Final Project Part 2

Stewart Johnston
CIS 127 – Intro to Information Security
NCMC
johnstons1@student.ncmich.edu

High-level gap analysis plan

The primary concern of the security team for Fullsoft is the information security and how to prevent similar breaches from occurring. We know that proprietary information was copied and leaked as a result of malware infecting machines. The scope of the analyses laid out here, therefore, is more concerned with technological aspects resulting in vulnerabilities to malware and information theft, and digital outages, rather than physical risks such as power-outages, flooding, etc.

The first part of a gap analysis is understanding the current state of things.

1. Identify existing conditions. This list remains open to suggestion of elements to inspect, within the scope stated above.
    (a) Who has elevated/admin rights over what parts of the network and why?
    (b) Software installed, why it is installed, and how it is updated.
        i. Process for requesting new software, if any. How static are software needs to perform operations? Is new 3rd party installation a common occurrence?
    (c) OSs in use, deployment and update method.
        i. Device policy. How are users' own devices handled, if there is a Bring Your Own Device policy in place?
    (d) Intrusion Detection System/Intrusion Prevention System in use, if any.
    (e) Exfiltration prevention mechanisms, if any.
    (f) File server/file sharing methods being used. Why and how are they being used? What kind of security of is being used?

2. Identify vulnerabilities or other outcomes of those conditions. A risk assessment on the current state should be performed at this point.
3. Identify the outcome we want as informed by best practices. Keep under consideration the balance between availability/convenience and security. How much convenience are we willing to sacrifice for the sake of security? Does availability/convenience even need to drop at all? The following list is subject to any order as determined by priorities from the risk assessment.
    - Who actually needs elevated rights? Principle of least privilege is best practice which should be applied liberally.
    - What are the broad strokes of software policy we want for requests, updates, etc? What portion should be self-managed vs managed by IT?
    - BYOD policy, and especially with consideration to how much it would upset ongoing operations to change it. Declaring that no outside devices are to be used for operations may incur some cost if a significant number of staff use BYOD.
    - The variety of platforms present in our network, and by extension, that IT needs to support. Homogenous networks are easier to manage, generally, but are highly subject to the same vulnerabilities across the whole network. Heterogenous networks are (in this professional's opinion, only marginally) more difficult to manage, but 1 compromised user or machine does not necessarily mean the whole network is compromised.
    - IDS/IPS system of choice.
    - Exfiltration prevention (especially weighed against the difficulty to implement). Most research indicates that this is difficult thing to do correctly.
    - File sharing needs and how to fulfill them in a secure way.
    - Any other conditions we'd like changed from the present state.
4. Once prioritized, going about finding and implementing these solutions is the final step.

Risk Assessment Methods

NIST 800-30r1

The NIST 800-30 (revision 1) is part of a series of publications by the National Institute of Standards and Technology. It is oriented largely around threats

and vulnerabilities. Its most well-modeled threats are adversarial threats and weaknesses in security controls.

OCTAVE Allegro

Carnegie Mellon University's Software Engineering Institute publishes the OCTAVE risk assessment methods. Allegro is the more distilled version of this publication. Allegro's scope has a wide-reach, and is focused on assets first. It covers a broad set of topics with a fairly general, widely applicable set of tools. It hesitates to go into much specific detail on any one topic, however.

Recommended Method

I recommend the NIST 800-30 for the risk assessment needs of Fullsoft.

- NIST 800-30 has a heavy focus on adversarial and technological threats, which are directly related to information theft and malware. The OCTAVE Allegro document also covers this, but it has a much less focused goal, and is more broad-reaching, with fewer elements specific to adversarial or technological threats.
- The NIST is fairly intuitive. While the appendices and tables used by NIST 800-30 are easier to use, the typesetting and structure of the OCTAVE Allegro document body is easier to read by comparison. OCTAVE Allegro's tables and diagrams have a lot of repeated information spread out over more space, and that's where a lot of the actual work gets done. OCTAVE Allegro, to the untrained eye, takes a lot of cross-referencing and context switching to perform the actual work. The NIST 800-30 can be followed fairly linearly once work on the assessment starts.
- The OCTAVE Allegro document is 50% longer than the NIST 800-30. That 50% is accounted for mostly in the addition of a series of examples, which serve as a good – but necessary – demonstration. The OCTAVE Allegro process, in my opinion, takes longer to grapple with to learn and use. Both documents are quite dry reading, but the NIST has more actual meat in it, in my opinion.