Realtime publishers

Securing SharePoint Content

The Essentials Series

sponsored by

Dan Sullivan

Copyright Statement

Common Practices that Undermine SharePoint Content Security

The growing popularity of Microsoft SharePoint should come as no surprise to IT professionals. We have long struggled to help business users capture, organize, and use content. In the past, we might have used shared network drives within a department to enable document sharing within groups, but the increasing use of multiple platforms, including mobile devices, calls for a more Web-oriented approach to collaboration. Microsoft SharePoint not only offers feature rich, Web-based collaboration services but also makes it easy for most users to set up sites and start sharing with minimal hassle. An application that addresses a pressing need and is easy to use is something of a dream come true for IT. There is, however, a dark side to this scenario.

Setting up a secure SharePoint site and maintaining appropriate access controls to content is not a trivial task. Sometimes the path of least resistance to getting a site up and running is to implement few security controls. Even if only some people in the department need access to some of the content, it might be quicker for an inexperienced SharePoint administrator to grant broad access to everyone in the department. This reality is just one example of practices that can undermine SharePoint site security.

This series on protecting and securing SharePoint content examines how to safeguard your SharePoint experience so that you continue to have the benefits of the collaboration tool while mitigating the risk of a security breach. This, the first article in the series, considers administration practices that can undermine content security, such as inappropriate access controls and lack of a data classification policy. The second article in the series reviews technical challenges to securing SharePoint use. This article covers browser vulnerabilities and the implications of employee-owned devices for controlling content distribution. The third and final article in this Essentials Series outlines techniques for securing SharePoint sessions and controlling users' actions with protected content.

Three areas require particular attention when discussing common practices that undermine SharePoint security:

- Shared administration
- Access control maintenance
- Lack of data classification schemes

Each of these areas presents a set of challenges that must be addressed to adequately protect SharePoint content.

SharePoint and Shared Administration

An unusual characteristic of SharePoint is that it often depends on a shared management model. Windows servers and Microsoft Exchange servers might be managed exclusively by IT professionals, but SharePoint distributes the management responsibilities between IT administrators who centrally manage the SharePoint infrastructure and SharePoint site administrators who create and maintain sites for specific collaboration purposes.

There are many advantages to this management model. Central IT is no longer a bottleneck to creating collaboration Web sites. If a team in the marketing department wants to set up a site to share potentially sensitive documents with a partner, a member of the marketing team can create the site. There is no need to submit Help desk tickets and then wait for someone in IT with the right skills to address that ticket. For IT professionals, this model is a plus as well. IT can set up SharePoint as a self-service operation (at least to some degree) and reduce the demand on their resources.

Problems arise with this kind of shared management when the responsibilities are not clearly defined. It is not difficult to imagine the infrastructure management team assuming site administrators will take care of certain tasks, while those site administrators assume the same tasks are managed centrally. In other cases, site administrators might not even be aware that certain security controls have to be configured.

Another area of potential vulnerability is with external users. Non-IT professionals might not be familiar with security concerns related to external users. In particular, they might not know the policies and procedures their organization has in place for granting external users access to internal systems and content. Central IT should have such policies in place, but that is not always the case.

The advantages of shared management in SharePoint can be undermined by poor coordination between central infrastructure management teams and distributed site-based management personnel.

Need to Maintain Access Controls

SharePoint users are granted permissions to access and modify content within SharePoint sites. SharePoint implements access controls through a combination of user groups, permission types, and the site hierarchy. Most of the time, site administrators can implement access controls by managing group membership and permission sets assigned to various groups.

For example, consider a marketing department that implements a collaboration site. Someone in the department might be designated as the site administrator, and she will need privileges to edit the site itself. Several other members of the department will generate content for the site, so they will need permissions to add, edit, and delete documents. Finally, another group within the department will need only to read content created by others, so that group requires only permission to view content.

