Intrusion detection system deployment recommendations

searchfinancialsecurity.techtarget.com/tip/Intrusion-detection-system-deployment-recommendations

Selection, placement and maintenance of intrusion detection systems (IDS) are based on the requirements and current...

infrastructure of a company. One product may work well for one company and fail for the next. Selection is typically the most difficult decision, for products MUST meet business requirements, function correctly within the intended network infrastructure and be supportable by current personnel.

Industry standards for most intrusion detection systems mandate the use of both a network- and host-based IDS. A network-based IDS provides an umbrella to the network by monitoring all traffic on specific segments that may contain malicious traffic or have mal-intent. The sole function of a network-based IDS is to monitor the traffic of that network. A host-based IDS is deployed on devices that have other primary functions such as Web servers, database servers and other host devices. A host-based IDS provides information such as user authentication, file modifications/deletions and other host-based information, thus designated as secondary protection to devices on the network.

Initial Industry Standard IDS deployment dictates use of network-based IDS, then host-based IDS. This ensures the network, and then host devices are protected. The core foundation of any company is the network infrastructure, then devices within those networks. IDS should be deployed in the same fashion.

A host-based IDS should be deployed as a secondary task in a three-tier approach, after a network-based IDS. Tier one deployment includes highly critical host devices located in the external-parameter of the network. These include critical Web, mail and other devices located in the DMZ or extranet (Internet facing network segments within or outside the DMZ). Tier two consists of other non-critical DMZ devices that can include most DMZ devices. Lastly, tier three would consist of all other devices located within the protected-private network inside the DMZ that are critical or contain confidential data such as client, financial and databases. As stated above, individual devices comprise the network and should be protected, but only after the network is first secure.

Network-based IDS recommendations

A network-based IDS should be deployed on the external demilitarized zone (DMZ) segment, then the DMZ segment. This will allow monitoring of all external and DMZ malicious activity. All external network segments should be monitored to include inbound and outbound traffic. This will ensure all devices connected to external hostile networks are monitored and checked. These recommendations are industry standards that are used to track malicious activity at both the extranet, Intranet and DMZ environments. Extra protection with the use of a network-based IDS at all entry points should be accomplished first to ensure monitoring of all malicious attempts on company resources, not only the well known network connections, but all known external connections.

Policy and tool recommendations

Additional recommendations beyond IDS deployment should include development of incident response manuals, procedures and tools. An IDS functions as a burglar alarm, thus human intervention is necessary after the alarm sounds. Possessing and using good incident response techniques enhance the value of data gathered from an IDS by providing the next-steps to forensic examination. Software tools for incident investigation should also be pursued to ensure tools are available to research, evaluate and report findings. If at anytime the company would be forced to take legal action due to malicious activity, these tools would be necessary along with the established policy and standards, to provide evidence. Without the tools or policy, the company may not be able pursue legal action or stop a perpetrator.

Product deployment

Deployment of a network-based IDS should be immediate at the external Internet facing network segments, then DMZ segments. A host-based IDS should then be deployed on all critical DMZ host devices. Finally, any other major host device should also have a host-based IDS applied to ensure those systems are protected, as well.

Project tasks for IDS

The project tasks identified below are generic in nature, but typically the industry standard for IDS deployment.

Develop management system: This should entail selection and number of network- and host-based devices to deploy, place of management consoles and the overall infrastructure.

Develop logging systems: Since an IDS can generate large amounts of data, logging systems should be chosen that allow gathering of large amounts of data, backup and recovery procedures and storage facilities. Hardware and software may need to be ordered during this phase.

Develop audit policy: This comes after the first two phases, for at this point the number of sensors and logging procedures should be chosen. *An IDS without an audit policy of IDS logging is like having no IDS at all.* Logs should be checked daily for critical incidents and weekly for all others. Severity levels should be developed to track and handle all incidents. These levels would include detailed descriptions on actions to accomplish, people to call and data to gather in case of true malicious activity or break-in of critical systems.

Deployment of network-based IDS: This should be done ASAP to start gathering data. Again, a network-based IDS should be deployed first as an industry and recommended standard. The approach should be three tiers, to start at the furthest extension of the security parameter, then DMZ and other devices.

Deployment of host-based IDS: Host-based IDS deployment should be after network-based, as an industry standard. This could actually be done at the same time as network-based, but the emphasis should be placed on network-based first.

Refine IDS polices: This step should be done through the entire IDS deployment process and afterwards. Polices change according to the business need or threat, thus this is an ever changing piece of the project.

Refine written standards: As with any system, there must be company standards in place to ensure compliance with standards. IDS standards should be started at the beginning of the project and continue through completion. These should include configurations, polices to use, logging, auditing and reporting.

Project task beyond IDS

As identified, a valid IDS must contain support beyond those of hardware and software. Written procedures for incident response must be developed and approved for a time when there is a valid malicious attempt against company systems. The following are recommended steps to go beyond an IDS.

Incident response: An incident response procedure must be developed to ensure a standard is in place once a malicious attempt is made on company systems. This should include a written procedure, actual next-steps, who to call, when to call, how to call and a notification chain. An IDS is only as good as the incident response behind the system. When the alert is sounded, the company needs to have a fully tested response procedure in place to ensure there is no loss, or to record if there was a loss, of critical information. A good incident response procedure will ensure data integrity is assured for historical chain of evidence in forensics investigation.

Forensic toolkits: Many products exist to accomplish the examination of data once an incident occurs. Tools should be researched that meet the company requirements and onsite personnel trained on their use.

Gramm-Leach-Bliley Act

Sections 501 and 505(b) outline the guidelines for all banks to establish standards for safeguarding customer information. If your company is not a financial institution, you should still consider the general recommendations listed below as standard information security practices.

Scanning and vulnerability testing: Scanning and vulnerability testing should be accomplished by third parties to ensure compliance with an IDS and other security recommendations.

Policy review: Information security policy must be maintained and reviewed to ensure accuracy and compliance with Federal standards.

Firewall and router review: Firewall and router reviews should be accomplished quarterly, at a minimum, to ensure that accurate and complete security configurations are used.

About the author:
Edward P. Yakabovicz has 19 years of experience in computers with a focus in security and engineering. He holds certifications in CISSP, MCSE, CCNA and CNA.