precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume 6: Issue No. 1 February 2022

We took a brief look at some vulnerabilities in cybersecurity, one of those being unsecured networks. Today, we put networks under the microscope and see how we could make our connections secure and safer.

Dr. Ronald Walcott
Managing Director

While most organizations focus on securing the application traffic, few put sufficient infrastructure focus beyond point solutions such as firewalls. Security must be incorporated in all layers and the complete networking life cycle to protect the entire network.

SECURE NETWORKING LAYERS

Secure networking involves securing the application traffic as it traverses the network. It should encompass these areas:

- Perimeter security protects the network applications from outside attacks through firewall and intrusion detection technologies.
- Communications security provides data confidentiality, integrity, and nonrepudiation, typically using Secure Sockets Layer or IPsec virtual private networks (VPN).

Secure networking extends this by protecting the underlying infrastructure from attack.

- Platform security ensures that each device is available to perform its intended function and does not become the network's single point of failure. The network security plan should include antivirus checking and host-based intrusion detection, along with endpoint compliance, to ensure that security policies check user devices for required security software.
- Access security ensures that each user has access to only those network elements and applications required to perform his job.
- Physical security protects the network from physical harm or modification and underlines all security practices. The most prominent forms of physical security include locked doors and alarm systems.

SECURE NETWORKING LIFE CYCLE

Providing a secure network is not a one-time event but a life cycle that must be continually reviewed, updated, and communicated. There

In this Issue:

are three distinct stages to be considered:

- How can security breaches be prevented? Along with the hardening of operating systems and antivirus software, prevention includes regularly reviewing the network's security posture, which is particularly important as new convergence and mobility solutions, or recent technologies and platforms are added to the network.
- How can security breaches be detected? Detection techniques include product-level and networkwide intrusion-detection systems, system checks and logs for misconfigurations or other suspicious activity. Although some breaches are obvious, others are much more subtle.
- What is the appropriate response to a security breach? A range of preparations must be made to respond to a successful breach, some of which may include removing infected devices or large-scale disaster recovery.

STANDARDS FOR SECURE NETWORKING

1. Use a layered defence. Employ multiple complementary approaches to security enforcement at various points in the network, therefore removing single points of security failure.
2. Incorporate people and processes in network security planning. Employing effective processes, such as security policies, security awareness training and policy enforcement, makes your program more robust. Having the people who use the network (employees, partners and even customers) understand and adhere to these security policies.
3. Clearly define security zones and user roles. Use firewall, filter, and access control capabilities to enforce network access policies between these zones using the least privileged concept. Require strong passwords to prevent guessing and/or cracking machine attacks, as well as other vital forms of authentication.
4. Maintain the integrity of your network, servers, and clients. The operating system of every network device and element management system should be hardened against attack by disabling unused services. Patches should be applied as soon as they become available, and system software should be regularly tested for viruses, worms, and spyware.
5. Control device network admission through endpoint compliance. Account for all user device types -- wired and wireless. Do not forget devices such as smartphones and handhelds, which can store significant intellectual property and are more accessible for employees to misplace or have stolen.
6. Protect the network management information. Ensure that virtual LANs (VLAN) and other security mechanisms (IPsec, SNMPv3, SSH, TLS) are used to protect network devices and element management systems so only authorized personnel have access. Establish a backup process for device configurations and implement a change management process for tracking.
7. Protect user information. For security purposes, WLAN/Wi-Fi or Wireless Mesh communications should use VPNs or 802.11i with Temporal Key Integrity Protocol. VLANs should separate traffic between departments within the same network and separate regular users from guests.
8. Gain awareness of your network traffic, threats, and vulnerabilities for each security zone, presuming internal and external threats. Use anti-spoofing, bogon blocking and denial-of-service prevention capabilities at security zone perimeters to block invalid traffic.
9. Use security tools to protect from threats and guarantee the performance of critical applications. Ensure firewalls support new multimedia applications and protocols, including SIP and H.323.
10. Log, correlate and manage security and audit event information. Aggregate and standardize security event information to provide a high-level consolidated view of security events on your network. This allows correlation of distributed attacks and a networkwide awareness of security status and threat activity.

HEADLINE NEWS:
Increasing Adoption of Phishing Kits Puts MFA at Risk

Because of increased use of multi-factor authentication, attackers are developing phishing kits that steal tokens and bypass this trusted layer of security.

"Threat actors are using phish kits that leverage transparent reverse proxy, which enables them to man-in-the-middle (MitM) a browser session and steal credentials and session cookies in real-time," according to researchers at Proofpoint.

Jon Gaines, senior application security consultant at application security provider nVisium, says more threat actors are using phishing kits that allow some form of 2FA bypass.

"There are even some open-source options, such as EvilNginx2. Since that is available, the organization's blue team and outside red teams should be performing phishing campaigns at least annually to learn how to recognize and monitor this type of phishing. This works by forwarding the request to the proper service, such as Microsoft, and capturing the credentials before they are sent, and the session's cookies in the response. And yes, it is in real time," Gaines says.

PHISHING KITS

The Proofpoint researchers say that phishing kits are software developed to help threat actors harvest credentials and quickly capitalize on them.

"Often installed on a dedicated server owned by the threat actor or covertly installed on a compromised server owned by an unlucky individual, many of these kits can be purchased for less than a cup of coffee," the researchers say.

There are numerous MFA phishing kits, ranging from simple open-source kits with human readable code and no-frills functionality to sophisticated kits that use various layers of obfuscation and modules allowing stealing of usernames, passwords, MFA tokens, Social Security numbers and credit card numbers, the Proofpoint researchers say.

Researchers at Stony Brook University and Palo Alto Networks took a deep dive and released a paper on MitM phishing kits that identified more than 1,200 MitM phishing sites. In their research paper, they say that, of those 1,200-plus sites, only 43.7% of domains and 18.9% of IP addresses appeared on popular block lists such as VirusTotal.

Frequently Asked Questions:

WHAT IS A FIREWALL?

A firewall is a network security device that monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) to block malicious traffic like viruses and hackers.

WHAT IS A VPN?

A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address, so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

WHAT IS AN IP ADDRESS?

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Example: 192.168.1.1