
Microsoft Office
SharePoint Server,
Modelación de riesgos,
y 34a Labs Prevent
Server

Informe técnico

Robert B Yonaitis

Contenidos

Introducción.....	3
Los participantes.....	4
Definición de los vectores de riesgo básicos	5
La perspectiva de la accesibilidad.....	6
La perspectiva de la privacidad.....	6
La perspectiva de la seguridad de las operaciones.....	6
Soluciones	7
Prevención en vez de seguimiento	7
Soluciones confiables basadas en estándares	7
Resumen	8
Términos técnicos.....	8
Acrónimos	9

Introducción

En el mundo actual de los negocios es difícil encontrar una empresa que no cuente con políticas y procedimientos específicos para manejar la información privada, los datos de los empleados y la información confidencial (datos económicos, de los clientes, etc.). Estos procedimientos protegen la organización y ayudan a minimizar los riesgos. Sin embargo, no es de extrañarse que muchas organizaciones no hayan tenido en cuenta el riesgo que representa para esta información, así como para el cambio de paradigma, la migración de algunos de estos datos a Internet a través de los sitios Web, las aplicaciones Web y las herramientas de redes sociales tan comunes en el ámbito del Enterprise 2.0 (E2) y el Government 2.0 (Gov 2.0). Al igual que los Departamentos de Recursos Humanos, el Departamento de Informática debe adoptar políticas y procedimientos que se ocupen de regular un amplio rango de problemas de conformidad, que abarca desde los datos de los empleados y los clientes hasta la seguridad general y la seguridad basada en funciones. Estas políticas se presentan habitualmente a través de modelos de riesgo.

Existen muchas definiciones para Modelación de Riesgos y se encuentran disponibles muchos libros que tratan del tema. Este documento usa un modelo de riesgo “software-céntrico” y examina algunos de los vectores específicos de riesgo relacionados con la información manejada a través del Microsoft Office SharePoint Server. También presenta medidas preventivas y otros factores a tener en cuenta para crear un ambiente seguro. Nótese que este documento presentará nociones básicas y vectores de riesgo básicos para crear un debate bien fundado y promover un análisis más profundo, pero **no** fue creado con el propósito de ser un modelo de riesgo **exhaustivo**. En cambio, el lector deberá desarrollar su propio modelo para que se ajuste a su implementación.

Los participantes

Es importante que utilice un alcance lo más limitado posible en el momento de delimitar el objetivo central del modelo de riesgo. Este documento observará tres objetivos similares y un tanto asociados, que pueden ser usados por separado o juntos como una sola unidad.

El conjunto objetivo será específicamente **Microsoft Windows SharePoint Services, SharePoint Server 2007 y SharePoint Server Publishing Sites.**

A los efectos de este documento, **el vector de riesgo** será **el contenido conforme en general, incluyendo –pero no limitado a– todo el contenido creado o ingresado en el sistema.** Los autores de los ataques serán los usuarios del sistema (intencionalmente o no) y los sistemas automáticos designados para atacar SharePoint Server. Este documento no explica cómo manejar otras extensiones, archivos HTML o filtros simples de palabras, que se pueden tratar fácilmente con el Microsoft ForeFront™ Server: <http://www.microsoft.com/forefront/en/us/default.aspx>. Además, este documento no analiza los virus u otros riesgos específicos de la plataforma, sino que se ocupa de la interfaz y el contenido.

El participante que se encargará de manejar el contenido que se discutirá a continuación es el 34a Labs Prevent Server. Esta solución proporciona validación de conformidad con: accesibilidad, privacidad, seguridad de las operaciones, filtro de malas palabras, suite de pruebas para datos de contabilidad, sitios inapropiados, filtro de teclado extendido y suite de pruebas personalizada.

Definición de los vectores de riesgo básicos

SharePoint se ha convertido en un elemento de misión crítica para las empresas y las organizaciones gubernamentales, y se ha vuelto esencial para Enterprise 2.0 y Government 2.0. SharePoint no solo se puede utilizar para administrar el contenido, sino también para proporcionar una interfaz de usuario a la información de misión crítica manejada con SharePoint u otras aplicaciones aparte de ésta. Teniendo esto en cuenta, se deben tomar medidas para proteger la integridad de la solución y para defenderla contra los ataques intencionales. Los administradores de sistemas deben actuar como escudos contra los virus y los archivos malignos, mientras que el personal de Recursos Humanos y de Política Informática debe proteger el medio de errores de conformidad, riesgos y descuidos.

Cada uno de los elementos de conformidad enumerados en la sección anterior tiene un vector de riesgo específico a tener en cuenta. Este documento define las ubicaciones posibles de los objetivos. Un vector de riesgo crítico que se debe tener en cuenta es la “intención” de la solución. Como SharePoint es una herramienta de colaboración, tiene sentido que un agresor ataque los puntos de colaboración:

- Bibliotecas de documentos
- Blogs
- Wikis
- Sitios de trabajo en grupo
- Sitios de publicación
- Y cualquier otra colaboración, reunión, empresa o sitio de publicación que se pueda implementar

La perspectiva de la accesibilidad

La accesibilidad al sistema y al contenido no es un ataque, no obstante representa un riesgo. En principio, el contenido no accesible puede representar un riesgo legal para la organización. Por otro lado, una persona que no consiga acceder a la información dado su carácter de inaccesible, puede intentar obtenerla de alguna otra forma, y esto puede convertirse en un nuevo riesgo ya que es posible que esa persona acceda a la información furtivamente por una puerta trasera del sistema. Algunos de los vectores de riesgo básicos a tener en cuenta son:

