ABSTRACT

A hybrid deployment of IDS and IPS on the organizational network is best practice. This paper describes the importance of defense in depth and security best practices and provides suggestions of IDS and IPS hybrid solutions that should be employed by organizations for their internal IT infrastructure.

Keywords: Intrusion Detection, hybrid, defense in depth

INTRODUCTION

Most of organizations have cyber security requirements that must be considered, measured and completed to protect the data and assets of the organization. Risks, threats, and vulnerabilities are real time problems in today’s interconnected web world. Cyber-attacks take place against governments, businesses and even individuals; therefore no party and/or organization is immune and must work together to be part of a solution (versus the problem). In fact, over the past 12 years, the growth of incidents reported to CERT Coordination Center (Carnegie Mellon Cyber Security Research Program) has paralleled the Internet’s explosive growth (McHugh & Allen 2000). As a protective measure, it is imperative that organizations follow best practices of Cyber Security (in light of security needs and available resources). Unfortunately, there are several vulnerability scanning and probing tools available for free to anyone with any intentions. One method cannot protect a network completely. Hackers will always develop new or progressive methods to gain a proprietary or financial gain from organizational networks. By The above statement does not imply that anyone and/or organization are complacent in implementing security practices.

There are many uses of technology employed by organizations. A calculated approach must be used to determine whether organizations should invest in cyber security infrastructure. It is incumbent upon the IT professionals to research and empower management with information required to protect the organization in light of policies, resources and procedures of same. Regardless of the financial and human capital resources of an organization; there are fundamental doctrines essential for best cyber security practices that serve to defend networks. Best practices include a layered defense with an in-depth approach for network infrastructure.
DEFENSE-IN-DEPTH AND BEST PRACTICES OF CYBER SECURITY

The Model

What is practicing a defense-in-depth approach on an organization’s network? Defense in-depth is defined as a best practice, practical approach for achieving information assurance in highly networked environments by relying upon techniques and technologies available in today’s computing environment (Small, 2011). Practice begins with appropriate, effective and well-tailored security policies to help ensure threats to critical organizational assets are described and understood by all involved parties (McHugh, Christie, & Allen, 2000). A complete, thorough security policy contains or references some of the following policies: Human Resources Policy to address security breaches, Password Change Policy to enforce selection of robust passwords, Privacy and Acceptable Use Policies, Change Management policies, etc. (Security Documentation Facts 2009). Most importantly, the security policy addresses training of employees on the protection and usage of assets and reflects the goals and ambitions of the organization. Once a policy is implemented, the defense in-depth layered model grows exponentially to encompass the organization as a whole addressing both foreseen and unforeseen events. In front of diverse and layered security mechanisms, the attacker is required to circumvent every individual layer in order to gain access to the data or the network, thus preventing a single point of security failure (Barnum & Gegick, 2005). Organization cannot solely rely on a single security mechanism to protect the network in its entirety.

![Defense-in-Depth Model](image)

**Figure 1 Defense-in-Depth Model**

The Defense-in-Depth model is layered like an onion. Each layer that is breached; another layer of the onion is removed thus invoking more tears from the “hacker” with each layer peeled off and rendering the attack unsustainable. The first layers of the “onion” are the access control layer and the physical security layer. Within the physical security layer, the hacker will encounter...
controls such as locks, lighting, building layout, doors, key pads, fences, surveillance cameras etc. Once the initial physical security layer has been breached, the second and third inter-related layers known as the access control and authentication layers are presented. Access control methods are crafted to protect an organization’s computer and data resources from unauthorized access and/or tampering from both inside and outside threats. Access control comes in three types of control: administrative, technical and physical (Harris, 2010). Administrative controls domain is dominated by security policy whereas the technical controls domain consists of software applications and settings to restrict users’ access to objects, such as operating systems, network access and architecture (Harris, 2010).

Lastly, the physical domain of access controls contains locks, mantraps, cameras, guards, etc. The third layer known as authentication is the use of a user name and password and one other authentication factor employed by the organization’s users to access the network and/or data resources. The use of a user name, password and a token or a biometric device is deployed on these two layers to frustrate unauthorized users from accessing the system. The authentication methods are used in cooperation with access control settings (such as ACLs, Group Policy and firewall settings, etc.) to determine what resources can be accessed by the user.

