Sample Defense in Depth White Paper

Author: Ken Foster
Published: January 16, 2011

Abstract:

This paper summarizes a fictitious briefing provided to the company Chief Information Officer (CIO) in regards to how their organization practices a solid Defense in Depth strategy. The purpose of this paper is to provide insight in how other organizations may be able to improve their current protective postures and lower their risk to data loss prevention. Key concepts addressed include:

- Defense-in-Depth
- Perimeter Zone Protection
- Intrusion Prevention Layer (IPS)
- Virtual Local Area Network (VLAN)
- Digital Rights Management (DRM)
- Security Event and Incident Management (SEIM)

Our organizational Defense-in-Depth deployment is a layered strategy that is designed hinder access by unauthorized parties to sensitive corporate systems while alerting security personnel providing their ability to identify, forensically store, validate the attempted breach. This strategy does not assume policy and access violations will only occur from the perimeter inward. To this end, we exercise not only physical and logical separations, but also integrate separation of duties to reduce the possibility of insider Coercion. Finally, any sound security implementation requires constant reassessment based on change controls and standard time increments. Our corporate Defense-in-depth approach takes all these issues into account and provides a mature approach as outlined below.

The organizational security strategy is divided into zones, each with independent security protocols and processes (Fadia & Zacharia, 2008). Layers are not interdependent for their protective properties, thus breaching a single layer does not provide open access to the adjacent layers. Each layer is managed by a different team, integrating separation of duties, significantly impeding the use of coercion as a method to compromise an insider within the security team (Coleman, 2008). The statistics and logs from each layer are shared for intelligent analysis. The sum of the whole picture provides a far more granular approach to the real-time risk assessments of the network.

Perimeter Zone

The perimeter zone consists of the router and Firewalls. To provide maximum availability, two diverse pathways from the provider have been provisioned into the core router. This provides two separate routes should either environmental or malicious acts impair the primary path (Hughes Communications Inc., 2009). Immediately behind the router exists a pair of redundant firewalls; set in active-active mode for failover. The firewalls insulate the external,

DMZ, and internal zones through the application of policies set to deny all, allow by exception to specific hosts. Should the Primary Firewall fail, the secondary firewall will immediately take over (Cisco System Inc., 2009). Both firewalls maintain state information and have duplicate rules applied. The Network team manages the firewalls through the Change Control Board (CCB), documenting each approved change prior to application. The firewall security configuration is modified and monitored by the security manager software. Changes not implemented through the security manager to a firewall are identified and rolled back with notification sent to the Chief Technology Officer (CTO) and Chief Security Officer (CSO).

Intrusion Prevention Layer (IPS)

Immediately behind the firewalls exists a redundant pair of Intrusion Prevention Systems. These are configured for high availability through a failover, then fail closed configuration. A firewall can be configured to either allow or deny specific ports and protocols to or from resources. They are not capable of analyzing and applying granular exception policies. This is where an IPS becomes that critical second level of the layered defense. The purpose of the IPS is to interrogate the traffic passed on by the initial filtering of the firewall for further inspection of policy violations (Fadia & Zacharia, 2008). A policy is the application of a response to a given packet payload event. For instance, if a request to send SMTP traffic to the internal email server arrives from the inside segment, that is expected and allowed to pass. However if a request from the internal network to bypass the internal server and send email directly to an external SMTP server is received, it violates policy and a TCP reset command terminates the request, logging the traffic. The IPS's are configured and monitored by the CSO's office. The Network team does not access to the configuration of the IPS's. The CTO and CSO both receive anomaly event reports directly from the device. Modifications to current policy sets must be

approved in writing by the CCB. This creates a system of checks and balances, preventing any one person from modifying the policies without alerting the staff. In accordance with current corporate policy, if both the primary and secondary IPS's fail, the system will fail closed. Depending on the direction of the Chief Information Officer (CIO), CTO, and CSO disaster action committee, a manual bypass can be initiated if directed.

Virtual Local Area Network (VLAN)

A Virtual Local Area Network (VLAN) is a method to provide isolation to a specific resource without the need to procure physical hardware (Davis, 2009). In our corporate environment, we have a requirement to isolate departmental resources and server management subnets from the reset of the network. This isolation consists of the application of departmental VLAN's and application of specific specified Access Control List's (ACLs). The VLAN's are provisioned and maintained by the Networking Team through a helpdesk ticketing system. This system documents the requestor, reason, CTO approval, and implementation of any VLAN requirements. The placement of assets on a VLAN is also a helpdesk ticket from the immediate supervisor, through the Department Manager, to the Networking Team. This only places the port on the switch in the requested VLAN. For access to resources, ACL's are applied to the resources within the VLAN and assigned to user groups (Microsoft Inc. (a), 2010). A helpdesk ticket from the immediate supervisor, through the Department Manager to the corporate Security Team is required to assign a user or resource to a specific security group. Only the Security Team has permissions to modify the organizational unit memberships within this container. All modifications generate an email to the CSO and CTO. VLAN's and ACL's are independent layers and not affected by firewall or IPS failures.