1. El agregado de un documento no accesible a la biblioteca de documentos
2. Los cambios a un Template (plantilla) que no es accesible
3. El contenido no accesible agregado por el usuario

La perspectiva de la privacidad

Los problemas de privacidad pueden representar un ataque o no. Algunos de los vectores de riesgo básicos a tener en cuenta son:

1. El ingreso en un blog (por parte de un usuario) de datos personales de uno o más empleados como respuesta a un posteo, que puede causar daños a la empresa al violar la política de privacidad.
2. El agregado (por parte de un usuario) de documentos de Recursos Humanos, como contratos o salarios, a un almacén de documentos sin protección
3. La creación de un template (plantilla) para un sitio de publicación sin contar con la información de privacidad necesaria

La perspectiva de la seguridad de las operaciones

Puede ser un ataque o no. Algunos de los vectores de riesgo básicos a tener en cuenta son:

1. El ingreso en un blog (por parte de un usuario) de información personal acerca de la ubicación de uno o más oficiales o de datos personales no relacionados
2. El agregado de documentos que incluyen los movimientos de las tropas
3. La creación de un wiki por parte de un usuario que contenga información de una determinada arma que le gusta

Soluciones

Implemente una solución proactiva que prevenga el ingreso de datos malignos y no malignos en el sistema. Desde el momento en que se ingresa contenido con problemas de conformidad en el sistema, éste ya se encuentra en riesgo. 34a Labs Prevent es más que una solución de seguimiento, es una solución proactiva. Tiene un enfoque completamente diferente que le permite a usted evitar los problemas de conformidad antes de que ocurran. Al ser un servicio Web para empresas de alto rendimiento, 34a Labs Prevent se combina con el sistema de gestión del contenido para enviar resultados inmediatos al sistema. Los resultados abarcan diferentes parámetros: Aprobado, Reprobado, Validar, Mensaje y Desviar. Los mensajes y el desvío los controlan los administradores para evitar efectivamente que los datos problemáticos sean importados al almacén de documentos o publicados en él. Con 34a Labs Prevent también es posible limpiar los datos y luego publicarlos.

Prevención en vez de seguimiento

En el pasado, hacer un seguimiento del contenido y reparar los errores después de que se habían cometido tenía razón de ser dado el alto porcentaje de datos estáticos en Internet. Hoy en día, Internet cuenta con una combinación amplia de escenarios de gestión de contenido, microblogging, E2, Gov 2.0. Existen incontables tipos de medios sociales. Para cuando haya encontrado el problema con una solución post-producción, el riesgo ya estará presente y probablemente ya habrá sido reproducido en distintos servidores. Es por eso que el seguimiento estático no sirve.

Soluciones confiables basadas en estándares

Cuando se trabaja con soluciones de seguridad, es importante tener en cuenta que una solución no resuelve todos los problemas, por eso la solución debe estar basada en estándares. 34a Labs Prevent está basada en estándares. Conduce cada prueba por medio de servicios web para empresas que han

sido evaluados con pruebas de carga que comprueban el funcionamiento con un determinado número de usuarios concurrentes en ambientes empresariales simulados; almacena los datos en una base de datos construida especialmente para optimizar su velocidad; utiliza EARL para niveles de toma de decisiones reales al momento de comprobar los resultados: <http://www.w3.org/WAI/intro/earl.php>; desarrolla y prueba las soluciones usando los mejores métodos de ingeniería estructural y garantía de calidad extendida. Todas estas características evidencian la fiabilidad de esta solución. Nuestro objetivo es que el usuario piense que 34a Labs Prevent es como la “electricidad”: es algo que siempre está fluyendo, pero que nunca debemos tocar.

Resumen

Este documento proporcionó un análisis introductorio del SharePoint Server y de la creación, a través de él, de un Vector de riesgo para las organizaciones. Los aspectos básicos de la modelación de riesgos fueron examinados teniendo en cuenta ataques específicos a grupos de conformidad específicos. Para poder manejar la conformidad efectivamente con SharePoint debe pensar en los términos y las prácticas de la modelación de riesgos en relación con el software informático. Hacer un seguimiento del contenido que ya se encuentra expuesto no previene los riesgos. De hecho, el seguimiento solo le permite darse cuenta de que ya se encuentra en una situación comprometida. 34a Labs Prevent Server lo puede ayudar a prevenir los riesgos de forma proactiva y a defenderse de ellos. También es posible que desee realizar una evaluación de la seguridad en relación con la conformidad. Para más información, diríjase al sitio web de 34a Labs: <http://www.34alabs.com/>

Términos técnicos

Modelo de riesgo: Si bien existen múltiples definiciones para este término, a efectos de este trabajo, se refiere a la seguridad informática, en la que el diseñador del software de aplicación se preocupa por la seguridad y los problemas de conformidad relacionados con los riesgos de conformidad o sistema.

Vector de riesgo: Es la ruta que una persona o una herramienta puede utilizar para atacar el objetivo especificado en el modelo de riesgo.

Acrónimos

E2 – Enterprise 2.0, nueva tecnologías para administrar las operaciones dentro de una empresa

Gov 2.0 – Government 2.0, nueva tecnologías para administrar las operaciones del gobierno