INFORMATION ECCURITON JULYAUGUST 2012 • VOLUME 14 • NO. 6

The Pen Testing Imperative

Why you need an internal team tracking down vulnerabilities

PLUS:

 HARNESSING BIG DATA FOR BETTER SECURITY
LOCKING DOWN SHAREPOINT

LOCKING DOWN SHAREPOINT

Businesses love Microsoft's collaboration software but can forget to secure it.

By Marcia Savage

EDITOR'S NOTE: Microsoft's SharePoint application has become a ubiquitous collaboration tool in the enterprise but securing it can be a tricky process. And all too often, companies fail to properly secure their SharePoint deployments, security experts say. In fact, a survey of SharePoint users released earlier this year by European security vendor Cryptzone showed that lax security practices were rampant among those polled. In this special report, we examine some of the issues surrounding SharePoint security and provide tips on SharePoint security best practices.

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

WITH A GOOGLE search and one minute of running one of his SharePoint hacking tools, it doesn't take long for security researcher Fran Brown to find exposed SharePoint administrative interfaces for a state health and human services department. The exposure—which could allow an attacker to add users and change information—is far from unusual. Brown, managing partner at security consulting firm Stach & Liu, finds this sort of stuff all the time. "I'm surprised at just how much SharePoint is out there and how much is vulnerable," he says.

Microsoft's Web-based collaboration tool has become pervasive in the enterprise, but experts say companies often overlook SharePoint security. Eager to enable collaboration among employees and third parties, organizations can neglect to lock down user access and take other steps to secure all their Share-Point instances. Since these SharePoint repositories commonly contain sensitive corporate information, that's risky business.

"I don't see SharePoint being secured nearly enough," says Michael Davis, CEO of Savid Technologies, a Chicago-based IT security consulting firm. "Think about what SharePoint does—by definition it's where all your crown jewels are."

<u>Securing SharePoint</u> can be complicated—there are a lot of aspects to it—but security experts cite several top <u>SharePoint security best practices</u> to focus on, including access control strategies, testing for exposures, and user education.

THE OCTOPUS

Collaboration is paramount for businesses today and SharePoint is easy to get up and running, resulting in many instances of it rapidly popping up across an enterprise, says Michelle Waugh, a senior director for the security business at CA Technologies. That's led to the term "SharePoint sprawl."

Adam Buenz, consultant at ARB Security Solutions, a Minneapolis-based firm that specializes in SharePoint security services, has seen a lot of Share-Point pilot projects snowball. "Now rather than just a pilot, it's a vital business system that's collected this business-critical, sensitive information. It can also assimilate a lot of other systems," he says.

"Once it gets to that point, defining expectations and assessing performance of the system becomes really difficult," adds Buenz, a Microsoft MVP. "It's a lot harder to rope an environment in than it is to start off in a proper state."

The problem, Davis says, is no one business unit ends up owning SharePoint

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

in the enterprise. "It's kind of an IT thing, kind of a database thing, kind of a business process thing," he says. "I call it an octopus—it has tentacles across many areas of the business."

In addition, the dynamic nature of the collaborative environment makes it difficult to manage, Waugh notes.

"From a security perspective, something that went into SharePoint as a nonsensitive document can in minutes change and become a highly sensitive document by virtue of a purposeful or inadvertent change to the content or movement of the document from one place to another," she says.

ACCESS CONTROL

The main problem organizations often have with SharePoint security is managing access to repositories with thousands of documents and hundreds of users, Davis says. Users can wind up with excessive permissions; for example, an employee might get access to an accounting repository that he or she shouldn't.

"Getting control of that by using proper [user] groups and privileges is the best way to reduce exposure of data," he says.

However, throw third parties into the mix, and managing access control becomes especially challenging. Today, many organizations are focused on securing SharePoint in extranet collaboration scenarios, according to Neil MacDonald, a vice president and fellow at Gartner.

"How are you going to have these users, who aren't employees, prove who they are? Are you going to support federation of identities? Are you going to manage these identities yourself? If so, where? You could use Active Directory but maybe you want to use an LDAP-enabled repository," he says. "It's a very complex decision with a lot of variables."

If an organization decides to manage the identities and use Active Directory, it's faced with additional questions, such as whether to permit self-provisioning and password reset, he says.

"How do you ensure sensitive information isn't disclosed inadvertently or inappropriately? You get into the governance issue of who takes responsibility for the ongoing management of these external identities, mapping for authorization and de-provisioning," MacDonald says. "All of the identity-related issues we've had internally in the past are just amplified."

