invalid and outside of the bounds of acceptable use.

4. Device Assessment: Employees in today's workforce regularly utilize personal laptops and other devices to work, it's a BYOD world. Therefore, ZTNA's device verification checking capability is crucial for a cybersecurity strategy to be optimal. A business should be able to verify that a device has the correct protections in place and that the device's patch level is up to date before access is granted. This helps manage BYOD and often can help secure a user's home or personal device.

ZTNA Benefits

There are five key benefits of the ZTNA approach to a Zero Trust strategy. They are:

1 Micro-segmentation: ZTNA enables companies to build a fully micro-segmented infrastructure while using virtualization optimally. This helps to limit attackers from moving laterally and decreasing the attack surface in the event of a breach. Compromise is going to happen, but by limiting the spread of the infection, you're able to manage damages within a narrowly defined surface area.

2 Protect against malicious insiders: A Zero Trust-driven security strategy powered in part by ZTNA limits the damage of malicious employees thanks to the least privilege concept and the enhanced visibility of users and their actions. Least privileged access, dense authentication requirements and intelligent telemetry make it easier to find indications of compromise originated by insiders, and/or infected machines that are potentially seeking assets that they should not be able to access.

3 Dark assets: Creates the ability to hide applications and assets. ZTNA helps an organization to deploy hidden or "dark" assets. Essentially this means that app discovery is not possible for non-authenticated users and machines. And this helps to limit an adversary's ability to discover additional targets when a breach does occur.

4 Supports trending work models: Hybrid work arrangements are the generally desired approach to work today. Businesses that have accommodated work from home models of multiple varieties can rely on ZTNA for improved security, increased speed and fewer vulnerabilities than traditional VPNs, to provide a seamless and safe computing infrastructure for its remote workforce.

5 Enabling compliance requirements: Thanks to the ZTNA architecture, corporate compliance requirements surrounding authorization and tracking for access to applications and data are automatically satisfied. Logging and the "need" for access is also enhanced and can help vector compliance operations. In other words, you are only compliant for what you must be compliant for. Not compliant for "everything".

More to Come

We will add more to this series of Zero Trust related discussions, but we think that the benefits are pretty clear. Yes, there is a lot of marketing in the space. That's how markets grow. Yes, there are many vendors claiming Zero Trust. Many of them aren't "wrong" as you could build a Zero Trust system with a wide variety of technologies.

But, representing a technology that is an enabler of one or two Zero Trust principles, without context and claiming that the solution qualifies or validates as an approach to Zero Trust is deceitful and contributes to the confusion.

It's critical that we share the basics, the four principles and the five steps to implement and the Kipling Method for Zero Trust policy so that folks can understand which capabilities are simple and directly beneficial and which ones are not.

We hope folks who read this find it educational, honest and useful as they consider embarking on a Zero Trust journey of their own.

About CyberEd

CyberEd.io is a comprehensive platform for developing cyber warriors, upskilling cyber professionals, and training executives, with cybersecurity education for all.

About ISMG

Information Security Media Group (ISMG) is an intelligence and education firm focused exclusively on cybersecurity.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io