Implementing the Security Process r.04.29.2011

Ryan Matthew Ferris of RMF Network Security

Introduction

I've created four separate documents outlining *The Security Process* for a consultant. The documents detail work flow from initial client meeting, to engaging *The Security Process,* and transitioning to monitoring/training of completed work. My text is intended as an outline for consultants and clients interested in understanding the steps of the *The Security Process*. The text is intended to function as a guideline to the process of developing security independent of operating system, network or company size. Additionally, the document is designed to function independently of associated disciplines of computer security: cryptography, network security, auditing, forensics, REM (reverse engineering of malware), secure authentication, etc. This document is an outline only at present. I hope to update it with more information.

Chapters include:

First Contact: Small Business Work Flow for *The Security Process*

Work Path:Top Level Steps

- Identify (Profile) Client
- Identify Problem
- Identify Client Needs
- Create individualized work plan (scope)
- Present bid/contract/scope for refinement

Probable Clients (Audience) by Size. Make notes on Size and Culture.

- Single Individual
- Small, Medium, or Large Business
- Small, Medium, Large Corporation

Business formats come in all shapes and sizes. Make notes on form, function, market share, competitors

- *Different budgets!*
- Different tax structures
- Different business ownership structures
- Different liabilities
- Different compartmentalization, security needs
- Varying levels of user education

Capturing the Client

- Understand previous and current client history with network security services
- Research client market position and existing service vendor contracts
- Identity client needs
- Sell them your skills exactly
- Sell them your reputation
- Outline steps in the *Security Process* and expected results for each phase
- An important question is whether the client wants a full forensic analysis as part of network security configuration. Forensic analysis is a separate field in computer security. A contract with Forensic analysis included will actually be two separate contracts.

Second Contact: Templates for Managing Expectation For All Clients

What are the realities of Network and Data Security in today's environment?

- A security administrator will almost always needs root level access to the resources they need to secure. This almost always brings up issues of trust and reliability.
- Achieving data and network Security is a high risk, multifaceted process that requires adaptive system design. The design of comprehensive security architecture anticipates future needs and cost.
- Comprehensive digital security is expensive, elusive and brittle in the current threat environment. Preparation for data and monetary loss is an essential part of disaster mitigation.
- All networked environments have risk of ex-filtration, denial of service, malware, stolen resources
- User and Administrator training is an essential piece of securing a network

What can the consultant do for your company?

- Assess and Inventory your Network(s) and Data
- Recommend Malware Removal, Configuration Management, Architectural Remodeling, Asset Replacement as needed
- Consult with management on cost and risk
- Train user base and IT staff as desired by management
- Detail current risks for data and network assets in today's Threat Environment

How will the consultant perform the work?

- With thoroughness and appreciation for detail
- With discretion
- With an appreciation for cost and disaster planning
- With constant communication and well documented work flow and configuration management
- With user and staff training as desired

What resources will the consultant need to perform the work?

- Administrative/Root access as necessary to your networks and data
- Access to existing IT staff resources
- A working “semi-sane” and at least “partially well-managed” network
- Reasonable “change management configuration” policies
- Management and staff confidence, patience, understanding

The Phases of the Security Process

Phase I: Inventory and Assessment

Initializing the Client

- After initial discussion: Sign their **NDA (Non Disclosure Agreement)**; They sign your **waiver (release of liability)**
- Inventory data and Network Assets
- Inventory ownership of data and Network Assets
- Query configuration of key or prototype assets
- Reality Check: "Do they have a sane and well-managed network?"
- Create a summary assessment of "Existing Security"
  - Sum types of assets and versions
  - Assess probability of current and historical infection/ex-filtration/penetration (high, medium, low)
  - Assess existing security infrastructure
- Create summary assessment of work flow and most probable "Problems to be Addressed"
- Create a detailed assessment of new security configuration, malware eradication, asset replacement, security architecture remodeling, client security, server security
- Present bid/contract. Discuss and revise as necessary.

Phase II: Security Testing, Log Analysis, Forensics

- Analysis of existing logs from hosts, firewalls, IPS (Intrusion Prevention System) can be an important part of this phase, however such work can also be a forensic analysis of existing infrastructure. Forensic analysis of existing infrastructure is a security function that *could* be optional; available as a client request. Forensics analysis is in many ways a separate consultancy and should be a separate contract perhaps performed by a forensics specialist.
- Security testing may reveal unknown adversaries, long-standing penetration attempts, surveillance, etc. This is important analysis and information, however, the consultant should be careful not to contribute geopolitical or forensic conclusions based on IP addresses or other evidence because of the problem of *reliability of attribution. (e.g. spoofed IP addresses)*
- Remember: "Physician Do No Harm!" (Or at least be able to fix anything you might break while testing. See consultant waiver form.)
- Use standardized tests and log results to a database!
- Use tests whose outcomes of which you are familiar!
- Document results *only* in this phase! Resist the temptation to change anything until all testing and a full analysis is complete!
- Remember, if you can't easily explain the relevance of a result to a client then that result is

worthless. Exercise some circumspection in the use of tests that produce esoteric results.