Variation in Permission Needs

This variation in permission needs is common and easily accommodated. Over time, though, the actual permissions assigned might no longer align with user requirements. If the site administrator leaves the department, another member of the team might be assigned as administrator. Ideally, the former administrator would have her permissions revoked, but that might not occur. The former administrator might keep her permissions in order to help during a transition period. This setup is a good idea, at least in theory. Without a clear deadline for revoking the former administrator's privileges and no formal method for tracking follow-up to remove those privileges, the former administrator may continue to have unnecessary access to the marketing department's site.

This same type of problem can occur with any user and apply to any set of permissions. Changes in roles and responsibilities can lead to a number of over-privileged users. This situation is obviously a problem if the over-privileged users are malicious and intend to harm the organization by tampering with or destroying content. Even well-intentioned users with excessive privileges are potentially problematic. For example, a careless user could mistakenly attach a sensitive document to a widely distributed email or download confidential data to a mobile device that is later lost or stolen. Even without malicious intent, careless users can be the root cause of data breaches.

Browser Vulnerabilities

Vulnerabilities in browsers, for example, create opportunities for someone seeking to steal confidential or private information. When users access content and view it in their browser, that content might be stored locally on the client device. Browsers maintain caches of content downloaded to the browser in order to improve performance. These browser caches have channels for data leaks, so there is a clear need to minimize the amount of confidential and private content left in browser caches. One way to mitigate this risk is to minimize the number of people who have access to such content.

Site administrators have to perform something of a balancing act when it comes to allowing access to content. One of the reasons so many businesses and organizations use SharePoint is because it supports collaboration on multiple devices, both inside and outside the corporate network. SharePoint users can utilize desktop or mobile devices running a number of operating systems (OSs). Vulnerabilities in any of the browsers used across these devices could be exploited in an effort to steal intellectual property, disclose private information, or other forms of data theft.

This idea leads to another common weakness in protecting SharePoint content: the lack of data classification schemes.

Lack of Data Classification Schemes

SharePoint makes no automatic distinction about the value of content. A Word document outlining a trade secret is subject to the same kinds of processing as a 5-year-old press release. Clearly, one is more valuable to the company than the other, and it is our responsibility, as SharePoint users and administrators, to apply appropriate protections.

Not all data is equally valuable to an organization. Some data is private or confidential and requires minimal distribution. A long-standing good practice in security is to grant users only the privileges they need to do their work—and no more. This idea is known as the principle of least privilege. It applies well to content sharing because the practice reduces the number of users with access to content to only those who need it.

One drawback of implementing the principle of least privilege is the cost. If someone were to review the privileges assigned to every object in a SharePoint repository and research how that content were used, the costs could quickly grow beyond the value of the content they were trying to protect. Rather than apply the principle with equal vigor to all content, organizations should prioritize their content and create a data classification scheme.

Data classification schemes are typically course-grained categories that group content based on the types of protection it requires. One such scheme categorizes content into one of four groups:

- Confidential data, which if disclosed could cause substantial harm to the organization. Trade secrets and strategic plans are examples of confidential data.
- Private data, which if disclosed could cause substantial harm to a customer, client, employee, or other individual. Social Security Numbers (SSNs) and protected health information are examples of private data.
- Sensitive data, which should not be disclosed but if it were would not cause significant harm to the organization. Internal memos about company leave policies are an example of sensitive data.
- Public data, which can be shared without harm to the organization. Press releases are an example of public data.

By categorizing content based on a data classification scheme, an organization can help site administrators prioritize security controls for content. In particular, a data classification scheme could prevent private or confidential data stored in SharePoint from being leaked due to poor management of SharePoint privileges or to browser vulnerabilities being exploited to steal data.

Summary

SharePoint is a valuable collaboration tool for many organizations. The shared management model that leverages centralized management of SharePoint infrastructure with a distributed model for site administration has many advantages. There are drawbacks to this approach, however. Miscommunication or poorly defined roles and responsibilities can lead to security vulnerabilities and data leak risks. These potential weaknesses can be addressed with a combination of techniques, including clearly defined responsibilities, data classification schemes, and technical controls to compensate for browser vulnerabilities.