Cyberoam

Unified Threat Management

White Paper

Threat Precedes Intrusion Paradigm Shift in IDP Technology

- Preface 2
- Only a Valid Threat matures to Intrusion 2
- Calibration of a Threat 2
- A Case of False Positives 3
- Internal Threat Case Scenario 3
- Internal Intruder's Identity Crisis 4
- Granular Approach for External Threat 4
- Internal Intruder's Identity Crisis Solved 4
- Summary 4

Preface

The concept of Intrusion Detection and Prevention Device (IDP) has been around for nearly twenty years but only recently has it seen a dramatic rise in popularity. In a world where boundaries tend to blur, keeping and maintaining a private space is a demanding task. Intrusion into the computer networks has haunted almost every enterprise, big and small.

During 2005, financial services giant Citigroup and media powerhouse Time Warner had sensitive data swiped from their "supposedly secure" databases. Smaller companies like Retailer DSW Shoe Warehouse and credit card processor CardSystems, were victims of cyber break-ins. The most disturbing threat that came to light was the fact that an insider was a party to these thefts. These internal threats are likely to grow in 2006, forcing more companies to add a layer to their network that will monitor the information accessed and distributed by employees. This has been the primary rationale behind having a multi-layer security approach like UTM, rather than having diverse applications trying to provide a "seemingly comprehensive" security cover.

During 2005, financial services giant Citigroup and media powerhouse Time Warner had sensitive data swiped from their "supposedly secure" databases.

The seminal concept of intrusion detection and prevention was born in 1980 with James Anderson's paper, Computer Security Threat Monitoring and Surveillance. However, in the modern times, an IDP blended into a Unified Threat Management (UTM) system definitely has an edge over its stand-alone counterparts.

From being a passive reporting tool called Intrusion Detection Systems (IDS) the current solutions have matured into Intrusion Detection and Prevention (IDP) tools, which not only detect an intrusion, but also launch a counter-offensive. In spite of being around for nearly twenty years the IDP technology is yet to mature. Intrusion is the final result of an initial threat. If a valid threat is detected and countered on time, intrusion is nipped in the bud. So, the perception of a valid threat gains importance over the actual intrusion.

The degree, intensity and danger of a threat can only be calibrated by an IDP, if the origin, destination and nature of a threat are accessed correctly, on time.

Only a Valid Threat matures to Intrusion

Perception of a valid threat is the panacea for the IDP technology. An event has to be has to be evaluated from different aspects to be actually classified as a "Valid Threat." Humans are often able to distinguish between similar situations and gauge the degree of threat, but to translate the same ability to a machine is a daunting task. To classify an event as a possible threat, the IDP has to be sensitized to a number of parameters.

An intrusion is a final result, which is preceded by a threat. If a threat is perceived on time and blocked, the intrusion can be nipped in the bud. Simultaneously, in a bid to refine the threat perception mechanism, the IDP should refrain from generating false positives. On the other hand, an overlooked legitimate threat can mature into an intrusion.

In real life: a cardboard knife in the hands of a stranger and a kid carrying a real knife are two different situations. The perception of the knife only, is not important, rather a holistic view of the complete situation is much more relevant in the calibration of a threat.

An intrusion is a final result, which is preceded by a threat.

Calibration of a Threat

The degree, intensity and danger of a threat can only be calibrated by an IDP, if the origin, destination and nature of a threat are accessed correctly, on time. Only after a threat is correctly calibrated, can an appropriate and customized counter-offensive be mounted. In case of an internal threat, especially the identity of the user become very important as it leads to the correct understanding of an internal event in a network.

To understand the perception of a threat, we will examine some real life scenarios.

External Threat Case Scenario

If a threat is of external origin, it has two focus areas:

I. External threat posed to specific and critical DMZ/machine

In any network all the machines are not equally critical. If a threat is posed to a specific machine (e.g. DMZ, Database servers) then the critical nature of the threat escalates dramatically.

In case of such a threat, the information of its intended destination is of vast importance. The information can not only provide a unique insight into the nature of the threat but also prove critical to the decision taking ability.

Most of the IDPs would provide an administrator with strict blanket policies leading to a large number of false positives.

II. External threat to all internal nodes

In case of a general purpose external threat, a traditional IDP provides a symptomatic treatment of blocking or dropping a potential request.