- In contrast to the last rule, A client's network can become a test lab for ferreting out the latest "zero-day" malware. Unfortunately, the most difficult of threats may require extra 'byte level' analysis. This will really slow down the *Security Process*. This should be discussed with the client beforehand, as de-compiling and analyzing (especially 'zero-day' malware) is a labor intensive process.

Phase III: Making Recommendations and Implementing Change

- Anticipate known conflicts from Windows Update, Virus software, Firewall policy changes, Proxy implementation,VLAN, VPN, UTM, enterprise based management and logging, application policy driven Firewalls, application based scanners, continuous scanners, client firewalls, MAC address lists, NAC (Network Access Control), biometric authentication,etc. The drumbeat of security of the new *'over-infrastructure'* of security products create their own deployment and integration challenges. The time and cost of integrating new infrastructure should always be over-estimated.
- Based on these test results, your *person/business/corporation* is vulnerable to …
  - Drive recommendations based on current and past vulnerabilities
  - Drive recommendations based on acceptable level of client risk
- Create an "Implementation Plan"
  - Create an architectural before and after schematic or visualization. Link each visual change with a security enhancement.
  - Redo estimate to reflect new configuration management, implementation of new hardware
  - Assess the need for deployment resources, training, configuration management, and documentation.
- Remember the tendency of even small changes to break complex infrastructure.
- Schedule into bid time/dollars to automate mass deployment.
- Review client "change management configuration" policies and procedures.
- Always have a "back-out" plan to return the client to a previous configuration. Client stability is paramount!
- In some cases a "pilot deployment" plan is necessary.
- Document (time and description) all configuration change and new assets or architecture!

Phase IV: Testing Configuration Changes

- Stress testing in the client's environment (*on weekend or evenings!)* can forestall many complaints.

- Anticipate known conflicts from Windows update, Virus software, Firewall policy changes, Proxy implementation,VLAN, VPN, UTM, Enterprise based management and logging, application policy driven Firewalls, application based scanners, continuous scanners, client firewalls, MAC address lists, NAC (Network Access Control), biometric authentication,etc. The drumbeat of security of the new *'over-infrastructure'* of security products create their own deployment and integration challenges. The time and cost of integrating new infrastructure should always be over-estimated.
- A customized test suite should be developed for each deployment from a series of stock templates designed to adequately test major security infrastructure and configuration management changes.
- Allowing adequate time and cost for post configuration (weekend or evening) changes should prevent '*user disaster'* on Monday morning. Even so, anticipate compatibility issues during the **Monitoring and Training** Phase.

Phase V: Monitoring and Training

- Monitoring and training phase could be turned over to existing IT staff for budget conscious firms, however, this removes the consultant's expertise from the network during a period of transition. In practice some period of monitoring and staff training will be needed after any significant changes.
- Forensics analysis can be incorporated into this phase of the *Security Process*. The client should be forewarned that forensics analysis is a separate field. The consultant should create a secondary contract for such work as it will be long and detailed depending on the needs of the client and law enforcement.
- Training existing staff could be time intensive. The consultant will need documentation to be left with staff specific to their configuration changes. A time and materials relationship could be developed with the client for maintenance of the *Security Process*.
- If the client is dealing with *Advanced Persistent Threat* or “zero-day” malware, a separate contract will have to be established to understand and de-compile novel threats.

Frequently Asked Questions

FAQ (Questions To Be Answered For the Client)

- How long will it take?
- How much will it cost?
- Whey should we trust you?
- Will we be guaranteed to be rid of infection and threat after you leave?
- Can you deploy all the products we need?
- Why can't my existing IT staff do what you do? What do you offer us?
- What will the process look like?
- Do we have to give you the “Keys to Our Kingdom”? How do we watch over you?
- How come our substantial investment in Microsoft technology can not guarantee us a secure network?
- What will do to our network and How will you do it?

FAQ (Questions To Be Answered By The Consultant)

- Can you handle the needs of this client?
- Is the client for real?
- Are the clients clued into the drama of today's insecure network environments?
- Do they have a realistic grasp on the competence of their current network administration?
- Have they been recently burned by ex-filtration or data-loss?
- Are they divided on the need for your services?
- Is the manager who hired you “on watch” with higher management for previous data loss or network insecurity events or audits?
- To what degree will existing staff be useful?