Politics of Security Webcast Summary
Cyber Threat News and APT Defenses

Introduction

Stories about cyber espionage and Advanced Persistent Threats (APTs) are part of the mainstream news cycle. Concerns about China's cyber espionage activities dominate public policy as well as business news.

The escalating visibility of the threat environment is putting CISOs on the hot seat. Security organizations have to respond to the advanced threat environment in two ways: addressing to the growing concerns of senior leadership and shareholders, and strengthening defenses against advanced and evolving threats.

As part of its ongoing **Politics of Security** webcast series, Tenable Network Security assembled a panel of past and present CISOs to discuss the unique challenges of handling today's increased press coverage and threat levels.

The panelists were:

- Chris Lockery, Director of Cyber Security and Threat Management at **Cigna**
- Mike Towers, VP, Information Security Assurance at **GlaxoSmithKline**
- John South, CSO at **Heartland Payment Systems**
- Vas Rajan, CISO at the **CLS Group**
- Craig Shumard, CISO for **CIGNA** 1999-2010, currently consulting

Key Take-Aways

- When a new threat hits the major news outlets, manage the conversation with senior leadership using a fact- and risk-based approach. Avoid playing on fear and uncertainty; translate the risks into terms relevant to your business, and educate people about what you're already doing.

- To address the changing threat environment, supplement traditional security measures with new approaches that focus on coverage, data and behavior.

- Share threat information with others in your industry and beyond.

Classifying the Types of Threats

The term Advanced Persistent Threat (APT) is used imprecisely. Panelists suggest focusing less on the threat tactic or vector and more on the *perpetrator* (who is instigating the threat) and *business risk* (what are they after).

- *Cyber espionage* refers to industrial or government spying, often perpetuated or sponsored by nation-states, is the source of many of today's headlines. Intellectual property is at risk.
- *Cybercrime* is malicious activity undertaken by criminals seeking financial gain, and usually targets personal data (identity information) or financial data.
- *Cyber hacktivism* refers to malicious or destructive online activities undertaken by people with a public agenda, such as Anonymous. Reputation is at risk.
- *Cyber warfare* is the extreme case of nation-state cyber threats. These threats may target weapons systems and infrastructure.

The relative prominence of these different threats will vary by industry. For example, the financial sector focuses heavily on cybercrime, but is also alert to hacktivism. By agreeing on terminology and understanding the nuances between what is targeted, you can better assess the actual risk to your business.

Addressing the News

Each major news story about cyber threats raises anxiety levels at the C-level and on the board. The CISO and security organization is responsible for determining the real threat level, understanding how it changes the risk exposure of the organization, and communicating this to senior leadership.

- Be prepared for questions and ready to respond. Stay on top of the latest intelligence and have write-ups and analysis ready proactively.

- Translate the threat in the news into relevant terms for your business. If you already have preventative measures and programs in place to address those threats, explain what you're already doing and what the real risk exposure is.

- Don't squander the opportunity to engage senior leadership in meaningful discussion. The new visibility can be a positive opportunity to let high-level leadership know what programs you have in place, and to get sponsorship or budget for gaps you need to fill.

Quote: "Our incident response team calls itself the 'article response team.' When news hits the major news outlets, it's the first thing the executives read in the morning. We have plans and write-ups ready so we can stay in front of questions." - Chris Lockery

Addressing Advanced Threats

Advanced threats are designed to find their way around traditional security measures. For example, many advanced threats used compromised credentials to gain insider access. Attackers may cover their tracks. And you cannot find zero-day attacks using signature-based technologies.

Traditional security measures still have a critical role to play, but CISOs need new approaches and preventative measures to manage the risk exposure in today's advanced threat environment.

Quote “Digital fortifications around data and systems are overrun or circumvented by techniques like APT and DDOS attacks. APTs use sophisticated intelligence gathering, and we’ve expanded our risk profile with social media, mobile and cloud activity. In addition to traditional security measures, we need new approaches to limit our exposure.” – Craig Shumard

Focus on coverage instead of capabilities. Security organizations used to focus on having the best tools and capabilities (firewalls, IPS, tools). Today it’s important to focus on coverage, and invest in the tools, techniques and policies that address gaps in coverage.

U**se continuous monitoring and vulnerability assessment**. Looking at networks, desktops or organizations with a point-in-time snapshot doesn’t work well as the players get more sophisticated. Continuous monitoring helps you to identify quickly when systems may be compromised, and to spot those zero-day exploits as they happen.

Share information. The panelists look beyond their own organizations to partners, industry communities and government agencies (Homeland Security) to augment their own threat intelligence. In the financial industry, the Financial Services Information Sharing and Analysis Center (ISAC) generates a tremendous amount of raw intelligence every day. Even in the pharmaceutical industry, which used to view information security as a competitive advantage, businesses are collaborating regularly to share information on threats.

Quote “By working with others in our industry through the Financial Services ISAC, we have access to a vast amount more data than we could ever accumulate as one company.” - John South

Test web applications. Perform security, vulnerability and penetration testing on web applications. For example, the SQL Injection attack is over ten years old, but a November 2012 study showed that over a million websites are still vulnerable.

Shift how you think about endpoints. With today’s BYOD workplace and cloud-based applications, IT has to protect the user experience on endpoints outside of IT’s control. Look at other techniques for protecting data, such as device reputation and device ID techniques that can detect Man-in-the-Browser and Man-in-the-Middle attacks.

Quote “We are approaching a time of ‘stateless IT’ in which data can live almost anywhere. We have to shift our thinking from protecting endpoints themselves to protecting the user experience on endpoints that may be beyond our control.” - Vas Rajan

Control the insider threat. Many external attacks are able to compromise valid internal credentials to gain access to system and data. APTs often find a way to compromise trusted insider accounts. Traditional, predictive behavior-based modeling and Data Loss Prevention (DLP) techniques still have an important role to play in defending against the insider threat.

Quote: “You cannot stop a motivated attacker from taking data, but you can better control who has access to data – and the business owns the data.” Mike Towers

Assume you will be compromised. Work from the assumption that you have already been compromised. This helps you understand what you need to protect and how to protect it. For example, encrypt data at rest and in motion, making it more difficult for someone to gain access. Rather than relying on a specific technology, look at the entire ecosystem and fill gaps.

Questions and Answers

The panelists also answered questions from the webinar audience, summarized below.

How do you deal with security controls (or lack of security controls) for data in cloud-based services?
Work with the Procurement team through the selection process to make sure that information security is a core component of due diligence and factored into contracts. Also, maintain an ongoing governance relationship with the cloud provider, so you can see what's happening with your data no matter where it resides.

Do you foresee attacks starting to target the hypervisor?
There have already been notable attacks on hypervisors. As virtualization becomes more widespread in the data center, we will see more attacks targeting that layer. Future workstations may have many profiles (for work, home, gaming, etc.) Attackers will look for ways to compromise the hypervisor to get to where data resides in virtual systems.

Since many of the APT threats involve insider access, is it enough to focus on managing insider threats?
External threats may take advantage of internal collaborators or compromise inside identities, but it does not follow that you can ignore the outside threats. When one avenue is closed to attackers, they will fill the void.

Summary

To listen to the full discussion or access past sessions of the Politics of Security webcasts, visit www.tenable.com/webcasts. Additional webinars in this series include:

- The Politics of Stakeholders in the CISO World
- The Politics of Risk Tolerance
- The CISO Job: Getting It and Keeping It (2 parts)

You can find more white papers, videos and webinars in the Resources section at www.tenable.com

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are used by many Global 2000 organizations and

government agencies to proactively minimize network risk. For more information, please visit www.tenable.com.