OPINION

The Zero-Trust Mandate: Never Trust, Continually Verify.

Etay Bogner, VP, Zero-Trust Products, Proofpoint.

The traditional network security model was designed to connect workers at headquarters or a branch office to the resources they needed in data centers. At that time, there were relatively few remote workers and they connected back into their home network using an operationally complex VPN.

Today, most employees work remotely at least one day a week and virtually all organizations also make use of multiple public cloud services. Those factors combined with the security vulnerabilities associated with VPNs means that the traditional model is no longer effective.

This potential attack vector can be mitigated by an expanded model in which the right of a user to access resources is continuously verified – ideally at the packet level.

The End of Trust

A critical defect in the use of VPNs for remote access is that once users are authenticated, they are considered trusted and are granted broad access. As a result, once a hacker penetrates an organization's firewall, he/she can move through the network with little if any resistance.

Back in 2010, John Kindervag, formerly with Forrester, created the zero-trust security model and in a recent article he discussed how trust is a human emotion and added that "It has no purpose in digital systems, such as networks. There is no use for 'trust' in these systems, except to be used by malicious actors, who exploit 'trust' for their own nefarious gain. The only thing that can happen to trust in a digital system is for it be exploited, and the only outcome for trust is some type of betrayal."

The zero-trust security model is based on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify everything trying to connect to its systems before granting access. In a zero-trust model, users have a unique, fixed identity and one-to-one connections between a user and the resources that he/she needs to access. A key advantage of this model is that a compromise to one asset does not compromise the entire company.

Taking Zero-Trust to the Next Level

One weakness in the original zero trust security model was that the connections that were established between a user and network resources and could last for an extended period of time. This potential attack vector can be mitigated by an expanded model in which the right of a user to access resources is continuously verified – ideally at the packet level.

In addition to continuous verification, an effective zero trust model must support next generation access. As explained by Chase Cunningham in a recent Forrester blog, next generation access encompasses a range of functionality including single sign-on, multifactor authentication and correlation between access and users; i.e., who is doing what, where, and why?

Moving to a Zero Trust Network-as-a-Service (NaaS)

The best way to address the systemic flaws in the traditional network security model is to replace that site-centric approach with an identity-based approach that includes both dynamic, per-user network segmentation and continuous authentication. A cloud-native NaaS is built around a zero-trust architecture in which each user has a unique, fixed identity and is bound by a software-defined perimeter (SDP). The SDP framework enables one-to-one network connections that are dynamically created on demand between the user and the specific resources that he/she needs to access – everything else on the NaaS is invisible to the user. No access is possible unless it is explicitly granted and any access that is granted is continually verified at the packet level.

Once data centers, clouds, and branches are onboarded to the NaaS, policies define what is visible to authenticated users.

Turning Theory into Practice

A zero-trust security model is critical in the age of digital transformation. In contrast to the old "trust but verify" approach, the new way of thinking is based on never trust, continually verify, as well as minimizing access to a company's resources with dynamic micro-segmentation.

Given the growth in the sophistication and impact of security attacks, IT organizations must move quickly to adopt the new security model. Many will find that the optimum place to start is where the current security model has the greatest weaknesses – remote access – and look into replacing VPNs with a zero-trust Software-Defined Perimeter.

About the Author: *Etay Bogner is the VP of Zero Trust Products for Proofpoint and focused on helping organizations rapidly provide secure remote access for employees, contractors and partners to corporate applications and the internet. To learn more, download a detailed whitepaper on the subject.*

www.proofpoint.com

Four Questions Organisations Need to Ask after a Cyber Attack.

Cyber attacks are inevitable, but it's how an organisation deals with them that can make or break their business. Have they got all the answers, and do they fully understand the implications? Can they be sure the attack won't happen again?

Swift and comprehensive incident response is a critical step to ensuring the future security of a business and protecting its reputation. It's not enough to be aware that an attack is taking (or has taken) place. There are four key questions organisations need to be able to answer following a cyber security breach – if a single answer is missing, the security team won't have the full picture, leaving the business vulnerable to impending attacks. Not having this level of insight can also damage an organisation's relationships with suppliers and affect customer confidence, as it means the business itself is not in control of the situation.

Andy Pearch, Head of IA Services at CORVID, outlines four questions all organisations must be able to answer after a cyber attack.

1. How and where did the security breach take place?

The first step of an effective incident response strategy is to identify how the attackers got in. Quite simply, if an organisation misses this first crucial step, attackers will exploit the same vulnerability for future cyber attacks. Guesswork won't cut it – any security professional can hypothesise that "it was probably an email", but security teams need clear evidence so they can fully analyse all aspects of the problem and devise an appropriate solution.

2. What information was accessed?

Understanding specifically what information was accessed by the attacker is paramount to knowing what impact the attack will have on the organisation. Identifying which departments were targeted or what types of information might have been stolen isn't good enough; organisations need to be able to articulate exactly which files were accessed and when. Headlines about attackers stealing information are common, but just as importantly, you need to know the scope of the information they've seen, as well as the information they've taken. Not only will this inform the next steps that need to be taken, and shed light on which parts of the business will be affected, but it will also enable the organisation to remain compliant with legal obligations, for example, identifying if a data breach needs to be reported under GDPR.

3. How can systems be recovered quickly?

Organisations will understandably want to get their IT estate back to normal as soon as possible to minimise damage to their business, service and reputation. If the compromise method is identified and analysed correctly, IT systems can be remediated in seconds, meaning users and business operations can continue without downtime for recovery.

4. How do you prevent it from happening again?

Knowing the IT estate has been compromised is useless without taking steps to make sure it doesn't happen again. Managed Detection and Response (MDR) is all about spotting the unusual activity that indicates a potential breach. If a user is accessing files they would never usually touch, sending unexpected emails or reaching out to a new domain, for example, such activity should prompt a review. The problem for most companies, however, is they lack not only the tools to enable such detection, but also the time and skills to undertake thorough analysis to determine whether it is a breach or a false positive.

A managed approach not only takes the burden away from businesses, but also enables every company to benefit from the pool of knowledge built up as a result of detecting and remediating attacks on businesses across the board. With MDR, every incident detected is investigated and, if it's a breach, managed. That means shutting down the attack's communication channel to prevent the adversary communicating with the compromised host, and identifying any compromised asset which can then be remediated.

Shifting security thinking.

Clearly, GDPR has raised awareness that the risks associated with a cyber attack are not only financial, as hackers are actively seeking to access information. Security plans, therefore, must also consider data confidentiality, integrity and availability. But it is also essential to accept the fundamental shift in security thinking – protection is not a viable option given today's threat landscape. When hackers are using the same tactics and tools as bona fide users, rapid detection and remediation must be the priority.

www.corvid.co.uk