Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-07
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Overcoming Cyber Security gap

[1]YaminiPurnaTilak Jakka,Faculty P.G. Dept of Computer Science, TJPS College, Guntur, yamini.jakka@yahoo.co.in
[2]Suneetha Akula, Faculty P.G. Dept of Computer Science, TJPS College, Guntur, asunitha24@gmail.com

ABSTRACT

Now a days the majority of successful threats are increasing. Majority of hackers take control of security systems, by deactivating antivirus software's and others. Antivirus and firewall tools are not enough to combat such threats. Cyber attacks have victimized private sector economic targets: law firms, investment banks, oil companies, drug makers, technology manufacturers and etc.

In recent years cyber threats pose a clear and present danger to Wall Street, Major law firms, technology companies and other key components of the economic engine. Cyber crime is a never ending battle of one up man ship between the hackers and those that stand between them and their potential victims.

Cyber Security solution providers are the first to admit that technology by itself doesn't solve the problem. Products tend to be programmed only for specific threat vectors. It always takes human intervention to restore systems to normal after a breach occurs. The damage suffered by an enterprise depends largely on how long the cyber threat remained undiscovered and unaddressed.

My paper presents the concept on Active Threat Protection (ATP), which offers a way to close the gap. ATP Combines advanced security software with human expertise. It also defends existing traditional cyber security by protecting enterprises against previously unknown threats even those that eluded other security defenses. ATP guides in immediate occurrence of threat of various types of threats.

My work verifies that, Security influences an organizational developmental process. It is increasingly recognized that there exist a relationship between security and development. ATP is the future of cyber security; all enterprises should possess comprehensive protection possible.

Key words: Security, Firewall, Threat, Network

INTRODUCTION

Many firms follow internet and other new technologies to improve the quality of service and efficiency. This has created an opportunity for criminals who attempt for our personal and business secrets. They gain access on resources and create awful situations to organizations. Many employees inappropriately download data from organization for later use at their new companies. It is worse to say that data breaches go unexplored for months or years. Some of the victim organizations rarely discover these threats. This type of security incidents raise questions about firm's ability to respond to critical incidents.

In today's world, breaches and threats are more likely begin internally. The majority of these internal cases are not malicious. As employees gain more access to more information and public file sharing tools, the risk increases that sensitive information can some how end up in wrong hands.

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Beyond implementing firewalls and anti-virus programs, firms must look beyond perimeter deface to evaluate potential security risks.

Firms must be proactive to manage security properly. Conducting a vulnerability assessment is a great way to test the threat level for your firm and it gives the necessary steps to combat the issues. They often expose malicious activity previously undetected.

Even simple security best practices can go a long way in alleviating troublesome and costly threats down the road. Most of the common security problems come from out-of-date network and anti-virus patches, application updates and internet browser activity.

ATTACKING WAYS

Attackers choose mainly three ways from an internal perpective. One of the most common ways used by cyber criminals was malicious content emails. By sending this type of malicious content emails through network they can infiltrate data. The second way was malicious content received while surfing the Internet ('By Download'). The third way was malicious content received through a lateral connection (an infected USB drive, CD/DVD, Or from another infected system connected to the network) . By using all these techniques cyber cirminals penetrate data about firm's security systems and will disarm antivirus and fire walls. Combating such threats is not possible by using firewalls and antivirus. Apart from these threats some threats will arise from employees . In this evolving environment, all firms need to carefully consider how to best address cyber security issues, including those that arise due to their reliance on service providers. In addition, firms need to design protections for investor and employee personal data, and firms that rely upon proprietary technology may require additional protections. Responding to a Cyber Attack Or Data Breach, A systems/technology assessment accompanied by a management effort to address business side concerns. (1) Organizations should keep a team to address the crucial tasks. (2) Gather the facts necessary to make an appropriate response. (3) Communication should be done with stake holders in a regular basis. (4) Make any appropriate technology fixes, (5) Verify that any fixes have fully addressed the issue, and(6) future problems also be assessed and should take necessary actions. Team size will depend upon organizations size. One team is enough for small firms and it needs two for large one.

Protecting yourself from Cyber Attacks have evolved from the high volume, low value (nuisance). Threats such as chain emails and spam to low volume (targeted), high value attacks all too common in firms with valuable assets such as investment research, patent applications, and mergers and acquisitions documents.

To Protect against malware and hacking

- ✓ Checking must be done whether the firewall and antivirus is correctly working or not, network servers and directories are secured with strong passwords, etc.
- ✓ Providing access to valuable data to employees should be done carefully. All the directories and files should be secured with passwords.
- ✓ An Acceptable Usage Policy (AUP) must be developed. It provides guidelines on using personal devices, cloud based mails

and downloading software. Employees should be trained on AUP procedures.

