

Holistic security

Introduction

In this, part one of a series of whitepapers on security, we will focus on “The Big Picture”. Most security alerts, articles and warnings deal with a specific vulnerability or threat assessment. These are all important and deserve all the attention they can be afforded. It is, however, important not to become myopic in ones focus. Security must be viewed holistically; it is not enough to tighten up one area (or probably more realistically one part of one area) when attack vectors flourish in other parts of the enterprise.

This document is meant as a high level holistic overview of security by means of example. Later documents in the series will be more focused on specific threats and remedies.

We will use two stories - one of Bob and one of Alice. Bob and Alice will be a continuous feature in our series, paying homage to the body of work in cryptography and computer security in which they frequently appear. They will, however, play different roles in each document. The stories are written in a fictitious manner for simplicity, but they should not be confused with fantasy.

Bob

The common conception of a security threat from an IT perspective is that of a socially unskilled teenager with massive amounts of time and deep skills in a specific topic. Lets call him Bob. Bob spends a lot of time in his room on his computer. He drinks a lot of caffeinated beverages. Bob likes to show off his skills. One of his favorite tricks is to place crude messages on corporate websites - a form of tagging in the brave new cyberworld. He can show his cyberfriends all over the world his achievement and his intrusion might even get mention on the news.

The defaming of a corporate website can certainly be unpleasant. It can even be humiliating but, in today’s climate, it is fairly benign. Bob’s goal, was short-sighted and simple. In fact, Bob’s deed could even be seen as helpful. Forensic research of his intrusion should lead to information about how Bob was able to intrude. His attack also provides a strong incentive to stay on top of the latest patches and releases. In the end, it will lead to a safer system.

One can be sure that if action is not taken rapidly to fix the vulnerability, Bob’s acquaintance Frank, who is not as skilled but craves attention all the same, will replicate Bob’s actions and be able to put up his own funny slogan.

However, neither Bob nor Frank should keep you up at night. Alice should.

Alice

Alice is a very skilled and multi-faceted professional. Her incentives are usually monetary in nature. She might be part of a team or she could be flying solo. Alice is hired by large companies to help them gain a competitive advantage or a speculator who needs a specific piece of a puzzle. Alice works in the field of corporate espionage.

If Alice does her job right, her presence will be stealthy and her intrusions unknown.

Alice knows that she is supposed to find out about a big deal your company is doing with another company. She knows your executive team will be buzzing about it. Maybe it is the biggest deal of the month, the year or even the lifetime of the company. Memos will be written. Emails will be sent. Draft agreements will be rewritten. Cellular conversations will be had and some dreaming might be done in the executive room of a local gourmet restaurant.

Alice might not have to go high tech at all. Basic reconnaissance might be the garbage bins outside the office. Perhaps some careless executive assistant threw away the first five drafts of an important document. A treasure trove might be waiting among the coffee grunts, the banana peels, and the crumpled transcripts from last week's meeting.

But no. Not this time. Alice now knows that the company is aware of such a brute attacks and that there is no way to gain access to the thrash from outside the building.

Alice studies the company. She hangs out at the local taverns during lunch and the bars during the evening. She hears a lot of complaints. She can tell that the average employee is underpaid, undervalued and doesn't get the respect he deserves. Over a few days of patient martinis at night and salads during the day, she might be able to zero in on a few people -people with access to the building, to the office and to the internal trash. She might offer money directly to a few but that is crude and traceable. She might be able to gain information simply by being an active listener. Adopting a skill set known as "social engineering" she might only get a fragment, a bit more of the hierarchy, maybe only knowledge of who knows.

Another approach entirely would be to take a job at the company, maybe as a temp assistant, maybe as a cleaning person. A lot of cleaning companies have high turnover. A lot of companies have stringent background checks for all employees (even temp assistants) but have outsourced the cleaning. A document left on a desk or a recycling bin that has not yet been emptied or shredded, might provide access to the elusive pieces of data Alice needs.

It is important to keep in mind that although Alice would prefer to find the piece of data directly, once she has gained access to the building, a chart of network topology, carelessly placed Post-It notes with passwords or a well placed key logger to be retrieved

a few days later, she has a means by which to gain more information and get closer to her data.

She might also be looking around the cubicles in the finance department. While dusting off the desktops, perhaps she notices that Wendy is an enormous fan of Lost and also is an avid Myspace user.

Later that night, Alice might craft an enticing email from the Myspace staff detailing the latest Lost features that will be coming up on Myspace. The email is sent to Wendy's work address. It might contain a Trojan directly or it might direct Wendy to click on a link that looks like a Myspace account. Perhaps it is. Silently behind the scenes, the Trojan disables Wendy's local firewall, installs a rootkit and starts probing the internal network. While all this happens, Wendy is enjoying the write up on Sayid's diary and the IT guys sleep well since no intrusion attempts have been detected.

But perhaps Wendy really is a bore and provides no new information. Alice is getting restless. Her clients want results and it is time critical. With the knowledge she gained of the IT network infrastructure, Alice can be very precise in her intrusion attacks or she might craft a very specific attachment to a director of the company. She knows all the directors carry around Blackberries. Her attachment will exploit a little known bug in the Blackberry attachment server. Certainly, by gaining access to corporate email, she would find what she is looking for. Alternatively, she could steal a laptop from a car or desk.

In a recursive manner, she builds her knowledge and her ability to get the information she needs. If she gets desperate, her stealthy approach might fail her. If she does her job well, her presence will never ring any bells and her clients will be very happy. Perhaps the only knowledge anyone will have is the news story of a very fortunately placed series of trades just a month before the deal was made public.

Conclusion

The idea of our two stories is to evoke an interest in viewing security as an integral part of each employees training and as a concern for each department of a company. Security is not something that should be delegated to the IT staff and the guys who check badges at the door.

It should effect HR (hiring, trimming of the staff, benefits and wages), IT (patches, updates, intrusion detection and extrusion detection). Every worker (shredding of papers, careful with speaking in semi public places --Loose lips sink ships even in the corporate world), Outsourcing (Are the people who are hired through an agency as closely vetted as your internal people?). Are your employees happy with their job? Do they love the company?

The two stories are not fiction, nor are they directly based upon a single story, but a combination of various real life events.

It is important to remember that security is a process - a continuous process. There is no real end but there are incremental improvements and milestones. There are rewards as you progress, measured in terms of increased security. It is a complex process; drastically improving one area might actually make things worse in another area. It is a process to strike an appropriate balance between the perceived threat level and the convenience of the staff. The hardest and most important factor to control in this field, as in many others, is the human factor.

Steps to improvement.

- Walk around the office. See what documents you can find.
- Train employees about general security concerns, document safety, door safety, the beauty of shredders.
- Promote loyalty and happiness in the company. Nothing is more important in security than the human factor.
- Create a clear and concise policy regarding printed documents and the disposal of them. Have an easy system to classify the sensitivity of the documents.
- Investigate if some of the Digital Rights Management systems for electronic documents might benefit you.
- Investigate using cryptography for email and important documents. A PKI system, like PGP, is a wonderful means by which to keep documents secure even after intrusion. (Given that the private key is safeguarded).
- Products like PGP Desktop can also encrypt the entire drive on a computer, making the data inaccessible even if someone steals it.
- Secure the login process with a product like RSA SecurID. It can make keylogging for passwords a thing of the past. (or at least a lot harder). (This does however not protect against new types of phishing attacks)
- Investigate Biometric security. This field is growing and for good reason. A single sign on system is driven from a two factor authentication system, where one factor is biometric.
- Investigate storing encrypted data in the database.

If you feel that you have already covered most the items on the list, give yourself a congratulatory hug and stay tuned for our next article: XSS and you.