Many admins and IT managers mistakenly fail to properly protect SharePoint. This e-guide, from our experts at SearchWinIT.com, explores four SharePoint security aspects that should not be overlooked.

SharePoint Security Should Not Be an Afterthought

Microsoft SharePoint has been around for 10 years now and it seems every company I work with uses it in some fashion. However, I’m always surprised at how frequently SharePoint security is an afterthought. Companies go to great lengths to protect servers running Windows, IIS and SQL Server, yet SharePoint controls are often overlooked.

Enterprises often see SharePoint as not quite a server and not quite a Web application. This view is the heart of the problem. Not only is SharePoint a public/private Web system, but it is an entire collection of systems that contains an abundance of sensitive information. And most of these systems can be accessed and exploited from inside your own network.

SharePoint has plenty of built-in security controls, but that doesn’t mean it is inherently secure. Below I’ve listed the top security issues facing SharePoint deployments:

1. Failure to take internal security policies and plans into account

I see lots of configuration and administration inconsistencies in SharePoint. And having a development team manage SharePoint systems -- which so many do --can create accountability problems. Be sure you always have the answers to the following:

- Who maintains SharePoint and its related systems?
- What security hardening standards do you use?
- Which Windows domain policies apply?
- How is data backed up?
Contents

SharePoint Security Should Not Be an Afterthought

1. How does the system fit into existing business continuity and incident response plans?

2. Failure to test the Web side of the system
   It’s easy to use a generic vulnerability scanner to scan the IP address of a SharePoint server -- and many do. However, many overlook the Web side of the equation.

   SharePoint environments have the same application vulnerabilities as traditional websites and applications. Don’t be scared to dig a little deeper to find everything that matters. This is especially important with SharePoint because there is so much custom code.

3. Failure to properly maintain patches
   Numerous server-side vulnerabilities have been uncovered in SharePoint. In fact, a simple search that uses the QualysGuard vulnerability scanner database reveals a couple of dozen vulnerability checks that apply directly to SharePoint.

   Consider Windows, SQL Server and IIS-based flaws that can be exploited as well. All it takes is a bored or unruly insider with a free vulnerability scanner and the free Metasploit tool to find and exploit missing patches and effectively “own” your system. Adding insult to injury, odds are that you’ll never know the exploit happened.

4. Failure to account for the mobile workforce
   It’s one thing to have SharePoint data locked down in the data center or in the cloud, but once you bring iOS, Android and Windows Mobile systems into the equation, you’ve got an entirely new set of issues.

   Chances are your users access SharePoint remotely. But just how secure are their mobile devices? Do they have password protection or encryption set up? How is their data being backed up? Are they properly protected from malware?
Many agree that mobile devices are becoming the new desktop, so it’s critical to keep these issues in mind. I suspect we’ll will have a slew of new mobile security risks in the near future.

Just because SharePoint sits behind a firewall, you cannot install it blindly and assume all will be well. Dig in and see what’s at risk. You may surprise yourself.
Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web’s largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more—drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

➢ SearchEnterpriseDesktop
➢ SearchWindowsServer
➢ SearchDataCenter