ZERO TRUST: THE EVOLUTION OF NETWORK SECURITY

Gemserv

Cyber & Digital

THE EVOLUTION OF NETWORK SECURITY

DEFENCE IN DEPTH

Due to a steep rise in the adoption of cloud technologies, remote user access, multiple devices connecting to a network and many more advancements, network architecture is changing. The traditional architecture of networks with a perimeter is virtually undetectable in many organisations today. The perimeter has expanded and often cannot be defined.

At the same time, the volume of malicious actors and threat vectors have increased significantly, they are incredibly creative and are continuously looking for vulnerabilities within protective solutions. No protective defence tool or approach can 100% guarantee protection.

Best practice has long been defence in depth; implementing complimentary and overlapping controls such that if one fails, another may still prove effective. While this is still hugely important, it needs to be backed up by a methodology which assumes any cybersecurity protection operates in a hostile environment – a zero trust approach.

PERIMETER AS A DEFENCE

Perimeter as a defence is the principle of utilising protective devices on the boundary of your network. A couple of commonly utilised perimeter protective devices are firewalls and antivirus software. A firewall is a device that will allow or block traffic in and out of your network based on the configuration rules applied by the administrator. Antivirus software scans and analyses incoming traffic based on sets of characteristics to identify and block malicious traffic. For a long time, these types of defences were effective in most cases and able to protect most malicious traffic that might attempt to penetrate your network.

The ability of a firewall to protect your network is dependent on proper configuration – the rules that are applied need to be relevant to your organisation and potential threat vectors. The effectiveness of perimeter endpoint protection software is limited to known threats and behaviours and a defined perimeter. Malicious actors are more advanced, creative and familiar with perimeter defence technologies. They are increasingly identifying and exploiting vulnerabilities. Ransomware families have grown by more than 700%[1], and as a result, malicious actors are consistently gaining access and enjoying unhindered lateral movement in networks.

1 Protect Your Organization From Cyber and Ransomware Attacks – https://www.gartner.com/

IDENTITY AS A DEFENCE

Due to the uptick in the working from home policy, which has become a necessity with the COVID-19 pandemic, many organisations have embraced global remote access for their employees and multiple devices connecting to their enterprise network. As perimeters were being increasingly breached, security experts looked for a way to reinforce security and access to a network. Identity and Access Management (IAM) is a principle that aims to authenticate and authorise user access to a network and to assets within the network.

A strong IAM policy and implementation goes a long way to further protecting a network. However yet again, malicious actors found ways to circumvent best practices. These include obtaining authorised credentials via social engineering (phishing, vishing, smishing) schemes and other means and hence can bypass firewall rules and gain authenticated access to the entire network. This causes breaches – from 662 million in 2010 to over 1000 million in 2020 in the US[2]; 46% of businesses and 26% of charities in the UK suffered a breach in 2020[3], breaches can go undetected for a long time, whilst they proliferate confidential data[4].

2 Cyber crime: number of breaches and records exposed 2005-2020 – https://www.statista.com/statistics
3 Official Statistics Cyber Security Breaches Survey 2020 – https://www.gov.uk/government/statistics
4 How to Respond to a Supply Chain Attack – https://www.gartner.com

ZERO TRUST

The zero trust principle was created by John Kindervag, a VP and principal analyst for Forrester Research at the time. It is based on his realisation that traditional security models operate on the outdated assumption that everything inside an organisation's network should be trusted[5]. In order to prevent security breaches and limit their impact, this principle adopts a "never trust, always verify" approach.

The following are the foundations of zero trust architecture design[6]:

1. **Know your architecture** including users, devices, services and data.
2. **Know your user, service and device identities.** It is important to have a single source of identity for each of the following: user (human), service (machine or software process) and device.
3. **Know the health of your users, devices and services.** Knowing where your users are accessing services from and how (and if that changes, why), plus service and device health – including compliance with configuration policies and the zero-trust principle.
4. **Use policies to authorise requests.** Every request to access a data or a service should be checked by a central policy engine, which compares signals with access policies to determine an access decision.
5. **Authenticate and authorise everywhere.** Assume the network is hostile and authenticate and authorise all connections that access data or services. Authentication controls such as Multi Factor Authentication are a requirement along with Single Sign On, to improve usability for users. Requests between services can be authenticated with Key Management Systems.
6. **Focus your monitoring on devices and services.** Given that devices and services are more exposed to network attack than in traditional architectures, it's important that comprehensive monitoring for attacks are carried out.
7. **Don't trust any network, including your own.** The network is considered hostile, therefore build trust into users, devices and services rather than the network.
8. **Choose services designed for zero trust.** Select services with built-in support for zero trust network architectures.

These principles remove trust from the network and adopt the approach that any network, regardless of the protective tools and policies applied, can be breached. There is no perimeter, no trusted software and anyone accessing the network from anywhere could be a malicious attacker and thus aims to implement additional verification and validation before access is granted.

5 What is a Zero Trust Architecture – https://www.paloaltonetworks.com
6 Zero trust architecture design principles – https://github.com

WHAT DOES THIS MEAN FOR CLOUD SECURITY TEAMS?

The Public Cloud Shared Responsibility Model means that cloud providers are responsible for the provision, security and availability of the cloud infrastructure (data centre hardware that runs computer, storage, database and networking), but customers are responsible for the security in the cloud, including their network security configuration.

As cloud adoption continues to accelerate for all types of enterprises within various industries, cloud security teams should look to adopt zero-trust principles for their networks. Operate with an understanding that a breach occurring is not a case of "if" but "when". Advocate for a defence that is focused on users, assets and resources; redundancy and recovery plans; verifying explicitly; and progressively implementing security best practices that will help to limit the probability and impact of a breach. Security teams should take a zero trust, defence in depth approach: perimeter, identity and access management whilst proactively implementing anomaly detection, continuous monitoring and conducting network breach simulations.

BREACHES SHOULD BE PREPARED FOR AND UNDERSTOOD NOT AS A CASE OF 'IF' BUT 'WHEN'

Gemserv

MAKING THINGS THAT MATTER
WORK BETTER FOR EVERYONE

GEMSERV.COM

BD@GEMSERV.COM

+44 (0)20 7090 1022