CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Analyzing Internet Traffic for Better Cyber Situational Awareness

Key Message: Automation, innovation, reaction, and expansion are the foundation for obtaining meaningful network traffic intelligence in today’s extended enterprise.

Executive Summary

Given the continued doubling of internet traffic volume and rate (with no end in sight) and the disappearance of defined enterprise network boundaries, business leaders are faced with the daunting challenge of having to understand the environment within which their critical services, applications, and systems operate. In today’s extended enterprise, many of these are being executed by service providers external to the organization. Such understanding includes anticipating the risks and potential impacts that leaders need to mitigate, even though they are not in control.

In this podcast, Derek Gabbard, Co-founder and Technology Director for Lookingglass, discusses how internet traffic monitoring, analysis, and visualization can help organizations develop better situational awareness to anticipate and defend against cyber attacks.

PART 1: HOW DO WE KNOW WHAT’S HAPPENING ON THE INTERNET?

The Internet’s Increasing Traffic Volume and Rate

Internet traffic is set to double every year [LG 2009a] for the foreseeable future, both in volume and rate. This is, in part, caused by:

- streaming video such as that offered by YouTube
- the movement toward cloud computing and other outsourced services
- organizations relying on the internet for an increasing number and type of business operations

Determining What Security Actions to Take

It is difficult to create, define, and execute a meaningful security posture when an organization cannot easily determine where its services and applications are being executed (such as when using cloud computing).

Requirements for network security, both internal and external, derive from:

- risk assessment and identification
- understanding your services and capabilities
- internet-based trends and issues such as traffic analysis, connectivity, peering relationships, and the impact of events beyond your borders
- moving beyond border-based perimeter considerations to include all networks that are involved in providing services

Becoming More Situationally Aware

Historically, organizations hosted their own services and applications, and had control over how they operated.

Today, components of operationally critical systems and services are being executed “in the cloud,” and are therefore out of the owning organization’s control.

Members of the Financial Services Information Sharing and Analysis Center indicate difficulties in understanding network traffic routing and topology for services that are hosted beyond their borders.

Other concerns include:

- the exponential increase in network traffic
- availability, including bandwidth capacity
- security

Situational awareness means having knowledge and an appreciation of:

- where and how applications and services are hosted
- connectivity between your networks and those of your service providers, your customers, your suppliers, and anyone else who needs to be connected
- the information supply chain – “these are the 20 organizations that need access”

Actions Based on Situational Awareness

Armed with this information, organizations can start to identify:

- key weaknesses
- critical connections between service providers
- the mapping of cyber assets to physical assets and locations
- potentially critical geographic regions
- service and system dependencies

Leaders can in turn begin to answer these questions:

- What is the nexus between physical infrastructure and cyber infrastructure?
- What is the nexus between required availability and services, and overall connectivity and geographic location?
- How are users going to access the services, applications, and systems that they need?

With this understanding, you can ensure that:

- you have the proper risk mitigation strategies in place
- you’re protecting the data that is in transit among services
- you know upon whom you are critically dependent for service continuity including your providers and your upstream providers’ upstream providers

This understanding is key to anticipating the risks and impacts that can result from cascading events such as connectivity issues between service providers.

PART 2: AUTOMATION THAT SCALES; INNOVATION THROUGH VISUALIZATION

Introducing Four Key Factors/Motivators for Achieving Situational Awareness

As detailed in [LG 2009a], these factors are defined by the acronym AIRE:

- A: Automation of network traffic analysis
- I: Innovation applied to analysis
- R: Reaction in real time, including possibly pre-reaction/anticipation
- E: Expansion to accommodate increasing network traffic

Lookingglass is positioning AIRE as the next security “device” that will eventually become ubiquitous, like firewalls are today.

AIRE is intended to provide meaningful results of network analysis that describe operational capabilities and help identify and manage risks.

Automation

Automation of the capture and analysis of network traffic and data flows is essential for dealing with the rate and volume of data.

Automation depends on the ability to build a backend data fusion capability that takes individual network traffic data sets and creates relationships among them. The supporting automation tools will provide a capability for significant and relatively quick ingestion of additional and new network data.

Automation approaches derive from how fusion is done manually by expert analysts and turning this expertise into an automated system process. The intent is to perform in several seconds what would take an individual analyst several weeks to complete.

This type of an approach can be scaled to handle increasing volumes and types of data.

Automation will support two perspectives:

- for knowledgeable network analysts to conduct detailed analysis
- for presentations to senior management; a red, yellow, green stoplight approach

Innovation

Innovation primarily centers on visualization and presentation. Good progress is being made using correlation engines to aggregate vast amounts of data into individual, presentable events.

There have also been advances in the amount of data that packet capture and network forensic devices can handle at one time.

What is needed is a breakthrough in tools for meaningful visual representation of information that can be acted upon by different levels of users.

Tools built for enterprise-level network analyses are insufficient when attempting to address network traffic at the levels experienced by the US Department of Homeland Security's US-CERT or Einstein data from over 100 different agencies.

PART 3: REAL-TIME REACTION; EXPANDING TO TRACK NEW ATTACKS

Reaction

Given timely data collection and analysis, and innovative approaches for data visualization and presentation, the next logical step is being able to react in real time (or close to real time).

There are generally two reasons to collect data:

- To gain a historical perspective and support forensic analysis. This type of detailed data analysis is not as time sensitive or time critical.
- Being able to quickly and accurately identify where an analyst needs to pay immediate attention.

Expansion

In the struggle between attackers and defenders, defenders are typically playing catch up. Expansion is about becoming more forward looking and getting better at anticipating what the next attack vector might be.

Attack methods and patterns that serve as today’s baseline will be obsolete in five years, likely not even in the picture

Modularity in support of automation, visualization, and expandability is key. You also need to take size, speed, and scale into account.

Examples include being able to easily address upcoming changes in the core routing protocols of the internet such as secure BGP (Border Gateway Protocol) and secure DNS (Domain Name System). AIRE approaches need to be developed with these types of changes in mind.

Staying in touch with the attacker communities and what they are discussing is useful for all security analysts.

Resources

[LG 2009a] Network Analysis 2.0: Staying Ahead of the Threat Curve with AIRE, Lookingglass, 2009.

The Cyber Intelligence Mecca: Ten Rules for Achieving Cyber Situational Awareness, Lookingglass, 2009.

Lewis, Jason & Gabbard, Derek. Network Topology Discovery and Exploitation, Lookingglass, 2009.

BlackHat conferences and community

DEFCON conferences and community

CERT's Network Situational Awareness website

CERT's Network Situational Awareness open source tools

CERT's FloCon Conference (includes past conference proceedings)