CYBER WARFARE – HOW TO FIGHT THE ELECTRONIC WAR

Smitha Mave
EMC
Smitha.mave@emc.com

Table of Contents

Disclaimer: The views, processes, or methodologies published in this article are those of the author. They do not necessarily reflect EMC Corporation's views, processes, or methodologies.

Introduction

Imagine switching on the TV and finding that terrorists have taken control of country's nuclear command center, crashed the computer systems in the country's stock market, and siphoned off all the money from the bank accounts to an untraceable bank account. Then the power goes off and the entire nation is in darkness because someone brought down the power grids. This is no longer a scenario from a Hollywood movie; it can happen anytime with the advent of cyber warfare.

According to an article in The New York Times in June 2012, the U.S. carried out increasingly sophisticated attacks using a computer worm called "Stuxnet" on Iran's computer systems to destabilize its nuclear enrichment facilities.[1] According to another news article, the terrorist group Al-Qaeda was planning to launch cyber attacks against the U.S. networks of both government and critical infrastructure, including the electric grid. Also, there have been multiple attempts to break into military networks to steal sensitive information. The list grows.

Wars are not fought in the traditional battlefield with the bombs and missiles anymore. It is fought online from a remote location. The enemy is unknown. The weapons are also sophisticated and undetectable. How do you fight such a war? Are the nation states and business organizations prepared to fight such a battle?

This article introduces the concept of Cyber Warfare and advanced persistent threats (APT) with a case study of Stuxnet. It also covers the security measures to identify and stop these attacks.

Evolution of Cybercrime

The initial hackers were mainly techies who just enjoyed the thrill of hacking and the challenge of reverse engineering and breaking a technology. Some of them did it for a name about which they could brag within the hacker community. Initial forms of viruses replicated themselves and did harmless things like popping up a message or shutting down systems on a specific date. The intent was to showcase the technical mastery or to support an ideology.

But, as more financial and other mission-critical operations went online, the hackers realized the financial gains involved in hacking. This led to more harmful activities in an organized manner.

The amount of damage caused by viruses and malware increased manifold. More resources were dedicated to find vulnerabilities in popular software and operating systems to be used for malicious activities. It also led to stealing credit card numbers, Social Security numbers, and other personal information to carry out fraud and identity theft.

Players in the cyber crime arena belong to various categories with varied motives. Table 1 gives an overview of the landscape. [2]

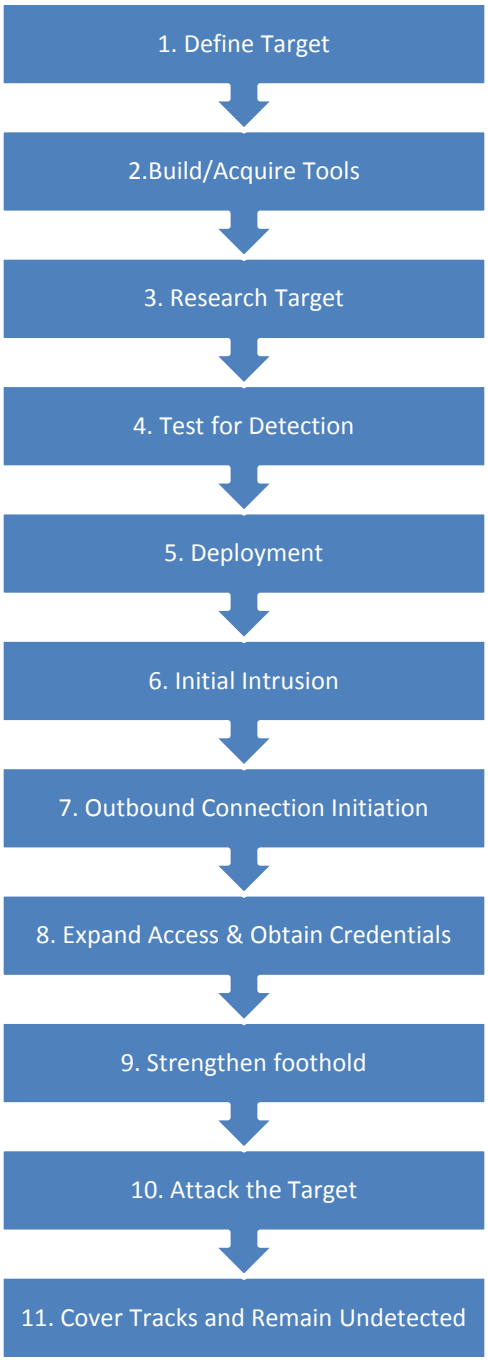
Typical cyber criminals

What is Cyber Warfare?