The fourth layer of the Defense-in-Depth model is known as the segmentation layer. Actions of the layer entails portioning the network into segments from other segments of the network to provide additional security protections including but not limited to: the protection of a vital server or host on another network segment, segmenting off a virus laden portion via the creation of multi-layer security on the network layer, including the deployment of multiple firewall subnets, a DMZ (demilitarized zone), etc. (Bragg, Rhodes-Ousley, & Strassberg, 2004). For example, on the segmentation layer of the Defense-in-Depth model, an IPS/IDS hardware or software device can be placed on a different segment of the network to provide protection to the individual resource. The fifth and sixth layers of the “onion” are also interrelated and are known as auditing and monitoring layers. The auditing and monitoring layers must imperatively use an IDS and/or IT professionals use audit logs produced by software/hardware to monitor the network for any anomalies in traffic, patterns or attachments. Audit trails can be layered with local system logs used in conjunction with network activity logs, such as firewall penetration attempts, dropped IP address logs, etc. (Bragg, Rhodes-Ousley, & Strassberg, 2004)

**Examples and considerations to model usage**

As illustrated above, deploying a layered security infrastructure is very advantageous and even more so with the employment of an IDS and/or IPS (McHugh, Christie, & Allen, 2000). A real life example of using a layered defense would be a network deployed with a packet filtering firewall on one segment with an IDS behind same with a switch to route the traffic once the packets have traveled through the firewall and IDS. Other defensive methods that may be used include , but are not limited to: application of patches, elimination of unnecessary services, usage of file integrity checking tools, deployment of firewalls, security guards, etc. (McHugh, Christie, & Allen, 2000). Ultimately, employment of the defense-in-depth strategy requires that an organization strike a weighted balance between operational needs, network performance, protection requirements and overall costs (between actual equipment outlay and human capital usage). All too often organizations are faced with resource limitations such as IT overhead availability, budgetary or process limitations (Small, 2011). It is absolutely imperative that the
IT professional have approval and support of upper management in implementing the security measures best fit for the organization. Also noteworthy, IT professionals of an organization must be familiar with and use timely methods and technologies in order to attempt to “keep up or stay ahead” of hackers and malicious users. Sadly, this proves to be a very daunting because the attackers have access to the same tools, technologies, resources, etc. as the IT professional. Attackers sometimes have more financial and human capital resources; forming alliances with other hacker groups. A recent example in the media highlights this reality with the known hacker group “Anonymous” The group targeted the Israel government in a “cyberwar.” (Sutter, 2012) Other known attacks by the same hacker group include targeted attacks on godaddy.com, Stafford (security based firm), law enforcement, etc. Law enforcement agencies around the world (including Interpol police) are on their toes trying to apprehend members of this publicized, world-wide organized movement.

**INTRUSION DETECTION AND INTRUSION PREVENTION SYSTEMS**

The main goals of an IPS/IDS are to bolster the security posture of the network and assist associated IT staff in preparation for attacks by collecting information from a variety of systems and network sources and by analyzing the information of possible security vulnerabilities and problems (Rozenblum, 2001). In general, an IDS/IPS system provides the following information, but is not limited to: monitoring and analysis of the user and system activity, auditing information of system configurations and vulnerabilities, assessing of critical system and data files, analysis of traffic patterns based on matching known attacks (based on detection type), abnormal activity audit (based on detection type) and/or operating system audits (Rozenblum, 2001). Obviously, having a hardware and/or software device providing this information to IT professionals of an organization is highly beneficial knowing the weaknesses of the network infrastructure and mitigating same. As with many technologies (to meet the varied challenges proposed by the computing environment), there are variations with IPS/IDS technology to assist in tailoring for appropriate fit of the network. Intrusion Detection and Prevention Systems narrowed down by its main action—whether the device is hardware or software based and whether it detects and alerts or detects and prevents malicious traffic/attacks. Both systems, IDS and IPS, can either be a dedicated hardware device that is physically placed on a network or a software based device loaded onto another physical device. The detection and response method employed by the device is determinative of type.