- ✓ Highly protected data should not keep on unsecured servers. Accessing of data should be given to those employees who need to work on that.
- ✓ Cyber security risk will increase or decrease according to the service providers. So service provider's scope should be checked carefully.
- ✓ Ensure that a separate network segment for Internet---accessible Systems is enforced. Even If someone is able to break into a system in the DMZ, Their access to the inside will be hobbled.
- ✓ Account names of administrator should be unknown.
- ✓ Ports that are not required should be disabled.
- ✓ Log history should be maintained to pay attention on authentication failures, especially for high profile users.
- ✓ Default access ports should be changed. HTTPS is carried over tcp/443, but it is not important to maintain that port constantly. We can change even if we have a SSL---Enabled VPN, by changing the port from tcp/443 to tcp/14433, Due to this we are not exposed to external entities those are performing broad scanning against the default ports.
- ✓ Consider Outsourcing web and email servers to a third party. For example hosted web servers and email servers generally have better performance and higher availability and they are two primary attack points. This Approach can segregate attack vectors and prevent a breach in one to escalate to others.
- ✓ Scanning should be done if any suspect found. Regular checking is important for finding vulnerabilities.

Active Threat Protection

Active Threat Protection closes the above gaps. ATP is one of the best way to protect the organizaitons confidential data.

Active Threat Protection has four capabilites which are very essential.

First, network events information should be known completely. This Means getting real time data straight "from the wire." This is known as ACTIVE ANALYTICS in network interceptor, A capability that finds both known and previously unknown threats.

Second, ACTIVE FORENSICS "operationalizes" event data. Software Tools and dashboards find out false positives while increasing bonafide threats.

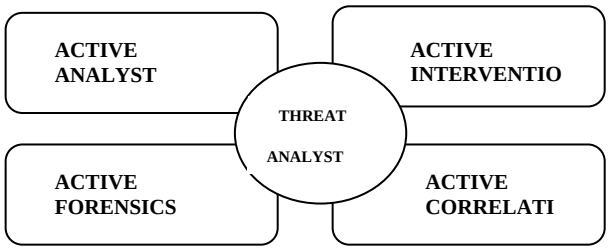
Third, When an incedent happens according to security then ACTIVE INTERVENTION will be done by security experts. They will assist you when you need and will act as an extention of IT team.

Fourth, The log based data already being captured by traditional security automation is still important. ACTIVE CORRELATION increases its value by aggregating it into the Active Forensics Database.

This Framework combines advanced detection technology with human expertise and is the only way to close gaps inherent to traditional security automation.

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Active threat protection is different from many other protection policies. Some of the features of ATP explains how it differs from other security guards.



Active Analytics Network Interceptor's possess some of these capabilites.

Direct Event Scrutiny There is no waiting for device logs to be aggregated and normalized. Network Interceptor Sits "on the wire," gathering a richer set of traffic data, and supplying crucial information to the Active Forensics Database.

Identifing Through Behaviour Each threat behaves in a different way , this makes network interceptor to identify the threats. Through this network interceptor find the threats where other systems miss.

Immediate Proscription These are used to stop attacks in their tracks using their remediation tactics which are already arranged.

Active Forensics Active Forensics Combines rich network event data and interpretive technology to pinpoint bona fide security threats. It is "operationalized" for an advanced tool set that security experts leverage to rapidly research and remediate cyber threats:

Active Forensics Database It consists of network event data for security systems. It consists of a richer information and is a key source for extending the traditional security systems.

Intelligent Threat Annotator This is used for finding the events that are truly need attention.This will apply software algorithms to the active Forensics Database for eliminating fake events.

Network Event Traceability By using this tool we can trace the series of related events to gain actionable information. With out this advanced tool the information is unobtainable.

Active Intervention To address the problems of security attacks, security experts are the only way who can access the Active Forensics. Active Intervention Extends the your IT Team with deep subject matter expertise precisely when it is most needed. Without Active Intervention, Many firms use "set and forget" technology. But it is not correct solution for attacks, when any attack occurs then they will get an "it's not my problem" message. Active Intervention solve these business risks and decrease these gaps.

Active Correlation

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Traditional Event logs have great value. Active Correlation supply data to the Active Forensics along with some security products and devices. There are some services which are provided by Active Correlation :

Log Sentry This service is used for checking and collecting log events, detecting anomalies and gives the data to the Active Forensics Database. It is used to support compliance monitoring and reporting.

Asset Manager Protect

This Service correlates threat data across a broad community of user companies, enabling Network Interceptor to prevent attacks from malicious sites when a threat emerges at just one community member's company.

Continuous Security Mode This service will do regular checking and penetration tensting. This will provide continuous vulnerability management. It closes the window left open by vulnerability assessments that are done only an annual or semiannual basis.

Conclusion

Few of these cyber security protections have been applied in vaious organizations.

Some of protection methods are in research stages.

References

- www.extremenetworks.com/
- http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm
- http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html
- https://www.tofinosecurity.com/why/network-threats
- http://www.arbornetworks.com/resources/infrastructure-security-report
- http://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats/facebook.aspx
- http://www.interhack.net/pubs/network-security/
- http://www.crn.com/slide-shows/security/240002785/7-security-threats-circling-your-network.htm