There are a number of third-party tools that can help, such as Web access

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

management products from CA Technologies, Oracle and IBM, he says. Epok Inc. specializes in extranet access governance for SharePoint. A number of vendors offer technology to manage entitlements within SharePoint, including Quest Software, AvePoint, Axceler, Idera, and Lightning Tools' DeliverPoint.

Earlier this year, CA Technologies updated its SiteMinder Web access management and DataMinder (formerly CA DLP) products to provide fine-grained control of users' access to SharePoint content. DataMinder, which includes data classification technology from CA Technology's acquisition of Orchestria, scans the content and SiteMinder uses the content classification to determine access rights.

TEST FOR EXPOSURES

There are a lot of SharePoint components that need to be secured—the SQL Server database, Windows services that SharePoint uses, and administrative interfaces. Microsoft's guides for securing SharePoint aren't always straightforward, and it's easy to make mistakes in terms of permissions and exposed data, says Stach & Liu's Brown.

In his assessment work, he found there weren't any good tools to test Share-Point security configurations. "It wasn't easy to see if you've actually locked down everything correctly," Brown says. About 18 months ago he addressed the problem by developing the <u>SharePoint Hacking Diggity tools</u>, which are freely available SharePoint penetration testing tools for organizations to download and use.

"Our free hacking tools leverage techniques like <u>Google hacking</u> and URL brute-force scanning to identify exposed admin pages in your public Share-Point deployments," Brown says. "They're a great way to spot check and have confidence that you've locked down your access permissions correctly. Otherwise, you could miss simple misconfiguration issues that may have inadvertently exposed admin functionality to the whole Internet, leaving a huge door open into your SharePoint environments."

One tool is a dictionary of about 120 preloaded Google queries that assessors can use to find exposed SharePoint administrative pages, Web services and site galleries. Another tool, SharePointURLBrute, automates forceful browsing attacks to help assessors find permissions holes that allow unauthorized users to access SharePoint administrative pages.

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

Brown says the <u>Shodan computer search engine</u>, which allows users to find devices connected to the Internet, also can help assessors by making it relatively easy to find people using SharePoint and exposed administrative interfaces.

Another tool, a free third-party plug-in called <u>SUSHI</u>, is a good way to check user permissions, Brown says. The tool gives administrators the ability to see all the libraries and galleries a user has access to across a site collection. "It's a good way to visualize what people have access to," he says.

In his assessments, Brown has seen a lot of exposed SharePoint deployments belonging to the federal government, which he says he finds particularly concerning. He noted that published reports indicate the WikiLeaks breach involved brute force of exposed government SharePoint services. According to a <u>Wired report</u>, a government digital forensic expert testified that he found scripts on the computer of Army Analyst Bradley Manning, who is accused of leaking classified data to WikiLeaks, which pointed to a SharePoint server holding the documents.

POLICY AND TRAINING

One of the most important steps organizations need to take to secure their SharePoint deployments is to make sure users understand the sensitive nature of the information in the repositories, experts say.

"You need to make sure they understand the data they're accessing is critical and the risks associated with what they're going to do with it and where they're accessing it from," Davis says. Many times, employees who are in a rush to get work done will download a document like a project plan from SharePoint and upload it to a personal drop box, then access it at home or on vacation, he says.

"That is a big potential issue because you're moving [the data] from a secured environment to an unsecured environment the company doesn't know about," he says.

A survey of 100 SharePoint users released earlier this year by European security vendor Cryptzone showed that even though most of the respondents understand that taking data out of SharePoint makes it less secure, 30 percent were willing to take the risk if it helps them get their jobs done. Thirty-four percent said they didn't consider the security implications of SharePoint and 13 percent said protecting company data isn't their responsibility.

Content governance is as important as taking application security steps to

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

reduce the attack surface, says Buenz of ARB Security Solutions. "Controlling access and raising awareness of that information is important," he says.

Organizations should craft their governance plan early on and not make the mistake of thinking there is a universal template they can use for it, according to Buenz. "Remember there isn't an industry accepted governance plan—you have to craft one adapted to the business. This plan has to be updated in an organic fashion as the business grows and changes," he says.

His mantra to clients is to follow three R's—record, retain, and revise when dealing with changes to overall SharePoint application security and content governance. "Record every change, retain it and remember it will always be subject to revision," Buenz says. "All the material you have regarding the actual security has to grow with the environment."