**IDS defined**

An IDS is an installed piece of hardware or software that monitors network traffic to detect unwanted or unauthorized activity and events such as malicious traffic or traffic in violation of the security policies and settings in place (Wu, 2009). IDS creates and stores an event log for IT staff reference and analysis. Essentially, the IDS device is passive and watches packets of data traverse the network from a monitoring port and compares the traffic to the configured rules (IDS vs. IPS Explained, 2010). If the IDS detects abnormal or malicious traffic, it will initiate an alarm to notify the system administrators to take action (the device itself does not initiate the action). The IDS is used as a compliment to the firewall since the firewall alone is not sufficient on its own. Relating back to the defense-in-depth model, simply using a firewall alone would create a single point of security failure if breached. Therefore, IDS must be used in
conjunction with the firewall to mitigate a single point of failure and to create a layered preventative approach. IDS can detect traffic and activities that may escape detection by the firewall, including but not limited to: Trojan Horse viruses, worms, attacks against particular network services, data attacks, host based attacks (such as unauthorized login access), etc. (IDS vs. IPS Explained, 2010).

**IPS defined**

When the blocking capabilities of a firewall are combined with the deep packet inspection scanning settings (described below) of an IDS, the result is an IPS (Desai, 2010). An IPS is defined as any proactive hardware or software device that has the ability to detect both known and unknown attacks and prevent same from being successful (Desai, 2010). The key difference to note is that the IPS can actually stop the traffic or behavior without system administrator interaction. Mitigating actions performed by the IPS include, but are not limited to: blocking an attack, terminating network connection or user session originating the attack, reconfiguring other security devices (firewall, router), applying necessary patches, blocking access to the targeted computer, data and/or application, etc. (IDS vs. IPS Explained, 2010). As such, the IPS is a proactive security tool vs. the passive IDS and is an evolution of IDS.

**IPS/IDS detection methods and components**

There are three detection methods employed by an IPS/IDS to detect malicious traffic on the network or host. Each type of detection has known positives attributes and drawbacks to usage and abilities of same. Signature-based detection, used frequently, relies upon known traffic data to analyze all traffic and to detect unwanted traffic (Wu, 2009). This detection method, while fast and easy to set up and maintain, is limited in its detection capability because a hacker can change the method of attack and overcome detection. Essentially, this type of detection functions by the use of pre-defined rules (or attack signature) that is entered by a system administrator on the device to screen traffic based upon the signature of the traffic that traverses the IDS/IPS (based upon already discovered and known malicious traffic signatures). This method of scanning is considered reliable; however as noted above, can be overtaken if the hacker is inspired to do so.

The second type of detection, known as anomaly-based detection, is IDS/IPS scanning of network traffic and detecting data that is not valid or is abnormal or atypical (Wu, 2009). This sort of detection method is great for detecting unknown and atypical traffic as it traverses the network. Rules for scanning are pre-defined by the system administrator based upon typical behavior patterns of the network and traffic traversing same in order to signal out traffic that does not look like “it belongs” or is atypical. For example, this method can detect TCP/IP packets traversing the network that do not have the normal shape or appearance as regular packets. Anomaly-based detectors equate unusual or abnormal traffic with intrusions and are able to recognize novel attacks (McHugh, Christie, & Allen, 2000). However, all abnormal traffic may not be recognized as a hacker can disguise same to make it look authentic.

The third type of detection, known as Stateful Protocol Inspection, works in a manner similar to anomaly-based detection; however it scans on deeper levels to analyze traffic at the network and transport layer and at a vendor level (relies upon vendor developed profiles on how protocols are used) to analyze traffic at the application layer (Wu, 2009). As such, this inspection examines
each and every packet as it comes through the network firewall. Stateful protocol analysis is used to compare predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations (Scarfone & Mell, 2007). While this scanning type would be more intensive, a cited drawback impacts network resources availability and IT overhead for maintenance of same.

There are common universal components of an IDS/IPS regardless if it is hardware or software based. The IDS/IPS must have a way to collect traffic (packets); therefore sensors are used to collect network packets, log files and system call traces then forwards all data to one of the analyzers (Wu, 2009). The second required component is an analyzer. The analyzer is used to collect data from the IDS/IPS sensor to determine if an intrusion has occurred. Within an IPS, the sensors and the analyzer would take mitigating steps to prevent and limit the intrusion.