According to Wikipedia, cyber warfare refers to politically motivated hacking to conduct sabotage and espionage. Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary, or classified information) from individuals, competitors, rivals, groups, governments, and enemies also for military, political, or economic advantage using illegal exploitation methods via the Internet, networks, software, and computers. [3] Such attacks are also referred to as Advanced Persistent Threats (APTs). They are targeted, dynamic, and stealthy.

Anatomy of an Advanced Persistent Threat

An advanced threat differs from the traditional cyber attack in that it requires extensive research, unlimited resources, technical know-how, and highly skilled hackers. The actors are usually nation states or terrorist organizations who have all of these requirements at their disposal. The following section lists the steps involved in an APT.



Anatomy of an APT

1. **Define Target**

   APT is a targeted attack. The attackers set out with a specific aim and target. The first step would be to define the target and set the objective of the attack.

2. **Build/Acquire Tools**

   Attackers can go to any extent to conduct this attack. They will acquire the required technologies and build special tools and software to carry out the attack. The final malware developed might be a collection of multiple malwares with different components.

3. **Research Target**

   This step will involve gathering all types of information about the target from various sources. It will include details about the infrastructure and employees which are publicly available. For instance, a simple Internet search may fetch information regarding the key officials, their designations, email IDS, and so forth. Satellite-based maps available on the Internet can give precise information about a country's critical installations such as power plant locations and defense bases which could be used for an attack. Key employees falling prey to spear phishing attacks—phishing attempts directed at specific individuals or companies to gather more information—also give away critical information to the attackers.

4. **Test for Detection**

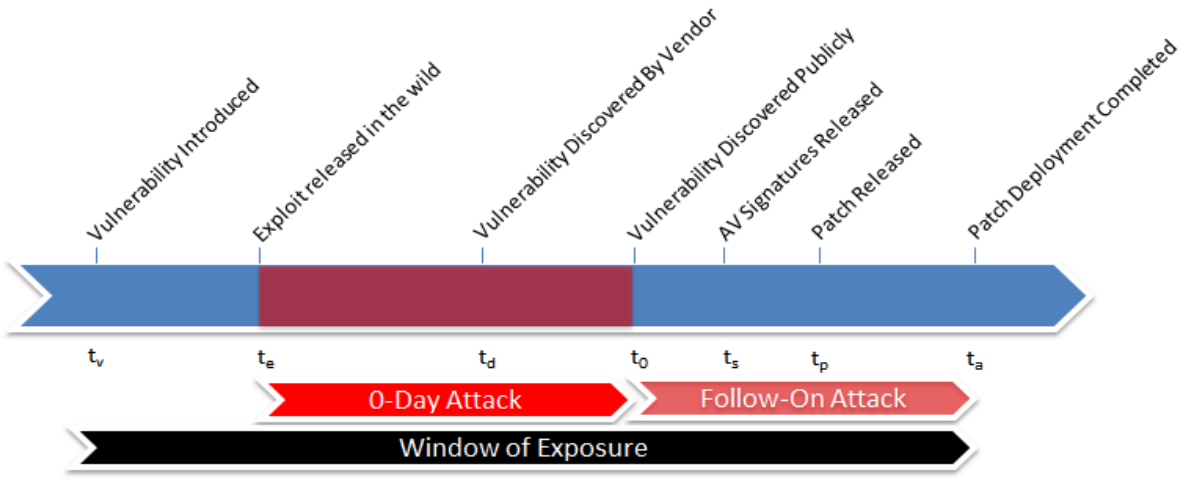
   It is very important to stay undetected for an APT to succeed. Attackers will carry out test attacks to check the loopholes in the perimeter security and check if the intrusion goes undetected. The malware is released only when it passes all the tests to bypass the security software and any other forms of detection.

