2006-07
The Life Expectancy of Defenses

Introduction:

Many people imagine that information protection products are set it and forget it, but of course they are not. In fact, most products take a lot of time to configure and get operational and only last for a relatively short period of time once they are operating. This month we discuss the life expectancies of security products.

Tactical defenses with short life spans

The shortest life span defenses are typically things like anti-phishing defenses and awareness programs. While these are often considered vital, they cost on the order of $10 per year per person affected and typically have to be replenished every 6 months or less. Antispam filters are typically good for a few months before they need to be replaced, although some modern product suites are starting to meet the antivirus industry standards in terms of updates.

Antivirus systems are typically licensed one year at a time for a set of computers, many companies have more than one product in place at any given time, and they tend to change from company to company about every year or two. Since antivirus typically cost about $40 per system per year, for a company with 10,000 systems, the cost is on the order of $400,000 per year. Antivirus is essential for each Microsoft platform run, but rarely necessary for other platforms today. Operational costs for antivirus run on the order of one full time person plus a support contract and setup costs involve upgrading all of the systems with patches. So the net effect is something like $50 per system per year for a large enterprise and more like $100 per system per year for a small enterprise. All of this is done every year or two as the values of different solutions come into play and market conditions change. Almost all of these projects succeed if adequately funded.

Defenses with moderate life spans

Most enterprises replace personal computers every 2-4 years depending on the specifics, with few running PC platforms for more then 3-5 years. But replacement cycles for the maintenance mechanisms tend to be somewhat shorter. An average configuration management solution today is less than a year old, and it has a life Expectancy of only 1-2 years. Patch management systems tend to change every year or two as the limitations of each system becomes clear and the grass is thought to be greener on some other product's side of the fence. Desktop security tools for controlling access to software, hardware, the PC itself, connection to networks, and so forth tend to last about a year as well, with some running for as long as 2-3 years, but these are the exceptions rather than the rules, and they tend to become unmanged over time. These tools and the management consoles that control them are constantly being updated, modified, and over the period of 1-2 years, mostly replaced.

Some suites have had their lives extended year by year, but most of these extensions are more like replacements, and the price that is paid is paid year after year in upgrades, licensing and support fees, and the eternal changes, upgrades, side-grades, and new replacements that come your way. Finally, for most of these tools, the success rate is on the order of 70% for properly funded efforts. While many projects succeed, dedicated staff and commitment for the full term of the effort are required for success in these medium-range efforts.

The longer-term tools

In the case of identity management, less than half of the large-scale deployments end up in large-scale successes, despite years of effort and serious enterprise-level commitment. While Active Directory may be reasonably effective in a Windows environment, the commitment to getting unification surrounding system and infrastructure management is far larger than usually anticipated, and even the strongest effort rarely gain control over all enterprise systems. Identity management efforts last for 1-2 years and the results are applied for 5 years or longer.

Enterprise-wide security architectures typically take from 1-3 years to get in place and often operate for 5 or more years, with minimal refreshes every 3-5 years to compensate for changes in technologies and the environment. Enterprise network security architectures are almost all successful, even when slightly underfunded, and they typically have lasting effects over long time frames. They are both highly effective at what they can do and last longer than most other solutions.

Conclusions:

Churn keeps most security vendors alive. With no real motive to make longer term solutions available and every reason to force updates as a key element of the ongoing revenue stream at the heart of the modern security company's revenue stream, we can expect no less.

But longer-term investments tend to be more significant to the enterprise, cost less per system, last longer, and work better over time. While you cannot really abandon the short term solutions, emphasis on the strategic is a better investment over the long run.

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 39, section 2.5.1.15 we present:

"Jamaican Switch – 419 Frauds"

> *"The target is asked to hold large sum of foreign cash for the "foreigner" who takes real cash as a deposit. These are also called 419 frauds because statute USC 419 covers these sorts of frauds.."*

The Jamaican switch has moved – first to Africa, where the major perpetrators were finally caught after more than ten years of success, and since then to South America. The game is the same, but South America is rapidly becoming the center of the Jamaican switch.

Countering 419 frauds is relatively easy – all it takes is awareness. But user awareness has proven one of the most elusive goals of information protection for a long time. That's because people – all people – have cognitive limitations that make them susceptible to deceptions. This is covered in detail at http://all.net in the Library under "Deception for protection" and more concisely within section 3 of Frauds Spies and Lies. There isn't much we can do about the inherent nature of human frailties, so user awareness continues to be a key focal point of counter-419 efforts.

Chet's Corner

The cool tool of the month helps figure out how to meet the ISO 17799 standards by relating them to the CISO ToolKit. Just pick a subsection of ISO and it pops up with a whole set of related areas from the ToolKit. Look for http://all.net/MAP/index.html.

Also, check out SUSE Linux Enterprise Desktop 10 from Novell. It's starting to look more like Apple's OSX interface and has more and more of the automation you come to expect from Apple and dream about in Windows.

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's security architecture development:

Security architecture is one of the best investments companies make when it comes to security. For a few tens of thousands of dollars, they can work out ways to restructure their architecture to dramatically reduce the frequency and severity of security incidents and make them more manageable when they do occur. And the approach works over periods of 3-5 years rather than 6-12 months.

> One of our clients recently asked for a security architecture review to cross check on their new network architecture. They had spent hundreds of thousands of dollars on plans for the new architecture and were about to spend even more building it out, so they wanted a cross check to make sure they got the security right. We spent 2 days on site and produced a report within 10 business days.

One of the most satisfying things we encounter in the security consulting business is clients who do a good job before we get there. This client was very satisfying and very satisfied. They had an excellent design and had thought through most of their security decisions very well. We helped in a few key areas and fine tuned some of their security decisions, but for the most part they were dead on target.

One of the best ways to judge the value of consulting to a client is to see what they do with it, rather than what they say about it. It looks like our work with their architecture group didn't become shelfware. They are implementing the changes we suggested along with their new architecture even as we write this.

Mollie gets the last word in

This month I am house sitting and one of my tasks is to read and repurpose some of the content of "Security Awareness Basics". It's cool that the same things companies train their employees to do I have to do when I house sit. Hopefully no burglars will show up and I won't have to carry out the instructions in section 6!