In the long run, Davis says he expects the corporate collaboration trend to lead to more breaches. The increasing popular centralized Web-based repositories—not just SharePoint, but Google Docs and others—offer business benefits but also could potentially help attackers, he says. "If someone hacks into one thing, they get access to all of it."

MARCIA SAVAGE is editor of Information Security magazine. Send comments on this article to <u>feed</u>back@infosecuritymag.com.

Three Steps for Securing SharePoint

Restricting user permissions, server hardening and dedicated service accounts are critical. BY BRIEN M. POSEY

SHAREPOINT 2010 IS easily one of Microsoft's most complex products, and the task of securing SharePoint can be overwhelming. Even so, there are some relatively simple steps you can perform that will go a long way toward improving the overall security of your SharePoint deployment and ensuring the sensitive data it contains is protected.

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

STEP 1: LIMIT PERMISSIONS

One of the most common SharePoint security problems is users receiving excessive permissions. The principle of least privileges should be used any time a user is being granted access to SharePoint. Unfortunately, users are often given excessive permissions, either because it is easier for an administrator to assign blanket permissions over granular permissions, or because the administrator does not truly understand the SharePoint permissions model.

To give you a more concrete example, imagine a specific user needs to be able to manage a large group of sites, sub-sites, lists, and libraries. In that type of situation, the easy thing to do would be to make the user a site collection administrator. Unless the user requires the ability to manage every site within the entire site collection however, then making the user a site collection administrator grants the user excessive permissions. Unfortunately, there are no shortcuts to making sure SharePoint permissions are assigned in an appropriate manner. If you already have a SharePoint deployment in place, then a comprehensive audit is required in order to verify nobody has excessive permissions.

Although it is extremely important to assign users the least permissions within SharePoint, it's also important to remember that using a solid permissions model within SharePoint alone is not enough. SharePoint is an application that has other dependencies. In order for SharePoint to be secure, its dependencies must also be configured securely. Specifically, this means granting users the least permissions at the Active Directory level and assigning users permissions to SQL Server only if absolutely necessary.

STEP 2: HARDEN SHAREPOINT SERVERS

One of the most important steps an administrator can take toward securing SharePoint is server hardening. Server hardening is the process of reducing your server's attack surface. To start, isolate the various SharePoint server roles from one another. SharePoint Server 2010 consists of three primary server roles: The Web server role, the application server role, and the database server role. Although SharePoint will allow you to install all of these roles to a single server, it is better from a security standpoint to use dedicated servers for each role.

In the not too distant past, the idea of SharePoint Server role isolation was considered to be cost-prohibitive for smaller organizations because of hardware

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

and software licensing costs. Today, server virtualization makes it possible to isolate the various roles from one another without having to spend a fortune on server hardware. Licensing costs are also reduced in a virtual environment since the Enterprise and Datacenter editions of Windows Server are licensed for use on multiple virtual machines.

Although role isolation is a good first step, it isn't enough by itself. In order to truly harden your SharePoint servers you must reduce the server's attack

surface to the point that only the services that are absolutely necessary are running.

The first rule of attack surface reduction is that each server (physical or virtual) should be dedicated to one sole purpose. In other words, if a server is acting as a SharePoint application server, then you shouldn't also try to use the server as a file server, domain controller, etc. The server should run SharePoint and Share-Point only. Once you have made sure your SharePoint servers are not running any unnecessary software, it is a good idea to disable or remove any unnecessary server roles, features or system services.

Of course, there are exceptions to this philosophy. In most cases, there are

certain support apps that need to run on production SharePoint servers, such as antivirus and backup agents. Running these types of applications on your SharePoint Server is perfectly acceptable and in the case of antivirus software, critically important.

Once you have made sure your SharePoint servers are not running any unnecessary software, it is a good idea to disable or remove any unnecessary server roles, features or system services. Fortunately, Microsoft provides a <u>list of the services required for each of the SharePoint roles</u>.

Another way to harden your servers is to configure SQL Server to listen on non-standard ports. By default, SQL Server listens on TCP port 1433 and UDP port 1434. The fact that these ports are well-known and used consistently makes them a prime target for attack. As such, Microsoft recommends blocking UDP port 1434 and TCP port 1433. After doing so, you can configure SQL Server to listen on a different port. Of course, you will also have to make Share-Point aware of the alternate port assignment as well; organizations can refer to Microsoft's instructions for this.