5. **Deployment**

   The deployment of the malware is performed through emails or removable media such as USB flash drives. An insider needs to connect the USB drive to a system in the network or click on an attachment in the email.

6. Initial Intrusion

The malicious program enters the system by exploiting zero-day vulnerabilities. A zero-day attack exploits an existing vulnerability for which the vendor has yet to release a patch. The timeframe between introduction, discovery, and patching of a vulnerability forms the window of exposure. An example is shown in Figure 2.[4]



7. Outbound Connection Initiation

Once the malware enters a network, it establishes connection with a command center. The command control architecture uses a command center at a remote location sending instructions to the malware inside the target environment. Through this, the malware can be upgraded and modified based on the real time requirements. The command control communication may use a custom protocol or deceptively insert itself into a legitimate network communication.

8. Expand Access & Obtain Credentials

Once inside the network, the malware rapidly spreads to other systems in the network using network protocols or Remote Procedure Calls (RPC). It also tries to elevate the privileges. With higher privileges it can access more information, perform more actions, and remain undetected.

9. **Strengthen Foothold**

   At this stage the malware will continue to spread and collect more data as a means to reach the final target. It will do all the preparations to perform the final activity.

10. **Attack the Target**

    Now the malicious software performs the final set of operations it was intended to perform. This may include stealing the data, sabotaging the system, or any other specific activity for which the entire operation was planned.

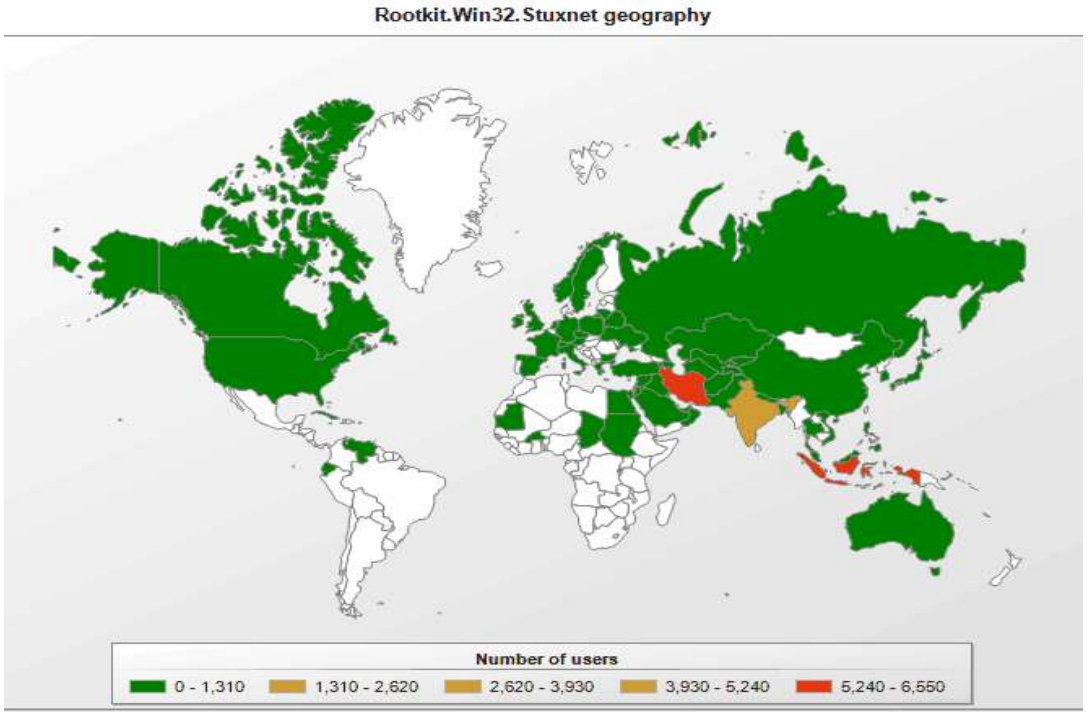
11. **Cover Tracks and Remain Undetected**

    The malware will have mechanism to delete itself once its final target is met. If detected, the attackers do not want their identities to be known unlike traditional hackers who like to show off. So, all care is taken to cover their tracks.