A Case of False Positives

Most of the IDPs would provide an administrator with strict blanket policies, which in due course, leads to a large number of false positivesi. In such cases, IDPs are a perfect case of The Boy Who Cried Wolf. Improper blockage leads to higher maintenance on part of the system administrator. Ultimately, to remedy the situation, the filtering policies are loosened, the security compromised and the wolf welcomed.

IDP solutions are not configured to rate a threat based on its origin, destination and nature. Their response is primarily based on its nature only and so they are configured to block only "general" and "more dangerous" threats. Consequently they ignore threats that have not yet reached a critical level and are perceived to be of "Low Danger". In a nutshell, they ignore the origin and destination of a threat.

Such short-sighted IDP fails to provide proper security.

Internal Threat Case Scenario

A survey conducted in 2005 by CSO Magazine in association with the CERT Coordination center and the U.S. Secret Service showed that 36% of respondent organizations experienced unauthorized access to information systems or networks by an insider. The internal threat level clearly exceeded the 27% committed by the outsiders.

In case of an internal threat, there are two focus areas:

I. Internal threats posed to local machines in DMZ

In any network, the perimeter defense is often competent enough to mitigate an external threat. However when local critical machines like, database servers or DMZ machines are targeted by an internal threat, it often turns out to be an Achilles' heel for a traditional IDP.

It is very important to remember that, in contrast to an external threat, internal threats are not anonymous in nature, if the information is correlated correctly.

II. Any internal machine used to launch an external threat

If a network harbors or provides a platform to a threat, it is completely responsible for the consequences. The threat may be anything ranging from a malicious attack to information being stolen. An organization is always responsible for its user's behavior. Once such a threat is detected it is also mandatory for the organization to provide sufficient data to the law of the and to take its course.

Internal Intruder's Identity Crisis

The concept of internal threat has dawned quite recently in the IDP technology. It has been neglected because a traditional IDP fails to provide a "face" to it. Once the identity of an internal threat is revealed, its significance escalates dramatically. According to Hercule Poirot, the eccentric Belgian sleuth, every crime has an intention, cause or a reason. The identity leads to the reason of the threat. While most network administrator fail to detect the threat within, it is ironically easy to put a face to it. Best-of-breed IDP solution can only be possible if it is able identify individual user. Moreover, just providing the identity is not enough. The system administrator should be able to formulate customized policies for individual users or a group of users.

Granular Approach for External Threat

In case of an external threat to critical/DMZ machines, once the origin, destination and the nature of a threat is obtained, the system administrator should be able to mount a counter offensive to respond to a threat, based on its degree, intensity and danger perception.

A system administrator should intelligently be able to identify and isolate the critical machines present on a network. On identification, a customized strict policy or control should be used to ensconce them securely.

If an individual user can be isolated and be made accountable for his or her network activities, the chances of an internal intrusion can be nullified to a large extent.

In the second scenario of external threat to internal network, the IDP should be able to identify the external problem/rogue networks. These networks should then be wrapped and isolated in a strict policy or control.

In short an IDP solution should be able to identify the source, destination and nature of an attack, should be able to rate the threat based on all the three parameters and should allow the administrator to configure a counter attack.

Summary

The best-of-breed IDP should be able to nip the threat before it matures into an intrusion. It should be able to timely perceive threats and not let them mature into an intrusion. To meet all these parameters is a tough task for a stand-alone IDP. Moreover, in case, if it is able to confront an intrusion or threat on all these parameters, the overheads would be very high. If multiple security systems are deployed, they would be treading on each other's toes while scrambling for the same data. It would simply be too chaotic.

About Cyberoam

Cyberoam Unified Threat Management appliance recently announced the introduction of an advanced version of Intrusion Detection and Prevention solution. Cyberoam's Single Sign-On pinpoints the source of internal threats by the username. This ensures highest levels of security even in Wi-Fi and DHCP environments with dynamic IP allocation. Cyberoam UTM, with its multi-policy capability, allows administrators to configure different user based policies.

Cyberoam
Unified Threat Management

Elitecore Product

Visit: www.cyberoam.com
Contact: info@cyberoam.com

USA - Tel: +1-978-465-8400, Fax: +1-978-293-0200
India - Tel: +91-79-66065606 / 26405600, Fax: +91-79-26407640