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

STEP 3: USE DEDICATED SERVICE ACCOUNTS

One of the biggest security blunders administrators make with regard to Share-Point is the misuse of service accounts. During the initial setup, the administrator is prompted to supply service accounts for SharePoint to use; the specifics vary depending upon how SharePoint is being installed.

From a security perspective, it's critical to use a dedicated service account for each function. When you supply a set of service account credentials for

SharePoint to use, SharePoint will assign special permissions to the account that enable it to be used for the task at hand. Normally, Share-Point will only provision the account with the bare minimal permissions required for performing the task at hand.

The problem occurs when you use the same service account for multiple purposes. Doing so causes the service account to begin to accumulate permissions that exceed those required to perform any one single task. Service accounts One of the biggest security blunders administrators make with regard to Share-Point is the misuse of service accounts.

that have been provisioned with excessive permissions could potentially be exploited.

At a minimum, Microsoft recommends administrators who are setting up a <u>SharePoint farm</u> use three service accounts. Those accounts are:

- SQL Server Service Account—This can be either a local system or a domain account, but for multi-server SharePoint deployments, domain accounts tend to work best. The service account is used for the MSSQLSERVER and the SQLSERVERAGENT services. If you are deploying a named instance of SQL server, then the service account will be used for services that correspond to that named instance.
- Setup User Account—The Setup User Account is used with SharePoint's Setup Wizard and the SharePoint Products Configuration Wizard. This must be a domain account and it must have administrative permissions on the server on which setup is run. Furthermore, the account must be added to the SECURITYADMIN and DBCREATOR roles that are found within SQL Server.

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

Server Farm Account—This account is used to manage and configure the SharePoint farm. It is also used to run the Microsoft SharePoint Foundation Workflow Timer Service and to act as the application pool identity for the SharePoint Central Administration website. The account must be a domain account. The account you specify is automatically added to SQL Server and given the DBCreator, SecurityAdmin, and DB_Owner roles within SQL Server.

It's important to remember that comprehensive SharePoint security consists of far more than these three steps. Other steps to consider include having a patch management solution in place, running the Best Practices Analyzer on a regular basis, and placing your SharePoint servers behind an application firewall. ■

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY

BRIEN M. POSEY is an eight time Microsoft MVP with two decades of IT experience. Before becoming a freelance technical writer, Brien worked as a CIO for a national chain of hospitals and health care facilities. He also served as a network administrator for some of the nation's largest insurance companies and for the Department of Defense at Fort Knox. Send comments on this article to <u>feedback@infosecuritymag.com</u>



EDITORIAL DIRECTOR Michael S. Mimoso

> EDITOR Marcia Savage

SENIOR SITE EDITOR Eric Parizo

SENIOR MANAGING EDITOR Kara Gattine

ASSISTANT SITE EDITOR Brandan Blevins

DIRECTOR OF ONLINE DESIGN Linda Koury

CONTRIBUTING EDITORS

Michael Cobb, Scott Crawford, Peter Giannoulis, Ernest N. Hayden, Jennifer Jabbusch, David Jacobs, Diana Kelley, Nick Lewis, Kevin McDonald, Gary McGraw, Sandra Kay Miller, Ed Moyle, Lisa Phifer, Ben Rothke, Anand Sastry, Dave Shackleford, Joel Snyder, Lenny Zeltser

USER ADVISORY BOARD

Phil Agcaoili, Cox Communications Richard Bejtlich, Mandiant Seth Bromberger, Energy Sector Consortium Mike Chapple, Notre Dame Brian Engle, Health and Human Services Commission, Texas Mike Hamilton, City of Seattle Chris Ipsen, State of Nevada Diana Kelley, Security Curve Nick Lewis, Saint Louis University Rich Mogull, Securosis Tony Spinelli, Equifax Matthew Todd, Financial Engines

VICE PRESIDENT/GROUP PUBLISHER

Doug Olender dolender@techtarget.com

ASSOCIATE PUBLISHER

Peter Larkin plarkin@techtarget.com

TECHTARGET

275 Grove Street, Newton, MA 02466 www.techtarget.com

©2012 TechTarget Inc. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher. For permissions information, please contact The YGS Group.

About TechTarget:

TechTarget publishes media for information technology professionals. More than 100 focused Web sites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

Cover: Getty Images/Liquidlibrary

EDITOR'S DESK

PERSPECTIVES

SCAN

[IN] SECURITY

TESTING FROM WITHIN

HARNESSING BIG DATA FOR BETTER SECURITY