Stuxnet – How Iran's Nuclear Reactor was Destabilized[7]

Stuxnet was the first known cyber attack performed on a nation's nuclear facility using a weapon completely made up of code. It is also the first known malicious program to target an industrial control system proving that the possibilities shown in movies can be turned into realities. Its source code is available online. This raises the questions about the security of nuclear infrastructure, power grids, and defense installations.

Stuxnet was designed to be activated only when the specified target was reached. Until then it lay dormant and spread stealthily. A study by security vendor, Symantec revealed that Stuxnet initially affected Iran, Indonesia, and India. Following diagram shows its spreading pattern.[5]



The Stuxnet worm consists of a layered attack against three different systems:

1. The Windows Operating system
2. Siemens PCS 7, WinCC, and STEP7 industrial software applications that run on Windows
3. One or more Siemens S7 Programmable Logic Controllers (PLC)

Stuxnet also contained code for a man-in-the-middle attack that faked industrial process control sensor signals so an infected system does not shut down due to detected abnormal behavior.

Windows Infection

Stuxnet used four zero-day attacks and other vulnerabilities in Windows OS. Initially it spread through removable drives such as USB flash drives. It then used other exploits and peer-to-peer RPC to infect other systems in the network which were not connected to an external network.

Windows component has both user-mode and kernel-mode root kit capability. The device drivers used in it have been digitally signed with the private keys of two certificates. These certificates were stolen from separate well-known companies, JMicron and Realtek, both located at Hsinchu Science Park in Taiwan. The driver signing helped it install kernel-mode

rootkit drivers successfully without users being notified. It could remain undetected for a relatively long period of time because the certificates were valid.

Two websites in Denmark and Malaysia were configured as command and control servers for the malware. Using this configuration, the malware itself was being updated from the remote location. The malware also uploaded information back to the command server.

Control System Software Infection

Once installed on a Windows system, Stuxnet infects project files belonging to Siemens' WinCC/PCS 7 SCADA control software (Step 7). It affects a key communication library of WinCC called s7otbxdx.dll. WinCC software running under Windows has the ability to configure and program Siemens PLC devices.

Stuxnet intercepts communications between the WinCC software and the target Siemens PLC devices when the two are connected via a data cable. This allows Stuxnet to install itself on PLC devices unnoticed. Further, it can mask its presence from WinCC if the control software attempts to read an infected block of memory from the PLC system.

PLC Infection

Stuxnet is programmed to target specific SCADA configurations. It requires specific slave variable-frequency drives (frequency converter drives) to be attached to the targeted Siemens S7-300 system and its associated modules. It only attacks those PLC systems with variable-frequency drives from two specific vendors: Vacon, based in Finland and Fararo Paya, based in Iran. Furthermore, it monitors the frequency of the attached motors, and only attacks systems that spin between 807 Hz and 1210 Hz. The industrial applications of motors with these parameters are diverse, and may include pumps or gas centrifuges.

Stuxnet installs malware into memory block DB890 of the PLC that monitors the Profibus messaging bus of the system. When certain criteria are met, it periodically modifies the frequency to 1410 Hz and then to 2 Hz and then to 1064 Hz, and thus affects the operation of the connected motors by changing their rotational speed. These details show that its designers had in-depth technical knowledge of the target and the malware was developed with very advanced technical details.

It also installs a rootkit—the first such documented case on this platform—that hides the malware on the system and masks the changes in rotational speed from monitoring systems.

