Talk on Cyber Threat Intelligence by Bob Stasio

Surya Valluri

02/11/2016

Summary

The lecture covered topics of explaining various attacks, analyzing the loop holes and some preventive measures in terms of cyber threat intelligence. Talking in the actual numbers, only 1% of the cyber threats/attacks can be sensed and defended the remaining go undetected. Starting with FIN4 attacks, a group of hackers gained access to different pharmaceutical companys data by doing phishing attacks. They started screening everyones mails and had access to sensitive information and they choose the static attack. Screening the mails they snatched the companys future plans, trading strategies and implemented in their firm. By following such strategy the attackers gained billions of dollars for the company they have been working for. In the similar way a couple of hackers walked into a bank, installed a program in the banks network and within no time they robbed billions from the bank.

The above mentioned attacks happened even if the organizations maintained pretty good security. But one small hole was enough for the hackers to storm in and gain master access to the data. The above attacks doesnt imply that the organizations lacked in security, but describes the asymmetric nature of cyber-attacks. However good the system security it is, there can be one or the other way to intrude into the system and break it by some or the other way.

If we had a closer look at these attacks, majority of them can be prevented by following a good firewall protections. The rest can be prevented by correct response to any threat/attack and also by maintaining good security hygiene. Lets take the Sony attack as the next example to get a better understanding about the measures to be taken for cyber-attacks. A group of hackers entered their network and started screening the data and worked towards moving ahead in the system. In the span of 6 months they gained accessed in the system to such an extent that they were able to delete around 30GB of data without anyone's notice. Even though they had better firewall security, attack did happen and loss did occur. But a better understanding on reporting minor threats/attacks could have helped the situation. Before the data was washed out, there were around 25 passive attacks by the hackers trying to gain secure credentials. But the internal system assumed that they were pretty passive attacks and didnt

gave much focus, which are actually very serious. Later after few days they observed some unusual server to server logins and along with which two malicious mails were opened. If they had taken special attention and tried to get the root cause for those small attacks, situation would have been way better instead of leading to massive data attack.There are mainly four areas which are hard to be taken care for cyber threat intelligence: Hidden threats in the system, Where should analysis of data look for, lack of actionable intelligence from the received threats, too much data and many sources to handle.

Reflections

The talk exposed bold facts about how weak is the present cyber security and the number were pretty shocking. Bob Stasio was visionary and very informative.Understanding the present scenario of cyber threats a perfect secured system actually doesnt exist but two measures can be taken into consideration while designing a system. One is to design a very good defense system and keep on upgrading the system just to make sure that hackers are not way ahead of the system. Because hackers keep on try finding ways to intrude the system which can be prevented by regular upgrades. The second one is, how much ever preventions we made there will be for sure an attack. But the system should not be in such a state that letting the user know about the attack after weeks or months. The security system should work as simple as a smoke alarm, raising the danger signal when it senses and danger to the system.