Realtime publishers

Securing SharePoint Content

The Essentials Series

sponsored by

Dan Sullivan

Copyright Statement

Best Practices for Securing Browsers for SharePoint

Web browsers are essential components for working with SharePoint. Maintaining secure browser sessions can mitigate the risk of both intentional and unintentional data leaks. Best practices for securing browsers for SharePoint include:

- Using secure sessions when accessing SharePoint
- Preventing users from reaching content unless they those users have a legitimate need
- Managing browser sessions centrally

This combination of best practices addresses the core technical challenges outlined in earlier articles in this Essentials Series.

Using Secure Sessions When Accessing SharePoint

IT departments may have well-designed and enforced security policies in effect on company-owned devices, but employee-owned devices, public computers, and other external collaborator–owned devices may be far less secure. These issues are commonplace. Device-centric security is no longer sufficient to meet requirements, particularly with regard to protecting SharePoint content.

An alternative approach to device-centric security is session-based security. The idea is that a network session between a client and the SharePoint server is secured in ways to mitigate the risk of data leaks. A secure session requires five characteristics:

- Data is encrypted between the client and the server
- Malicious or problematic browser extensions are blocked
- Data stored in the browser cache is encrypted
- Malware on client devices is blocked
- Data is deleted from the browser cache when the session is ended

These characteristics are required to prevent a variety of methods an attacker could use to steal data.

Encrypt Data Transmitted Between Client and Server

Data that is transmitted from the SharePoint server to a client device may use an insecure network, such as the Internet. Someone interested in stealing data in transit could capture data using packet sniffers and other network monitoring tools that are freely available on the Web. The first step to avoiding this kind of data loss is to encrypt all traffic between a server and a client. If an attacker were to capture the transmission, the data would be useless. Only the sender and the recipient would have the encryption key needed to decrypt the content. This type of encrypted session is easily managed because the user does not have to manage encryption keys; at the beginning of each session, the client and server negotiate how to encrypt data for that session.

Block Problematic Browser Extensions

During a secured browser session, problematic browser extensions, or plugins, should be blocked. This block can be done with a white list–based policy. Browser extensions listed in the policy are allowed, while all others are blocked. This approach allows SharePoint and network administrators to define which extensions are trusted. It also avoids a weakness of black lists, which only block known malicious extensions.

Encrypt Data in the Browser Cache

Following the same line of reasoning that calls for encrypting data during transmission, a secured browser session should encrypt all data stored in the browser cache. Doing so ensures that a malicious process reading cache contents will not be able to capture useable data.

Block Malicious Programs

A secured browser session must be able to block malicious programs on a client device. For example, even with encrypted data and blocked browser extensions, a keylogger on a compromised client could allow an attacker to capture keystrokes as they are typed into the SharePoint interface. This vulnerability needs to be addressed by blocking such programs.

Delete Cached Data

As a general rule, no data should be left in the browser cache once a secure session is ended. The session is over, so there should be no need to refer to the cached data again. Therefore, there will be no adverse effect on performance by deleting the cache, which is a key reason to cache data in the first place.

Overall Strategy: Defense in Depth

These five characteristics of a secure session may appear redundant or at least somewhat overlapping. For example, if data is encrypted, does it really need to be deleted? If malware is blocked, do we really need to disable browser extensions? These are reasonable questions. The driving principle in this case is known as defense in depth.

The defense in depth approach uses multiple, sometimes overlapping, security measures under the assumption that at some time, one or more of the security controls may fail or become vulnerable to attacks that are not currently known. Employing all five techniques to secure browser sessions provides additional layers of security than methods that employ only a subset of these controls.

Control User Actions with Protected Content

A secure browser session mitigates a number of data leak risks, but we should not forget the need to prevent users from accidentally or intentionally leaking protected SharePoint data.

Limiting Access to Content

The first step to controlling users' interactions with SharePoint content is to ensure that users have access only to content they need to do their jobs. This idea is an example of another security principle, which was mentioned in an earlier article in this series, the principle of least privilege. The basic idea is that if users have more access to content or applications than they actually need, then we are unnecessarily increasing the chance of compromising data or systems.

Consider a person in product development with extensive access to product roadmaps, trade secrets, and other proprietary information. The person might not actually need access to all of this information to perform her duties but poor administration practices have lead to excessive privileges across the organization. If the employee is unethical, she could use her access to confidential information to land a job with a competitor, in part by promising access to her current employer's trade secrets and product strategies.

Limiting Access to Web Sites

During secure sessions, users should not browse to sites that could compromise confidential information. Web applications and Web sites are vulnerable to a range of threats, including cross-site scripting attacks, injection attacks, misconfigurations, and others. Compromised sites can put their visitors at risk as well, especially with drive-by downloads that could infect client devices with malicious software.

Consider the need to block access to Web sites and Web applications unrelated during secure sessions. The same security applications that implement secure browser sessions should provide a URL-blocking mechanism as well.

Prevent Inappropriate Copying, Saving, and Printing

Sometimes seemingly innocuous activities such as copying, saving, and printing can present security risks. The employee described earlier who is attempting to land a job with a competitor by promising access to new customers would probably not want to print the client list in the office; instead, she might decide to download and print documents from home. A secure session that blocks printing, saving, and copying could thwart that attempt.

Here is an example of where defense in depth demonstrates its value. In theory, the unethical employee should not have had access to the content in the first place, but because of an oversight, she did. The first line of defense, SharePoint access controls, was not in place, but fortunately, another security control was in place that blocked the data leak.

User actions, both intentional and unintentional, can lead to data leaks. Implementing SharePoint access controls, blocking access to unnecessary Web sites and applications, and blocking inappropriate copying, saving, and printing can help improve the security of SharePoint content. In addition to securing browser sessions and limiting user actions, we should consider security management activities.

Manage Browser Sessions Securely

SharePoint users can access content from virtually any Web-accessible device, so it makes sense to manage browser sessions and related security centrally. In particular, look for browser session security tools that support:

- Policies that can be applied to company-owned devices as well as employee-owned devices
- Define and enforce acceptable use policies
- Log and review user activities

Reviewing activities can help identify attempts to inappropriately copy, save, or print documents from SharePoint sites. Even in cases where the attempts are blocked, log data about such activities may help identify patterns that need further investigation.

Summary

Microsoft SharePoint is a widely deployed collaboration tool that is easy to use and fits the needs of many organizations. One of the reasons SharePoint is so easy to use is the ability to access SharePoint sites from browsers. This feature does, however, have its disadvantages with regards to security and protecting SharePoint content. Fortunately, there are applications available that can secure browser sessions, help control user activities during secured sessions, and provide for centralized management. Browser-securing applications can mitigate many of the risks described here without adversely affecting legitimate use of SharePoint sites.