From an extensive analysis of the Stuxnet, it was concluded that it is an advanced malware aimed at a specific target. Some of the unique features that researchers found in Stuxnet which led to this conclusion were:

- It was designed to be activated only when the specified target was reached.
- It is very unusual for malware creators to use four zero-day exploits. Each of these fetches very high rates in the open market.
- Stuxnet is unusually large—half a megabyte in size. It is written in several different programming languages (including C and C++) which is not very common in regular malware.
- It used two (compromised) digital certificates.
- It injected code into industrial control systems, the first known attempt to do something like this.
- It included an upgrade mechanism which was triggered by the remote command center.
- It had the code to cover its footprints and delete itself.

Cyber Counter-intelligence

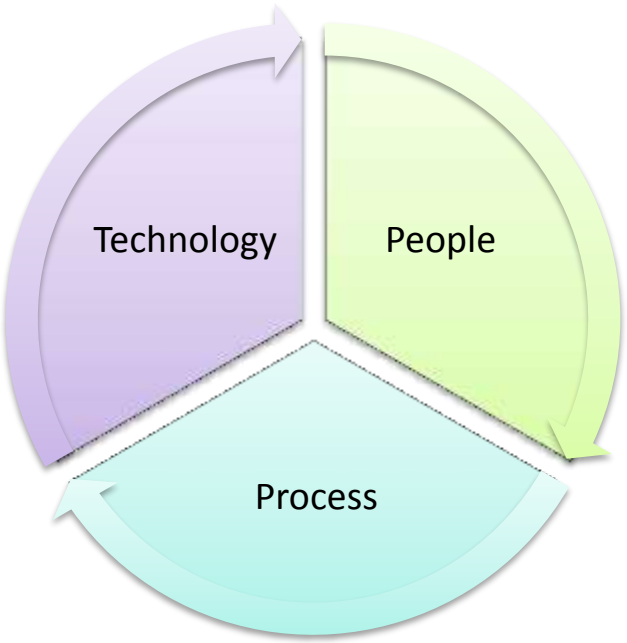
Cyber counter-intelligence are measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.[2] Most governments have passed laws and strengthened their security cells to factor in the strategy to defend against APTs. As an attempt to strengthen the defense against cyber war, NATO established the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia.

But, there are still grey areas. When the crime is initiated at a foreign country and the crime was perpetrated in another country, the legal jurisdiction is not very clear. Attackers are taking advantage of these loopholes in the system. Now, government agencies as well as large enterprises are forming new strategies to fight cyber warfare attacks.

Comprehensive Security Strategy

From the description of APT and the example, it is clear that it is very different from traditional attacks. They are a sequence of multiple attacks at different levels with a specific target. It uses technology, information, and people.

Since the problem is multi-faceted, the solution also needs to be at multiple levels. The traditional approach to security cannot defend against these sophisticated attacks. The defense mechanism should be intelligent enough to detect and stop an advanced attack. The solution can be broadly designed around three factors; technology, process, and people.



