Technology Best Practices for Intrusion Prevention

Introduction

Intrusion Prevention is a new technology category that focuses on taking a proactive approach to IT security by *preventing* attacks on corporate IT resources, as opposed to similar technology that merely *detects* and reports on attacks that have already taken place. Intrusion Prevention is gaining visibility in corporate and government organizations due to the inherent limitations in existing security technologies, as witnessed by the significant financial loss experienced by organizations in 2001. Intrusion Prevention can be thought of as the logical follow-on to signature-based technologies such as Intrusion Detection and anti-virus, and to network-oriented protection solutions such as firewalls.

Traditional security products have focused on the biggest threats that emerged as computer networking, email and web applications were adopted by corporations. As corporations adopted these technologies, they purchased products to solve the security issues inherent in these technologies, namely perimeter protection (firewalls), network protection (network-based intrusion detection), and file-based security (anti-virus). These technologies do not address new attacks that ride over existing protocols to attack applications, or new content-based attacks that attack systems before vendors are able to release and distribute signatures and other countermeasures.

This document will outline the technology best practices for Intrusion Prevention solutions, to help organizations make informed decisions when choosing Intrusion Prevention products. It will not make a detailed case for Intrusion Prevention compared to other technologies – that subject is covered in a companion document.

Best Practices

Any organization that intends to protect itself through the use of Intrusion Prevention technology should take a number of factors into consideration when evaluating products that address the organization's defined security requirements. Care should be taken that chosen solutions meet corporate security, manageability, and flexibility requirements, lest the solution be a partial one, or worse, introduce a significant management burden that overshadows the security benefits.

Best practices should include

1. **Host-based protection**
   As technologies such as high-speed networks, switching, and end-to-end encryption are more widely adopted, providing desired security at the network level becomes a major challenge. The best place to enforce security is at the desktops and servers, where the actual work is performed and the potential for damage is greatest.
2. **Real-time prevention decisions**

To ensure the highest levels of security and minimize the ability to bypass the security policy on a host, application calls must be intercepted at the kernel level where the determination is made of their adherence to policy. Solutions that are implemented by replacing shared libraries or analyzing system audit logs can be bypassed relatively easily. An effective Intrusion Prevention strategy includes preventing violations in real-time, rather than noting attacks or system changes after the fact.

3. **Defense in depth – protection from attacks at various phases**

   In order to completely enforce a company's security policy, Intrusion Prevention must intercept all major points of communication between applications and the underlying system. Network control must limit client/server communications at the port and protocol level, as well as hosts for permitted communications; file system controls must allow/deny read and/or write access to folders and files on an individual and group basis; registry controls must prevent the overwriting of important registry keys that control how the system and other applications operate; and COM controls to restrict inter-process communication to allowable access.

   Attacks have multiple phases – exploiting network and application-level weaknesses, replicating and distributing themselves, and making unauthorized changes to the system. A complete Intrusion Prevention strategy must protect systems from all of these phases, so that if a new class of attack is released, it will be thwarted at one or more of the stages.

4. **Real-time correlation at the agent and enterprise level**

   Correlation is vital for an Intrusion Prevention technology. Correlation deployed at the agent provides a level of accuracy on prevention decisions that does not exist with signature matching approaches. Correlating sequences of events within the context of an application's behavior eliminates the potential for false positives.

   Correlation at the enterprise level enables security to be adaptive. By correlating the events on distributed agents, Intrusion Prevention policies can be dynamically updated to prevent propagation of malicious code, thus preventing widespread damage to numerous resources.

5. **Behavioral approach**

   The Intrusion Prevention approach must enforce appropriate system and application behavior to ensure that the security implemented is proactive, not reactive. Solutions that rely on signatures only provide security to the release of the most recent signature update.

6. **Flexibility to meet unique corporate needs**

   Every corporation is unique in the details of how it configures and manages its systems and corporate applications. Intrusion Prevention solutions that are considered must be flexible to accommodate this uniqueness by permitting the customization of policies and creation of new policies that accommodate both unique applications and unique implementations. The solution must support automated policy creation to ease the management burden of creating policies by hand.

7. **Ease of deployment**

   The Intrusion Prevention strategy should minimize the personnel overhead associated with agent deployments. Solutions that are considered must provide out-of-the box functionality to allow for rapid deployment of the desired security policies, and must allow for new and custom policies to be rolled out as needed without additional intervention at the host level.

The solution must support web-based deployment, and allow for easy integration with standard corporate software distribution mechanisms.

8. **Centralized event management**
   All events generated by the agents must roll up into a centralized repository from which alerts and reports may be generated. Solutions that are considered must support standard alerting interfaces such as SNMP, paging, email, flat files, and allow for custom interfaces to the alerting system to easily integrate with corporate systems.

9. **Platform coverage, with support for desktops and servers**
   Solutions that are considered must provide coverage for the key operating systems that the corporation wishes to protect. In light of recent attacks like NIMDA, which target multiple hosts, the same management and enforcement paradigm must apply to both desktop and server-based systems.

10. **Administration**
    To ease policy management, policies must be definable centrally and automatically distributed to agents on a configurable interval. Policies must also be exportable for replication and archive purposes.

    Companies with more than one administrator require a “manage from anywhere” capability to ease management of their environment. Intrusion Prevention solutions considered should be manageable from anywhere using a standard web browser to avoid the installation of custom software at each administrator’s desktop, to avoid the installation of insecure and difficult to maintain software that enables remote administration, and to lower the learning curve for the IT staff.

    Large corporations that have many thousands of systems which require protection should consider solutions where a single manager can support thousands of agents, and allow for the replication of policy across organizational or regional boundaries.

Summary

This document has described the technology best practices that companies should consider when implementing Intrusion Prevention products to better secure their IT infrastructures. Companies should ensure that their Intrusion Prevention solutions meet the security, manageability, and flexibility requirements outlined above in order to avoid limited or unmanageable solutions.

For information on the OKENA approach to Intrusion Prevention, please visit us at www.okena.com, or (781) 209-3200.