Nige the Security Guy

Bringing Together a Virtual Community of Security Thought Leaders

APT Strategy Series

November 8, 2013

www.secureadvisor.com

APT Strategy Series

There is a wealth of news and noise with regard to advanced threats, also known as persistent targeted threats and, marketed as the Advanced Persistent Threat (APT). The APT Strategy Series of blogs aims to try to cut through the hype and provide practical steps to our readers to help mitigate the threat.

There is a lot of hype and yet there is no silver bullet. However there is much an organization can do to extend their defense-in-depth strategy, to improve their detection and containment capability and, to gain key visibility to rapidly respond to a compromise or attempt. There is also a win-win in that many best-practices, controls and, detection techniques needed for APT also help address the Insider Threat.

The APT Strategy Series covers, as follows:

- **APT Architecture & Strategy**: Architecture and Design principles that help address APT and Insider Threats
- **APT-Focused Best-Practices**: Practical steps to improve security posture and reduce threat/risk
- **APT Detection Framework**: A framework to enable organization and analysis of attack and detection methods
- **APT Detection Indicators**: Practical steps, methodology and tools to gain key visibility and identify a potential compromise

Strategic Defensible Security Posture

The **Advanced Threat Defense** series of blogs takes a top-down approach for those organizations who have the opportunity to address their security architecture and design to create a Defensible Security Posture, enabling the ability to seamlessly Detect, Contain, Respond, Eradicate, Recover.

In this series we have currently published, as follows:

- Defensible Security Posture
- Advanced Threat Defense – Part 1
- Adaptive Zone Defense – Part 1
- Adaptive Zone Defense – Part 2
- Adaptive Zone Defense – Part 3
- Adaptive Zone Defense – Part 4 [Coming Soon]

Tactical Best-Practices and Detection Techniques

The **APT Defense Puzzle** series of blogs takes a bottom-up approach for those organizations that need to take more immediate tactical steps to address their current security posture to address APT and the Insider Threat with practical best-practices and detection techniques. The blogs will gather together the best of the best-practices from the multitude of sources and gather them together to discuss the merits based on industry, organization size, threat/risk tolerance and, security profile.

In this series we have started the process with, as follows:

- APT Defense Puzzle
- APT Detection Framework – Part 1
- APT Detection Framework – Part 2
- APT Detection Framework – Part 3 [Coming Soon]
- APT Detection Indicators – Part 1
- APT Detection Indicators – Part 2
- APT Detection Indicators – Part 3 [Coming Soon]
- APT Red Teams – Part 1

Some quite fundamental but practical steps in that regard we will discuss are, as follows:

- Maintaining a list of application systems at risk
- Creating an APT checklist for assets at risk
- Focusing on APT detection techniques and analysis tools
- Focusing on incident response for APTs

- Creating ready to use APT rapid response tactics
- Preparing an APT forensic response plan
- Increasing use of external threat intelligence
- Focusing on APTs in security awareness training

And … significantly, implementing a policy requiring least privilege and authentication for all intranet services because trust-based access is a weakness that must be eliminated.

The Importance of a Defensible Foundation

While deploying tactical improvements and countermeasures is very important if organizations do not have the luxury to address their architecture and design near-term, a good solid foundation is critical. A Defensible Security Posture, Strategy and, Roadmap should be developed and factored into IT planning as a future goal.

Develop a Secure Architecture Strategy & Roadmap Blueprint

I would like to illustrate my point with an extract from *What Continuous Monitoring Really Means* by Dr. Ron Ross, which appears in the Summer 2012 issue of *FedTech Magazine.* At the end of the day it can cost more in terms of operations, resources and, operational costs to maintain a complex and fragmented infrastructure with band-aids than migrate to a new architecture and design that flexibly supports the business. This is even more important in the age of advanced targeted and insider threats.

Security done right is a business enabler that dramatically reduces total cost of ownership (TCO) providing a tangible Return on Security Investment (ROSI).

IT complexity and fragmentation replaced by an adaptive modular and flexible architecture enables agility and improves your competitive edge — so the business can refocus quickly as new opportunities emerge.

What Continuous Monitoring Really Means

Continuous monitoring is an important part of an organization's cyber security efforts. But without establishing an effective security framework first, those efforts may be misspent.

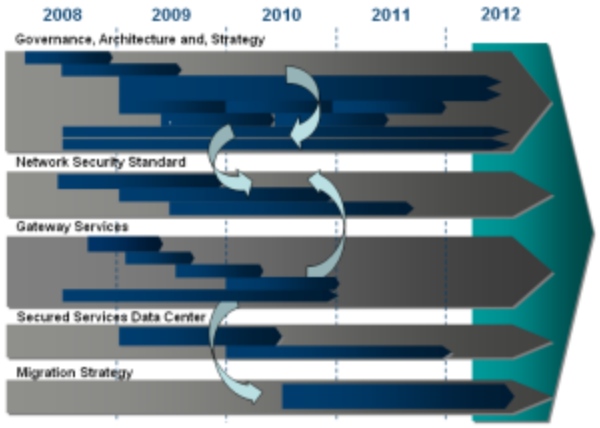
Prototype, Iterate and Evolve towards Holistic Monitoring

Organizations that begin work on a continuous monitoring program with a narrow focus on security controls at the information system level without first doing some basic investment in strengthening their underlying IT infrastructure face significant problems.

First, they may end up wasting significant resources monitoring inherently weak information systems — in essence, throwing good money after bad. You can check a broken lock on the front door of your house once a day or every hour, but the lock is still broken. Better to fix the lock first, reinforce the doorjamb, and then with the remaining resources, check the lock on an ongoing basis.

Second, premature allocation of resources toward continuous monitoring of security controls for information systems may preclude organizations from investing the resources needed to build stronger, more penetration-resistant systems. Such investments are critical as organizations address the advanced persistent threat and cyber attacks associated with sophisticated and well-resourced adversaries. This is especially important for information systems that support key infrastructure.

Strengthening the IT infrastructure begins with establishing a sound cyber security and risk management governance process. Next, organizations must manage the complexity of their IT infrastructures by using enterprise architecture to consolidate, standardize and optimize the current inventory of IT assets as well as developing “threat aware” mission and business processes.



Develop a Security Improvement Program to Evolve Capability Maturity

Organizations must also develop and integrate into their enterprise architecture a security architecture that guides the effective allocation of security controls to their information systems. And finally, organizations must initiate continuous monitoring of all of the above activities to ensure ongoing effectiveness of cyber security and risk management governance, mission/business processes, enterprise and security architectures, and security controls deployed within the enterprise.

Continuous monitoring, broadly applied, can provide important benefits to organizations with regard to cyber security and risk management. It can support and enhance a dedicated, mature process for building the necessary trustworthiness into the information systems. [*Extract from article by Dr. Ron Ross*]

Thanks for your interest!

Nige the Security Guy.