Technology

Traditional Security is not enough

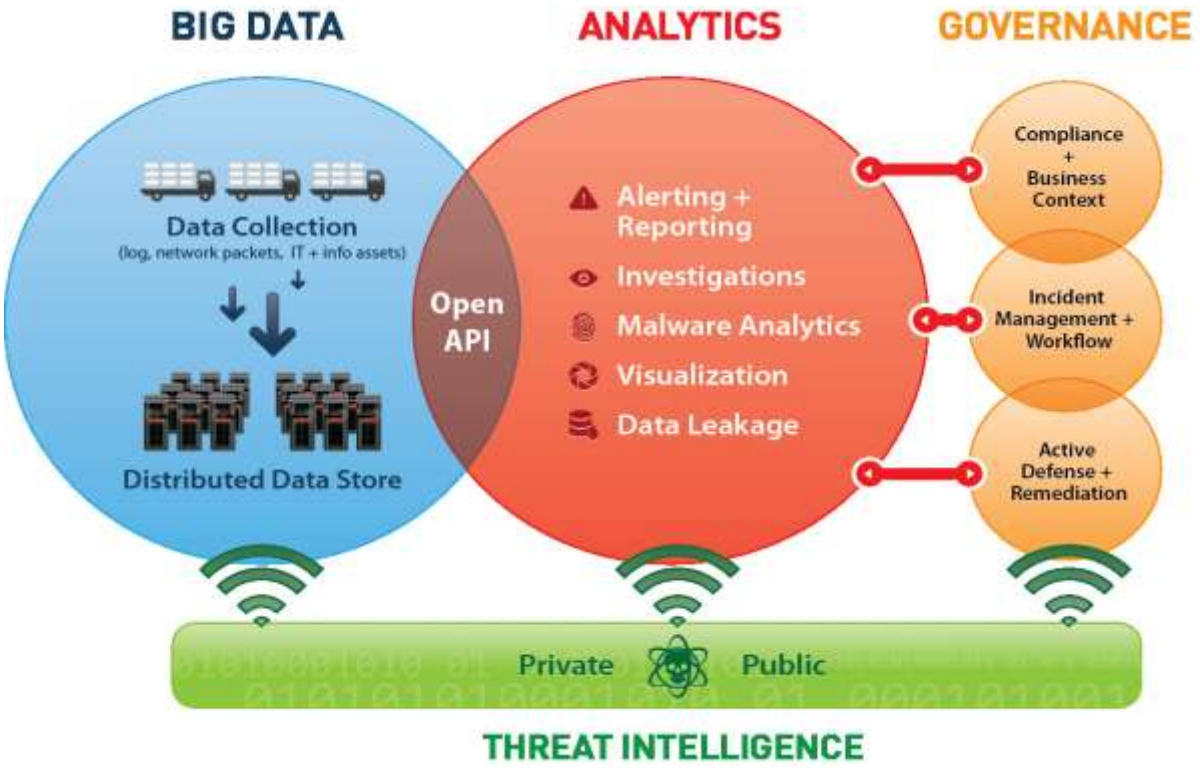
Technology infrastructure of an organization consists of various components through which the information flows—mainly servers, network, storage, and end points such as desktops, laptops, and mobile devices. Traditional security software includes firewall, anti-malware, Intrusion Prevention Software (IPS), Data Loss Prevention (DLP) software, Encryption software, and so on. While they might be able to detect a single sequence of intrusion or an attack, these tools lack the intelligence to track all the activities in an IT ecosystem and detect an advanced attack.

Security Analytics - Security meets Big Data

Security Analytics, the emerging solution to detect and prevent an APT, uses big data analytics to analyze security data and derive actionable intelligence from them. It can help in linking a sequence of suspicious activities which might seem unrelated and finding a pattern of attack.

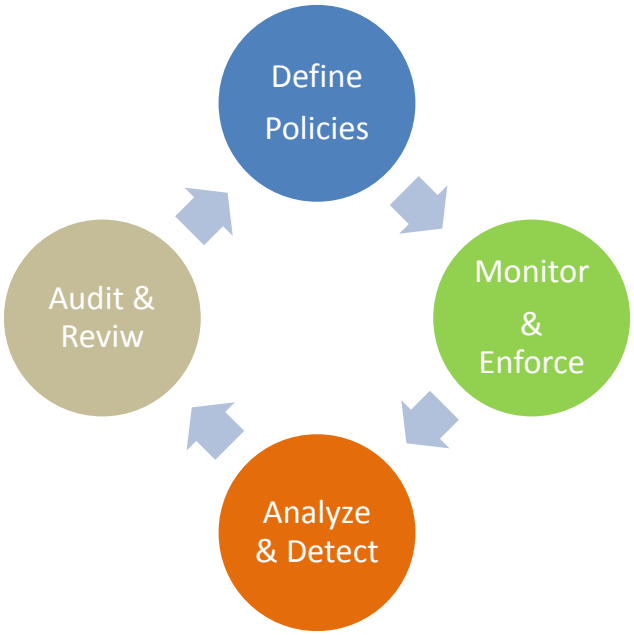
Traditional security products may not be able detect an APT themselves. But, they are still useful to collect data about various components in the infrastructure and to enforce policies.

