Solution Note: Protecting SharePoint Deployments

Applying a Layered Security Approach to Enable Secure Usage

Introduction

Microsoft SharePoint helps streamline workflow and accelerate time to market by enabling employees and non-employees alike to collaborate using familiar tools such as Microsoft Office (Word, PowerPoint, Access, Excel, and Outlook). When deploying SharePoint, there are several network security factors to consider, over and above the default SharePoint security and control capabilities.

- Network administrators should take steps to eliminate rogue SharePoint deployments.
- Collaboration often involves employees in a variety of locations as well non-employees such as contractors. To protect the content and the network, appropriate measures to isolate and control access to SharePoint should be implemented.
- SharePoint is built upon three application components (IIS, MS-SQL, ASP.net) that are commonly targeted by malicious users, so it is important to apply appropriate threat prevention policies to protect SharePoint deployments as well as the network.

Using a Palo Alto Networks next-generation firewall enables organizations to apply additional levels of network security to SharePoint deployments.

The Problem: Rogue Deployments, Component Access and Security Threats

The wide range of users that may be accessing SharePoint, combined with a component-based architecture that is highly targeted by malicious users presents IT managers with three distinct challenges.

- The first challenge is to reign in unknown or rogue SharePoint deployments. Surprising as it may seem, research by Neil MacDonald at Gartner shows that as many as 30% of the SharePoint deployments are rogue. A rogue SharePoint deployment represents significant business and security risks primarily because the deployment has been done outside of IT guidelines and procedures and as such, may introduce a significant security hole.
- The second challenge that IT managers face when deploying SharePoint is to enable collaboration while maintaining compliance with regulatory and/or internal policies that dictate who has access to the applications and who may be able to post.
- The third challenge relates to ensuring that the SharePoint components (IIS, MS-SQL, ASP.Net) are protected from serious threats such as SQL injection attacks and IIS buffer overflow attacks. Without protection against these types of threats, proprietary information held within SharePoint may be exposed to theft or destruction.

Part of the challenge that SharePoint presents to IT departments is the fact that it looks like common web traffic (HTTP or HTTPs), making it more difficult for to delineate the SharePoint traffic from web traffic in order to apply appropriate security controls using today's existing port-based security tools.

The Solution: Identify, Control, Monitor and Inspect SharePoint Traffic

Palo Alto Networks next-generation firewalls can help organizations protect SharePoint environments by taking a very systematic approach that includes determining or confirming that SharePoint is in use, then applying added levels of isolation and control to those environments and finally, protecting SharePoint traffic and information from threats or theft.

- **Identify SharePoint Components:** The first step is to determine if SharePoint is installed and who is using it. Using this information, the security team can work with the business groups to determine if the deployment is rogue and assess the business case, making suggestions on how to apply appropriate security policies. Even in cases where SharePoint deployments are supported, knowing which components are being used and applying firewall policies to those components provides an added layer of network security. In addition to MS-SQL, Palo Alto Networks currently identifies six SharePoint functions including: SharePoint, SharePoint-admin, SharePoint-blog-posting, SharePoint-calendar, SharePoint-documents, and SharePoint-wiki. Using data from the Palo Alto Networks *Application Usage and Risk Report (Fall Edition,2009)*, the most commonly used components are shown in the Figure 1 below.

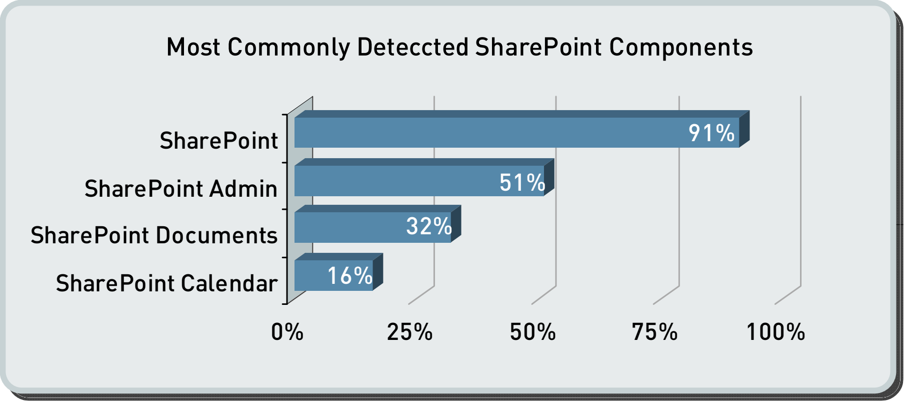

Figure 1: Most commonly discovered SharePoint components across more than 200 different organizations.

