Cyber Security, Offensive and Defensive Internet Management

(2)

# Reece Hugo Zunino

# March 29th 2015

# Introduction

Cyber Security in recent years has become a growing occupation for IT Specialists and students seeking a growing challenge in the IT community. Like with most problems there are different ways in handling the same problem either we use an offensive approach or a defensive approach. Offensive Cyber Security is a proactive approach and adversarial approach to the problem in the security. Conservative Cyber Security, sometimes referred to as Defensive Cyber Security focuses on reactive measures, such as patching software or finding and fixing venerable systems. These two approaches are used in many different ways as explained above and the most commonly used method in by far the Offensive approach which is done on a daily basis with daily scans and monitoring of the systems and making sure to prevent attacks and repelling them instead of fixing and cleaning up the damage to the software and network data.

# Ethical Issues

Cyber security crimes must be treated by systems of law with the same importance as traditional crimes. In the digitally augmented world in which we live, criminal organizations are no longer limited by their physical theaters of operation. The cloud, with its multiple actors and access points, presents a lot of blind spots where it is easy to threaten the integrity of the data that are shared. The surest way to make it secure is through an end-to-end security framework where responsibilities and penalties are clearly defined.

Cybercrimes weren’t always easy to pin on an individual for things like identity theft and still even today are harder to track down the suspect in the cyber world. Even with the many different advancements in Cyber forensics it is hard to trace, track or identify the individual or persons responsible for committing the crime which is why being proactive in Cyber Defense or practicing Offensive internet management verses Defensive Internet management will have better results in the long run.

## First Sub-section

Many of the ethical issues that face IT professionals in the Cyber Security world involve privacy. Below are some examples:

Should you read the private e-mail of your network users just because you can? Is it OK to read employees' e-mail as a security measure to ensure that sensitive company information isn't being disclosed? Is it OK to read employees' e-mail to ensure that company rules (for instance, against personal use of the e-mail system) aren't being violated? If you do read employees' e-mail, should you disclose that policy to them? Before or after the fact?

Is it OK to monitor the Web sites visited by your network users? Should you routinely keep logs of visited sites? Is it negligent to not monitor such Internet usage, to prevent the possibility of pornography in the workplace that could create a hostile work environment?

Is it OK to place key loggers on machines on the network to capture everything the user types? What about screen capture programs so you can see everything that's displayed? Should users be informed that they're being watched in this way?

## Second Sub-section

Then there are money issues. The proliferation of network attacks, hacks, viruses and other threats to their IT infrastructures have caused many companies to "be afraid, be very afraid." As a security consultant, it may be very easy to play on that fear to convince companies to spend far more money than they really need to. But does it make it right for Cyber Security professionals to charge more than needed for their services? Well from an economic stand point yes it does since the need for their expertise is in high demand than you will always see an influx of prices with those services until there is a massive influx of up incoming IT professionals offering the same services for a lesser price than the ethical over pricing will slowly fade away.

# Trends and Ways

Is Defensive Cyber Security also known as conservative the best approach to fighting off Cyber Attacks?

The offensive approach to cyber security is not a new concept. As a matter of fact it has been one of the most widely used approach among the cyber security world for many years. Considering that cyberspace has no physical boundaries, it must be considered that an offensive approach could have consequences on internet users located in foreign states with serious repercussion under legal profile. Since there are not always hackers hacking in from our back door and instead from all over the world that leads us to this approach in Cyber Security

Is Offensive Cyber Security the best approach in preventing cyber-attacks on a network?

The Offensive approach isn’t always the best option since usually the attack and damage has already happened and now you’re piecing back together the network and eradication all the Ware left behind from the attacker and hoping you catch all the holes the attacker left in your system if it happened to be such a severe of an attack. We will not cover much more of this part of the topic since it is not the most widely used or best way of approaching a cyber-security problem.

## First Sub-section

What are the different tools of the Cyber Security arena?

There are a few different tools used in defensive cyber security. One of these tools is called penetration testing. Penetration testing is used to find out if there are any weaknesses in a networks capability in defending its self from an outside source against its networks and system. The definition for penetration testing is “a penetration test, or the short form pentest, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data”.

Wireshark is the very first step in vulnerability assessment is to have a clear picture of what is happening on the network. Wireshark (previously named Ethereal) works in promiscuous mode to capture all traffic of a TCP broadcast domain. NAP is probably the only tool to remain popular for almost a decade. This scanner is capable of crafting packets and performing scans to a granular TCP level, such as SYN scan, ACK scan, etc. It has built-in signature-checking algorithms to guess the OS and version, based on network responses such as a TCP handshake. And those are just a few of the tools available in the Cyber arena.

# References

Conneran, K. (2014, September 14). Cyber Security Active Defense: Playing with Fire or Sound Risk Management? –. Retrieved from <http://jolt.richmond.edu/index.php/cyber-security-active-defense-playing-with-fire-or-sound-risk-management/>

Cyber Security Manifesto. (2012, October 1). Retrieved from <http://cybersecuritymanifesto.com/>

Cyberethics - Wikipedia, the free encyclopedia. (n.d.). Retrieved April 29, 2015, from <http://en.wikipedia.org/wiki/Cyberethics>

Paganini, P. (n.d.). The Offensive Approach to Cyber Security in Government and Private Industry - InfoSec Institute. Retrieved from <http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/>

Phatak, P. (2012, February 22). Attention Required! | CloudFlare. Retrieved from <http://www.opensourceforu.com/2012/02/top-10-security-assessment-tools/>

Shinder0, D. (2005, August 2). Ethical issues for IT security professionals | Computerworld. Retrieved from <http://www.computerworld.com/article/2557944/security0/ethical-issues-for-it-security-professionals.html>

Wigmore, I. (2012, November). What is offensive security ? - Definition from WhatIs.com. Retrieved from <http://whatis.techtarget.com/definition/offensive-security>