Realtime publishers

Securing SharePoint Content

The Essentials Series

sponsored by

Dan Sullivan

Copyright Statement

Technical Challenges to Securing SharePoint Content

Browsers are a key client technology for accessing and manipulating SharePoint content. Although Microsoft provides SharePoint-specific client applications, such as SharePoint Workspace, the browser is a standard for SharePoint access. The advantages of using a browser with SharePoint include SharePoint hosting services and cross-platform (including Bring Your Own Device—BYOD) support as well as avoiding the need to install a client application. With these advantages, however, come technical challenges. Together, these challenges create conditions that can be exploited to intentionally steal or unintentionally leak confidential data stored in SharePoint repositories.

Browser Vulnerabilities and Internal and External Threats

When you try to understand risks to your information, it sometimes helps to think like an attacker trying to steal your content. We will assume for the moment that you have valuable content in your SharePoint collaboration sites. The documents stored there might include trade secrets about business processes and products, strategic plans for business expansion, or confidential information about clients and customers. The specifics are not too important; the crucial point is that your SharePoint content is the target of an attacker.

Thinking Like an Attacker

Begin by assuming you are an external attacker. You do not have legitimate access to the corporate network, and you cannot easily walk the halls of the company. Thus, your best bet is to steal information electronically. You could invest time and effort to probe the corporate network for vulnerabilities that would allow you to gain access to servers and applications. You could then work to avoid detection as you probe servers for software vulnerabilities, run password detection programs, and try other means to compromise servers. This method is one approach to content theft, but there is a path of potentially less resistance: target client devices.

Client devices are often subject to less control than servers. Users can install applications or browser extensions. Laptops and mobile devices are not always connected to secured corporate networks. Users may browse compromised sites or open malicious emails that lead to malware infection. In spite of best efforts by desktop administrators, client devices such as desktops and laptops can harbor malware that leave them easier targets than hardened servers. There are two particular types of external threats that are relevant to protecting SharePoint content: malware on the endpoint and browser cache mining.

Malware on Endpoints

There are many forms of malicious software (malware), including Trojan Horses, keyloggers, and rootkits. Trojan Horses, as the name implies, are applications that appear to be benign but are in fact malicious. For example, a utility for displaying weather updates on your desktop might also scan your drives and copy data to a centralized server.

Keyloggers are designed to capture keystrokes as you type, allowing attackers to collect usernames and passwords. Of course, attackers will also end up collecting everything else you type, but text-processing tools can easily analyze large volumes of keystroke data to find information of particular interest to attackers.

Rootkits are sets of programs that attack the operating system (OS) at low levels, allowing them to circumvent OS security controls. This kind of malware is especially difficult to eliminate. These are just three examples of malicious software that can reside on client devices.

Browser Cache Mining

A particularly promising target for some attackers is your browser cache. The browser cache is used to store data temporarily to improve browser performance. A cache is quite useful when navigating Web pages. For example, assume you are reading a long article divided into several Web pages. If at some point reading the article, you decide to go back to the previous page, you would probably click the previous page button on your browser. In theory, your browser could simply download the page again but doing so would unnecessarily take time and consume network resources. Instead, your browser keeps copies of data in local temporary storage known as the cache.

This setup sounds like a reasonable tradeoff of resources: some local storage is dedicated to storing browsing data temporarily in order to save time and network resources. Here again, we have to think like an attacker. Your SharePoint content, which may be well protected on the SharePoint server, may be cached on endpoint devices. Malware designed to scan and analyze browser caches could gain access to your SharePoint content. This attack is known as cache mining.

The benefits of caching apply equally well to SharePoint content as to other Web content, so we do not necessarily want to eliminate caching. We do, however, want to ensure that confidential or sensitive information is not retained in the cache longer than needed, say, after a user's session with SharePoint has ended.

In addition to caching data to improve browser performance, some online applications allow users to store copies of data on their client devices so that they can work offline. This functionality is useful for those who work in multiple locations or find themselves traveling with intermittent Internet access. The more data that is stored locally, however, the greater the potential for a data leak.

Internal Threats: Careless and Malicious Employees

In addition to the sophisticated, technical approaches an attacker may use to steal valuable information, there are more pedestrian methods. Some threats to business information stem from carelessness while others have more malicious origins.

In the course of the day, many of us try to streamline tasks to save time. We might, for example, download documents and email copies to collaborators who do not have access to the content in SharePoint. We might justify this task by thinking we are working more efficiently. Our business partner might need a piece of information in that document and we get it to them in the most efficient way possible. The problem with this approach is that we lose control of that digital copy of the document once it is emailed to our collaborator.

At that point, we have no control over how our collaborator shares the document. Will it be deleted after only the necessary information is reviewed? Will it be forwarded to someone else? Will copies be stored on email servers that might be attacked in search of valuable data? There is also the question of whether additional content in the document needs to be shared. Does the collaborator need to know everything in the document? Could we compromise our business by sharing too much information?

These are difficult questions to answer. Rather than risk the negative consequences of such carelessness, organizations can implement security controls that block inappropriate copying of SharePoint content from client devices. These controls have the additional benefit of blocking disgruntled employees or others who might intentionally attempt to steal data such as client lists or design documents.

Another type of challenge we face in protecting SharePoint content is the increasing use of employee-owned devices.

Increasing Use of Bring Your Own Device

Organizations are grappling with the increasing use of Bring Your Own Device (BYOD) practices. Employees are working with their own laptops, tablets, and smartphones to access content and applications on corporate networks. Although there are tools to help manage laptops and mobile devices, organizations have less control over endpoints. There are limits to what an IT organization can impose on BYOD users, and this reality creates potential conflicts. IT professionals may be responsible for protecting corporate information assets, but employees reasonably expect control over their devices. The potential for conflicting expectations is high.

Consider a user who installs a browser extension to help monitor the prices of products the user researches. When the user searches for a product or service, such as a flight from San Francisco to New York, the browser extension checks multiple sites and displays information about the best prices. To perform this kind of service, the extension needs access to the browser data. An employee might be willing to allow access to personal browsing information, but what about work-related browsing? Do IT professionals responsible for information security want SharePoint content exposed in that way?

In addition to apps and extensions users intentionally install, we should consider the possibility that employee-owned devices might not have adequate security controls in place. For example, do employees:

- Keep their anti-malware software up to date? Databases used by anti-malware software are updated frequently. Endpoint anti-malware programs should be configured to automatically check for and download data and program updates.
- Run vulnerability scanners to check for known vulnerabilities in software installed on the client? Vulnerability scanners were once tools limited to network and server administrators, but even end users can utilize tools like Microsoft Baseline Security Analyzer on their desktop and laptop devices.
- Update OS and application software? Malicious software can take advantage of vulnerabilities in widely used productivity or utility software. Keeping software up to date is a key security practice.

BYOD has many advantages for both employees and their employers. As with so many technologies and practices, there are benefits and drawbacks to employee-owned devices being used for business purposes.

Summary

Securing SharePoint content is challenging. Sending copies of documents from well-secured SharePoint servers to poorly secured endpoint devices can leave your information vulnerable to stealing or leaking. Threats range from malware to malicious employees. Changes in the way we work, particularly the increasing practice of BYOD, compound the challenges SharePoint administrators already face. The next paper in this Essentials Series considers techniques for addressing these challenges.