Within the IDS, these two components would notify the IT staff. There is also a user interface to simplify the interaction between end user and device (control and configure same). As an optional deployment to an IDS/IPS, the system administrator may also choose to install a “honey pot” (decoy system) used to attract attackers from the legitimate network.

HYBRID DEPLOYMENTS OF INTRUSION DETECTION AND INTRUSION PREVENTION SYSTEMS

The IDS/IPS can be deployed in various manners with the actual placement of hardware or software device determinative of device usage. The three locations of determinative iterations of IDS/IPS are as follows: Network IDS and IPS (hereinafter referred to as “NIDS” and “NIPS”), Wireless IDS (hereinafter referred to as “WIDS”), Host-Based IDS and IPS (hereinafter referred to as “HIPS” and “HIDS”). NIDS and NIPS are hardware or software based devices placed on the network to scan traffic and notify or react accordingly. WIDS is placed on the wireless network and is used to monitor for typical network traffic attacks as well as attacks specific to wireless networks (Wu, 2009). Lastly, HIDS and HIPS are placed on a specific host (i.e. critical database or server) to detect network and/or host based attacks and react accordingly (Wu, 2009). Due to the fact that IDS and IPS devices reside on different points on the network, said devices should be used concurrently to help prevent attacks such as worms and viruses (Wu, 2009).

How should the organization capitalize upon these devices within the defense-in-depth framework? The answer lies in constructing a hybrid topology infrastructure. Using a hybrid deployment, an organization will be able to benefit from the latest technology provided by an IPS while also using proven and mature capabilities of an IDS (Holland, 2004). It must be noted, that any IDS/IPS device must be coupled with a patching and with an antivirus updating plan on the network. Many companies place a NIDS on the perimeter of the network either between the border router and firewall or it is placed outside of the border router (Holland, 2004). If the IDS is placed on the outside perimeter as a first line of defense, the device will be bombarded with traffic (malicious and benign). A wise investment for an organization to use a NIPS on the network, directly behind the firewall (in-line deployment) to provide protection to the enterprise on a whole. By having the NIDS or NIPS placed in this very position, all traffic that is permitted through the firewall will go through the NIDS or NIPS. In addition, the organization should deploy other IDS/IPS options throughout the network infrastructure to create cyber security best practices layered effect.
Another hybrid deployment approach is to use a HIDS on a critical system to catch any errant traffic that has escaped earlier detection coupled with a NIPS configuration noted above. A HIDS should be deployed on any segmented portions of the network that are critical. The host-based system operates on a protected system to inspect and/or audit the log data to detect any intrusive behavior, regardless of whether or not the NIDS or NIPS is working on the perimeter (McHugh, Christie, & Allen, 2000). The choice of a HIDS or a HIPS is all dependent upon the assets to be protected and the available resources.

Lastly, a newer use of a hybrid IDS/IPS security infrastructure would end the use of virtual servers and VLANS (virtual segmentation) on a network. Many organizations use virtual infrastructures and platforms (such as VMWare) to create “virtual” machines and servers within physical infrastructure. This practice is frugal in terms of saving money for the organization on physical assets and resources, utilities (such as power) and company overhead. An additional virtual segment, known as a VLAN, can be formed on physical network resources within the organization. Typically, any software that can run on an actual physical environment can run in a virtual environment, including software based HIDS and/or HIPS. As such, the organization can segment critical servers or other parts of the network to a VLAN (or create virtual servers) and deploy IDS/IPS software on same. This practice adds another layer of protection for critical assets and insulates the other part of the physical network from same.

CONCLUSION

In conclusion, there are many options that should be deployed within an organization in light of the defense-in-depth layered model of cyber security. The over reliance on a firewall or an IPS alone can be detrimental to the organization. Accordingly, an IDS/IPS should be an accompaniment to a firewall, the physical controls, access/authentication controls and other deployments to prevent a single point of security failure. In order to save money and segment the network, the organization should consider VLANS and virtual servers in contrast to all physical hardware. The hybrid placement of IDS and IPS devices is very dependent upon the resources and goals of the organization and criticality of the network being protected. Lastly, the key to the entire cyber security infrastructure is employee training and organizational commitment to enforce a comprehensive security policy.
REFERENCES