- **Isolate and Control SharePoint Components:** Once the SharePoint components and associated users have been identified (via Palo Alto Networks Active Directory integration), an administrator should take steps to isolate key architecture components (MS-SQL, SharePoint) to achieve appropriate levels of security. Rather than physically re-architecting the network to isolate the SharePoint components, Palo Alto Networks simplifies the isolation process through the use of security zones, which are logical containers for physical interface(s), VLANs, a range of IP addresses or a combination thereof.

  Using security best practices, administrators can place MS-SQL into a highly restricted zone while the SharePoint server can be placed in a different zone, with appropriate access restrictions. Once the key architecture components have been isolated, administrators can leverage Palo Alto Networks Active Directory integration to complement existing SharePoint feature controls with user-based policies to control access to the six individual SharePoint functions currently identified as well as MS-SQL.

- **Protect SharePoint Traffic From Attacks:** The next recommendation for securing SharePoint environments is to ensure that SharePoint, and its architecture components are protected from aggressive attacks. SharePoint relies on IIS, ASP.net and in many cases, MS-SQL, which means that the exposure to vulnerability exploits is significantly higher. As a proof point, an evaluation of the data collected from more than 200 organizations for the most recently produced *Application Usage and Risk Report (Fall Edition,2009)* shows that there were 35 different critical, high and medium severity threats (more than 220,000 instances) that targeted SQL, IIS, ASP.NET and SharePoint.

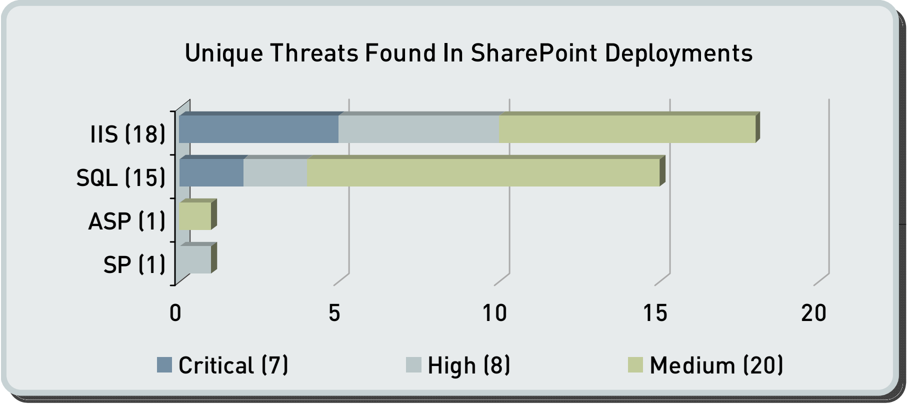

Figure 2: Critical, high and medium severity threats discovered in organizations where SharePoint was in use.

The most heavily targeted component was SQL with 85% of the threat instances identified. Using the Palo Alto Networks next-generation firewall, an administrator can first isolate MS-SQL and then apply threat prevention policies to specifically block attacks against MS-SQL as well as the other supporting SharePoint components.

- **Monitor and Control Unauthorized File and Data Transfers:** Collaboration means sharing information, in some cases, with external (non-employee) users. Extreme caution should be taken when determining what types of files can be shared as well as by whom. While SharePoint has very granular controls over who is allowed to post, the realm of control is limited to only SharePoint environments.

  Taking advantage of the Palo Alto Networks file transfer and data filtering control capabilities, administrators can apply policies that will extend file and data transfer controls beyond the SharePoint controls. More than 50 different file types are identified and can be controlled with response options that include outright blocking, block and send the user a warning message or log and send an alert to the administrator. In addition to file transfer controls, confidential data patterns (credit card and social security numbers) can also be detected with varied response options depending on the policy.

Summary

Collaborative tools like SharePoint enable efficient yet freeform information sharing that fosters new ideas, improves communication efficiency and ultimately improves the bottom line. At face value, freeform communications contradicts security best practices, which may help explain the rogue SharePoint deployments. Regardless of whether or not the deployments are rogue, IT departments must determine the key business requirements and how they can enable the safe and secure use of SharePoint without hindering workflow. With a Palo Alto Networks next-generation firewall, the IT department can achieve the best of both worlds by enabling the use of SharePoint while protecting users and the company from a wide range of data loss, compliance and security risks.