Logs from firewall, anti-virus products, intrusion detection systems, access management software, and so forth can provide voluminous data about various activities at different component levels. Security Analytics is equipped with the technology to mine these data and get useful information. Also, it gives a complete view of an organization's information infrastructure. The figure below depicts an overview of how Big Data Analytics can help in analyzing the logs and other information from traditional security products and detecting an attack.[3]



Process

From the above section, it is understood that there is no single technology solution for detecting and preventing APT. However, with the help of a wide range of security solutions and analytics, a solution can be developed. But, deploying the technology itself will not be sufficient. The organization should have a dynamic self-learning process in place to ensure that all the security policies are being enforced and are being reviewed and modified periodically. Below is a simple framework which covers the fundamental aspects of security management and governance.



Define

Defining the security policy is the first step in security management. Security policy dictates what role security plays within the organization. It can be an organizational policy, an issue-specific policy, or a system-specific policy.

As part of security policy, define a list of approved software which is tested by the security specialists for vulnerabilities. This is required because the attacker may exploit the vulnerabilities in third party software. It is also necessary to have a hot fix and patch management policy which ensures that the software patches are deployed as quickly as possible to every single system in the IT ecosystem to reduce the possibility of a zero-day attack.

This phase will also include setting individual security product policies such as firewall, anti-malware, IPS, DLP software, Encryption software, and so on. This might require the administrator to set policies in each product or the vendors may provide a unified management console which can make the security administrator's job easier.

GRC (Governance, Risk Management and Compliance) software such as RSA Archer help organizations build an efficient, collaborative enterprise governance, risk, and compliance program across IT, finance, operations, and legal domains. The next three phases in the framework focus on implementing the policies and monitoring the adherence to them.

Monitor and Enforce

This step will ensure that the policies defined in the above step will be enforced. The various security products deployed in the infrastructure monitor for all known threats and also take preemptive measures to stop intrusion or any malicious activities based on various heuristics-based methods.

This step also includes identifying the systems which do not have the latest patches and security software signatures and taking immediate action. Security Management tools can help view the entire network and find the systems which are not in line with the policies defined in the first step. For example, a laptop which does not have the latest anti-virus signature or a server which does not have the latest patch of the OS installed. The administrator should ensure that these systems will be brought to the required specifications, manually or automatically using scripts or third party software deployment tools.

Analyze and Detect

In today's security landscape, new threats emerge frequently. The traditional security software deployed will not be able to detect a sequence of malicious activity pointing to a bigger threat. Hence, analyzing the activities in the infrastructure through logs or other data can help detect the advanced threats. For example, if a user has tried to access a resource for which he/she did not have access according to RSA Access Manager logs, search for the same in the DLP Datacenter report to see if that resource was identified as sensitive. If yes, investigate this incident further.

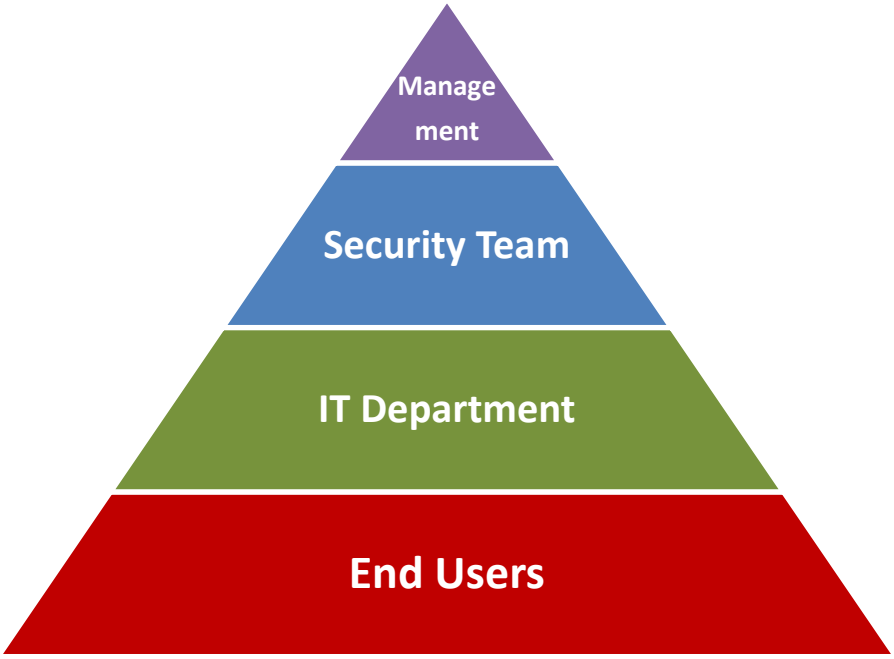
Analyzing the security data requires a team of security analyst specialists responsible for analyzing the activities going on within the IT infrastructure in real time. Traditional Security Incident and Event Management (SIEM) software is a first step towards this. Big Data analytics of the security data (Security Analytics) is an emerging trend as the data collected is very large and requires advanced analytics capability.

