IBM i2

-by Vikram Patil

Tuesday, February 11, 2016

There have been many famous attacks on big enterprises like Sony, Facebook, and Google etc. from various parts of the world. Such big enterprises spend millions of dollars just to make their systems safe and threat free. IBM i2 is a product for cyber security which prevents threats and keeps the business interests. Here is a summary of Mr. Bob Stasios seminar on IBM i2.
An attack was detected recently where attackers run a client side script. This script generated a prompt asking username and password. These prompts suggested user that the browsers session has expired and ask for credentials of the site visited such as bank website. Hence the credentials of the users were maliciously stolen in a well organized attack. This particular group of attackers called, FIN 4 Group was arrested and it turned out that they had made 100 million USD profit since 2013. The problem with the security is system is that it detects the threat when attack has already happened.
The attackers are pretty smart in the way of organizing and executing the thefts. Growth I such asymmetric attacks is changing the landscape. Even a very cheap hardware like a remote control device can make huge theft. Here is an example. This attack on a bank happened recently where a man in an IT technicians disguise installed a remote control device on a bank branch office computer. The thieves then accessed banks servers from a nearby hotel. They transferred 2.1million USD to fake accounts.
Information security and cyber analysis must address the problem of non-linear relationship between effectiveness in security and the investment done for the same. With low cost an enterprise can achieve 80Security can be learned from medical analogies. Consider, hospitals reduce the casualties in three steps. 1st level is hygiene where general infections are prevented. Then comes the specialization level where emergent situations such as accidents are handled. At the third level called research, more complex diseases such as cancer are treated. The same levels can be applied to security. At the 1st level, threats from hackers can be stopped by changing passwords. Then in next levels, more sophisticated attacks can be handled by security analysis and cyber analysis.
The cyber analysis is made up of mostly three components.
Information Security: It involves aspects of network security, confidentiality, assurance and malicious software threats.
Intelligence Analysis: Here information is collected, processed and analyzed to create a intellectual framework for decision making.

Forensics Science: This involves an investigative process, evidence handling and evidence searching.
Cyber security results in Integrated data feeds, Enterprise awareness, Compliance monitoring, Threat discovery, Risk management and Enable Decisions.

Reflection on the Seminar

Research in cyber analysis plays a big role in keeping todays internet world safe and it is very essential. It is a very interesting field as it involves intelligence of both humans and machines. The strategic intelligence can help detecting threats and patterns in threats well before the actual attack. IBMs strategic threat analysis platform provides this intelligence which helps in keeping the enterprises safe from threats. Cyber analysis is a new discipline and it is made of three components, information security, intelligence analysis and forensics science. Information security is kind of basic system in preventing attacks which involves high expertise from companies like CISCO and SOC organizations. Intelligence analysis is much sophisticated than information security. It involves high expertise from military and the intelligence communities like CIA, FBI etc. Forensics science involves investigative processes. It has high expertise from law enforcement and HR community.

This is my Github repository : `https` : //`github.com/vikrampatil1/IBMi2.git`