Digital Rights Management (DRM)

To prevent accidental loss of control of sensitive information, the corporation has implemented a Digital Rights Management (DRM) solution (Microsoft Inc. (b), 2010). Using DRM technologies and enforced through group policy at time of document creation, every document must have a classification and security template applied. Documents can be classified as Public, HR Only, Legal Only, Mgt Only, Special Distribution, or the general corporate use only classification of Internal. Additionally attributes such as Print, Read Only, Copy, Email, and Share are assessed based on Organizational Group memberships. Any attempted access to a file controlled by DRM by someone not assigned rights is blocked, preventing access. Inside the network, DRM services are cluster to provide high availability. Externally a single virtualized machine exists in the DMZ so that traveling users and Special Distribution documents can be viewed off-site as appropriate. Updates to the DRM server occur via a Virtual Private Network secured channel from the cluster using a service account which only has the rights to update the DMZ server. The DRM server has granular rights controls established and delegated to each department manager. Managers can review and modify rights on any document within the enterprise that they have permissions. In cases where document controls exceed the rights of a department manager, those document rights are controlled by the CSO. For safety reasons, only the CIO can manage rights assigned to the HR or Legal groups. DRM permissions and control are independent from the ACL's on the VLAN's, not impacted by IPS policies, or to the larger extend firewall rules.

Security Event and Incident Management (SEIM)

The keystone of our Defense-in-Depth strategy for the Forensics Response Team is the Security Event and Incident Management (SEIM) implementation, analysis, and reporting capabilities. The SEIM collects real-time events from our firewalls, IPS, DRM, Anti-virus servers, and Domain Controllers. It uses the events along with net-flow data to apply artificial intelligence analysis and correlated to these events (EMC Corp., 2010). The resulting output is a risk analysis of events and their impacts on corporate targets. The SEIM aids in addressing risk of Zero-Day exploits and provides us an analysis tool to validate our firewall and IPS rules sets. Should an attack penetrate the LAN, the logging of events from the various devices will allow the forensics team a chronology of what, how, and when the event occurred. All traffic is stored in a forensically sound format, accepted by federal courts of law. Should the need arise; the legal department can obtain copies of the logs and the forensics teams' analysis for use in pursuit of legal matters.

The corporate strategy for Defense-in-Depth analyzes the risks of a connected network against the usability of services. A full classification system enforces values and places restrictions on files and resources through a granular application of DRM, VLAN, and ACL technologies. Traffic on all segments of the corporate controlled network is scanned in real-time for policy violations from the IPS. The perimeter is protected by a series of firewalls. These independent solutions provide an environment where the breach of any one layer does not provide uninhibited access to others, while providing a forensically sound audit trail.

References

Cisco System Inc. (2009, November 4). *PIX/ASA: Active/Active Failover Configuration Example*. Retrieved November 21, 2010, from Cisco.com: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080834058.shtml

Coleman, K. (2008, August 26). *Separation of Duties and IT Security*. Retrieved November 21, 2010, from CSO Magazine: http://www.csoonline.com/article/446017/separation-of-duties-and-it-security

Davis, D. (2009, January 8). *What is a VLAN*. Retrieved November 21, 2010, from Petri IT Knowledgebase: http://www.petri.co.il/csc_setup_a_vlan_on_a_cisco_switch.htm

EMC Corp. (2010). *Security Information and Event Management*. Retrieved November 21, 2010, from RSA.com: http://www.rsa.com/node.aspx?id=3182

Fadia, A., & Zacharia, M. (2008). *Network Intrusion Alert.* Boston, MA: Thompson Course Technology.

Hughes Communications Inc. (2009, August). *Guarding Against Network Failures*. Retrieved November 21, 2010, from Hughes.com: http://www.hughes.com/HNS%20Library%20Presentations%20and%20White%20Papers/HN-AccessContinuity_H38054_HR.pdf

Kruse II, W. G., & Heiser, J. G. (2010). *Computer Forensics.* Boston, MA: Addison-Wesley.

Microsoft Inc. (a). (2010, September 30). *Access Control Lists*. Retrieved November 21, 2010, from Msdn.Microsoft.com: http://msdn.microsoft.com/en-us/library/aa374872(VS.85).aspx

Microsoft Inc. (b). (2010). *Windows Rights Management Services*. Retrieved November 21, 2010, from Microsoft.com: http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx