SOPHOS

Eight Trends That Are Changing Network Security

By **James Lyne**, Director of Technology Strategy

Technology in the network security space has been through many dramatic changes recently. New mobile operating systems, growing use of personal devices, and SaaS (software-as-a-service) delivery make securing the network a growing challenge. Enhancements in the network infrastructure that connect devices within or across the network make all these developments possible. We're seeing ever faster network connections, more remote users, and extensive upgrades to mobile networks. We need to think about security policies and where and how to provide protection. Below are the eight trends we think will impact network security and your security strategy.

1. Mobile networks, VPNs and roaming users

Today's connect-from-anywhere road warriors regularly test the traditional boundaries of network security. Firewalls are increasingly porous as employees access services from devices such as iPads, Android phones, tablets and PCs—all of which require security that mirrors but also improves upon PC solutions. Extending connectivity to small branch or home offices is also a focus for many organizations. Your network strategy needs to consider how to secure access across platforms over an expanding network perimeter.

Consumerization and BYOD increase the importance of alignment between your various security layers.

2. Targeted attacks and APTs

APTs (or advanced persistent threats) represent the next generation of Internet crimeware. For years network security capabilities such as web filtering or IPS played a key part in identifying such attacks (mostly after the initial compromise). As attackers grow bolder and employ more evasive techniques, network security must integrate with other security services to detect attacks. We'll need to evolve security capabilities in response to these threats in the coming years.

3. Consumerization and BYOD

Consumerization and the BYOD (bring your own device) movement means consumer devices like iPads, iPhones and Android phones are moving onto the corporate network. To deal with consumerization, your security strategy needs to focus on network security for devices where an endpoint agent may not have been deployed, or may not be functioning properly.

For example, if a user connects with a Mac running malicious code, your network security layer should be able to identify that the device is attempting to retrieve malicious code updates or other suspicious activities—and be able to identify and remediate it. Otherwise you may not find out until you're already infected, and remediation can only happen after the fact. Consumerization and BYOD increase the importance of alignment between your various security layers.

4. Web application and web server protection

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cybercriminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Organizations used to focus security investment on PCs and preventing conventional malware from spreading to them and onto the network. Now, you need a greater emphasis on protecting web servers and web applications. Similar challenges lie ahead for emerging technologies such as HTML5. See our article HTML5 and Security on the New Web for more information on this trend.

5. IPv6: Major surgery for the Internet

IPv6 is the new Internet protocol replacing IPv4, long the backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Whether your organization adopts it later rather than sooner, make sure that IPv6 is on your network security agenda. For more on IPv6, check out our article Why Switch to IPv6.

6. Contending with cloud services

Small, medium and large enterprises are beginning to adopt cloud services and SaaS at a greater rate. This trend presents a big challenge for network security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve.

For example, which users should be able to interface with which services? Who should be able to post data, and who should have read-only privileges? While cloud services are developing their own security models, they will still need to be harmonized with your own strategy to avoid multiplication of password, permissions and other security infrastructure concerns. To be sure, the cloud represents a great opportunity. But as the cloud evolves, so too must network security.

As the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve.

7. More encryption

Encryption at every level protects the privacy and integrity of data. We're increasingly deploying encryption at every layer. However, more use of encryption will bring more challenges for network security devices. For example, how will your network DLP (data loss prevention) inspect traffic which is encrypted end-to-end as it accesses a certain cloud service? Collaboration between the network and the endpoint to deliver complete security in scenarios like this will be critical. You need to have a network security strategy that integrates your network security with other layers of security such as endpoint, web protection and mobile devices.

8. The elastic network

The network perimeter is expanding like an elastic to include high-speed 4G and LTE networks, wireless access points, branch offices, home offices, roaming users, cloud services, and third parties accessing your applications and data to perform services. These changes to the size, scope and surface of your network can lead to misconfiguration or change control errors that could lead to security breaches. You'll need security solutions you can consistently deploy at each device or point of infrastructure. And you need central management to keep on top of the dynamics of this elastic infrastructure and the various layers of security at each endpoint.

James Lyne, Director of Technology Strategy @jameslyne

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK