VTC
Virtual Training Center for SharePoint 2007

Layered Security Modeling for SharePoint Portals

ABOUT THE AUTHOR

Devereaux Milburn is the author of VTC for SharePoint 2007. As the lead SharePoint architect and developer, he serves as an advocate of solutions, tools, and techniques that promote the advancement of information systems, collaboration, and internet communications through proper adoption of Share-Point technologies.

His training solutions have been employed at Nike, Intel, Cisco, Medtronic and Booz Allen Hamilton to successfully on-board millions of users and accelerate adoption rates. In addition to training other SharePoint consultants and IT shops on how to implement SharePoint, his SharePoint Developers Academy is taught in multiple continents to quickly retool web teams with the skills, discipline and theory to govern and deploy enterprise-class SharePoint portals.

SoftwareFX
Data visualization for every need, every platform

As SharePoint has proliferated across the landscape there has been a phase shift in how organizational information is kept secure. In one aspect, business assets are more secure employing a formally built and community tested Microsoft technology. This is in stark contrast to the past model where each organization tried to home grow web applications from scratch with internal resources; some web teams more experienced than others on security. However the flip side is that with SharePoint so easy to install via the wizard, thousands of SharePoint portals were created in a cavalier fashion without formal security model and thus vulnerable to exploit or compromise.

This issue of The SharePoint CollaborusTM addresses 10 key elements that help to achieve a security posture with your organization's SharePoint implementation. While not a recommendation for a specific model, each role below outlines a layer that when combined with other layers provide progressively higher levels of security. The key in addressing the security of your SharePoint platform is to ensure that each role is addressed and a formal model adopted based on the risk your organization can accept and resources it can provide.

#	ROLE	DESCRIPTION / BENEFIT	ISSUES / RISK
1.	Dedicated Web Team	Managing trust boundaries vertically and horizontally in a site collection is an engineering discipline. SharePoint's easy web tools provide a management *capability*, but does not provide the *ability* for a user to know how to manage security. Essentially, the product's *capacity* for security is dependent on the administrator's *capabilities* which come from formal training and experience.	It is critical to appoint trained professionals to manage security. 99% of all SharePoint security violations are due to SharePoint purposefully being told to associate *UserA to AccessLayerB* by a user not trained on security modeling.
2.	Dedicated Network IT Staff	Governing enterprise hardware is not an ancillary responsibility when there's time to do so, rather it's the core competency of an IT professional. In addition to the years of experience and certifications one must have, a Network Engineer is more aware of the variables to harden and monitor an environment; not just using the wizard to set it up.	
3.	Network Operations Center	Physical controls are just as important as virtual ones. Even with all other security layers added, an environment can be easily compromised if servers are sitting on a desk or in rental offices. Access control to the building, NOC, cabinet and machine all provide layers of security and are important. Each datacenter has different levels of physical security in place and may vary whether they use keys, electronic, and/or biometric access controls.	
4.	Secure Socket Layers	Adding SSL to a website allows packets of data (representing the file or web page) to be transferred between the server and the destination computer in an encrypted state. This ensures that any potential "listener" of the session would not be able to see the contents of the transmission. Employing SSL may be helpful to add if the SharePoint portal is deployed as an extranet, or is transmitting potentially sensitive/proprietary content.	The IIS worker process that is responsible for crawling content for the search indexes cannot crawl in an encrypted state. Thus going with SSL kills indexing and search results. A locked down, non-SSL local mirror on the same server is required to sustain indexing and search results.

5.	**Authentication Method**	**Integrated Windows Authentication** relies on Kerberos authentication protocols and is more secure for authenticating into SharePoint sites. It is encouraged to use it, however many Share-Point sites are demoted to using **BASIC** authentication which is less secure	
6.	**Dual Factor Authentication**	Dual factor authentication provides advanced security for websites and relies on: A) Something a user knows (ie: a password) B) Something a user has (ie: Key Fob, thumb print, etc) Employing both factors in concert ensure that the system is not vulnerable if a user's password is shared or compromised.	Between licensing and hardware for every user (ie: key fobs), dual factor authentication has historically been very expensive to implement. Additional costs are incurred to provide staffing resources to train and support users adoption of Dual Factor authentication.
7.	**Domain Policies**	Through effective use of Group Policy, all domain users can have requirements on their system accounts. Standards vary based on the SOPs of the organization, but usually include having a password of minimum length, using special characters, and enforcing expirations to ensure passwords are changed regularly.	If a full extranet where users are not on LAN terminals, additional enhancements to SharePoint need to be made to provide the password management, notification and reset tools normally provided through a network login.
8.	**Intrusion & Virus Detection**	Employed to detect several types of malicious behaviors that can compromise the security and trust of a computer system, an intrusion detection system is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems for threats from the outside. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).	
9.	**Server Maintenance Schedules**	Server maintenance includes all physical and virtual servers in the farm, their operating systems, and add-ons such as SQL server or SharePoint. As new vulnerabilities or design flaws are discovered, Microsoft issues hotfixes, Windows Updates, and Service Packs. When risks are logged by the community, network engineers must gauge whether the maintenance should fall in the next scheduled window, or based on the organization's SOPs be fast tracked for immediate implementation.	
10.	**Virtual Private Network Tunnel**	Though use of a VPN, a SharePoint site can be restricted to LAN access only which ensures there is no remote access. However, that level of restriction excludes both potential hackers and staff alike. Making a SharePoint only accessible from a VPN does ensure only VPN users can access it, but simultaneously demotes it from an Extranet to an Intranet.	Users will always have an added sequence of steps to participate in the environment which may limit their participation. Additionally, an increase in support staff is required to train users how to download, install, and connect into the VPN environment.

This Makes You Look Better.

Introducing DataParts, Data Visualization Tools For SharePoint 2007

DataParts is a powerful new way to add interactive business intelligence to SharePoint portals. With DataParts, visualizing and analizing data becomes remarkably easy -and code-free. DataParts includes our complete suite of advanced lists, card views, charts, digital panels and gauges as web parts that can easily configured for the type of data desired in just minutes.

This Makes Your Life Easier.

Introducing VTC, The Virtual Training Center For SharePoint 2007

With VTC, IT and help desk personnel will no longer be overloaded with SharePoint questions and training tasks. VTC delivers a complete program of expertly produced, self-paced tutorial modules designed to empower every user and maximize the value of every SharePoint feature. VTC installs in minutes on your server - providing instant on-demand access for everyone in your organization.

DataParts

VTC - Virtual Training Center

WSS 3.0 and MOSS 2007

Visit SoftwareFX.com for free trail versions, interactive demos and more information about our latest products

SoftwareFX

Data visualization for every need, every platform