Audit and Review

It is essential to be alert and modify the policies based on emerging threats. This step will involve auditing the logs, policies, and procedures to check for compliance and also review if the defined policies and the enforcement mechanisms are fulfilling the security requirements of the organization. The recommendations from this stage will again be fed to the first step, completing a full circle.

People

People play an important role in the war against advanced threats. A security infrastructure is only as strong as its weakest link. Despite having strong technologies and policies in place, security can still be compromised due to a single action of an individual. The pyramid below shows the different types of users from the security perspective.



While security policies, standards, procedures, baselines, and guidelines are often formed to meet the regulatory requirements, they may not be enforced completely. To effectively enforce these, it must be clear that the directives came from senior management and that the full management staff supports these policies. Hence, the management is placed on top of the pyramid. The security awareness should be driven top down.

The security team headed by a Chief Information Security Officer (CISO) is responsible for developing the security policies and making decisions on which security products to install. Often, the security analytics team also will be a part of the security team.

The IT department responsible for the deployment and maintenance of the entire infrastructure also has an important role in the security lifecycle. The administrators of servers, databases, and other enterprise IT assets should understand the security implications and follow the highest set of precautions against a possible attack.

Finally, the majority of people in an organization fall into the End User group. End users must understand what is expected of them in their actions, behaviors, accountability, and performance. An end user falling prey to a phishing attempt is an entry point for an advanced threat. Hence, end users should be educated and be aware of the security policies and the intension behind them.

Conclusion

Biological evolution confirmed that only the species which adapt to change and respond to the changing ecosystem around it survive. Similarly, organizations which are alert and respond to the changing security landscape can survive in the long run. Given that, the only way to fight the cyber war is to continuously learn and evolve. Technology, process, and people play a key role in defending the organization against advanced security threats.

Appendix A

Glossary

GRC – Governance, risk management, and compliance, includes activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.

Heuristics – refers to experience-based techniques for problem solving, learning, and discovery.

Man-in-the-middle attack –a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Phishing – tricking individuals into disclosing sensitive personal information through deceptive means.

Root kit – a stealthy type of software, often malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

RSA Access Manager – access management software from RSA, the Security Division of EMC which implements role-based access management solutions in an enterprise environment.

RSA Archer – Governance, risk, and compliance product from RSA, the Security Division of EMC.

RSA DLP Data Center – Data Loss Prevention solution from RSA, the Security Division of EMC which can scan servers and databases for the existence of sensitive content.

SCADA (Supervisory Control and Data Acquisition) – a type of industrial control system (ICS). Industrial control systems are computer-controlled systems that monitor and control industrial processes that exist in the physical world.

Spam – The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

WinCC – SIMATIC WinCC is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) system from Siemens.

Worm – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Appendix B

Bibliography

1. "Obama Order Sped Up Wave of Cyberattacks Against Iran". The New York Times.
2. http://en.wikipedia.org/wiki/Cyberwarfare
3. http://www.rsa.com/products/envision/sb/11737_87640-h9093-impsa-sb.pdf
4. http://hackmageddon.com/2012/10/19/a-0-day-attack-lasts-on-average-10-months/
5. http://ebiquity.umbc.edu/blogger/2010/09/23/is-stuxnet-a-cyber-weapon-aimed-at-an-iranian-nuclear-site/
6. http://en.wikipedia.org/wiki/Stuxnet