VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
www.tecnimap.com
Ponencias

Valoración de la Seguridad
Primer paso hacia la Seguridad de la Información

Ceferino Raposo

Director de Desarrollo de Negocio de GE Capital ITS.

1 TECNOLOGÍA Y RIESGO

Las Tecnologías de la Información (TI) se han convertido en el combustible que alimente el motor del comercio, permitiendo a las organizaciones que mejoren sus procesos de trabajo, reduzcan los costes operativos y, por último, impacten de forma positiva los resultados. Utilizando apropiadamente las TI cualquier organización puede alcanzar altos nivels de proudctividad, muchisimo mayores de los que podrían ser alcanzados nunca sin el uso de la tecnología. Sin embargo, aunque la tecnología tiene un enorme impacto positivo en las actuaciones de las organizaciones, también conlleva un riesgo sustancial asociado.

Hoy en día las organizaciones son cada vez más dependientes de la tecnología para el soporte de sus operaciones diarias, por lo que el impacto en estas por la perdida (o por una disrupción seria) de los recursos asociados resulta sustancial. En muchos casos, los procesos de trabajo han evolucionado hasta un punto donde un proceso manual no puede ser utilizado en casos de emergencia para mantener activas las operaciones. En la mayoría de las organizaciones

modernas, el coste de una disrupción del sistema o en los recursos tecnológicos puede medirse en miles, e incluso, millones de euros por hora. De hecho, un evento de la suficiente gravedad puede dejar a una organización fuera de su negocio.

El reto viene a ser, para cualquier organización, identificar el nivel de riesgo que es inherente al despliegue de la tecnología que necesita y desarrollar un plan estratégico que ayude a mitigar esos riesgos. Una de las tendencias interesantes a destacar al hacer las consideraciones de calculo de riesgos, es que en la medida que una organización se mueve hacia arriba en la curva tecnológica, el crecimiento de la curva de riesgo es aún mayor.

Antes de calcular el nivel de riesgo propio, es necesario entender el riesgo individual que está presente al depender de una tecnología determinada y, a la vez, entender que impacto puede tener cada riesgo en la organización. Algunos riesgos ocurren con cierta frecuencia, pero son de un impacto mínimo, mientras que otros rara vez ocurren, pero tienen un impacto tremendo en la disponibilidad del servicio.

Algunos de los factores comunes de riesgo son los siguientes:

Fallo en la Conectividad. Pérdida de la conectividad entre un cliente potencial y el sitio de intercambio electrónico.

Sobrecarga del Sistema. Un nivel de actividad mayor que la capacidad del sistema para aceptarlo.

Divulgación de material confidencial. Se pública de forma inadvertida información sensible de los clientes.

Sobrecarga de Volumen de Trabajo. Un volumen de ordenes de servicio que sobre pasa la capacidad del sistema para atenderlas.

Integridad comprometida. La información que reside en el sitio web es alterada de alguna forma no autorizada.

Pérdida de Información. Información o solicitudes del sitio web se pierden o no pueden ser recuperadas.

Los riesgos con mayor impacto los constituyen aquellos que son frecuentes y tienen consecuencias sustanciales; estas son las áreas donde hay que incidir con los mayores esfuerzos. Los hechos que son menos frecuentes, pero que toda-

vía generan un alto impacto, deben recibir el siguiente nivel de atención. El resto de las categorías deben recibir el menor de los esfuerzos. Utilizando esta estrategia, se dedicará el mayor esfurezo a las áreas que poseen el mayor riesgo potencial para la organización.

El papel de la Seguridad de la Información en la Valoración del Riesgo

Uno de los mayores riesgos de la tecnología en cualquier organización lo constituye la falta de una Seguridad de la Información consistente. Una organización que falla en asegurar de forma apropiada sus recursos corre el riesgo de que información sensible pueda ser robada, que operaciones y procesos importantes sean entorpecidos, así como recursos críticos puedan ser destruidos.

Un factor importante a tener en cuenta, en todo lo relativo a la seguridad de la información es que, a diferencia de los desastres naturales o eventos similares, los temas de seguridad son predecibles y, en la mayoría de los casos, prevenibles. Es improvable que, independientemente de lo que se haga, se pueda evitar el proximo desastre natural, sin embargo, una buen esquema de seguridad de la información puede, definitivamente, prevenir (o al menos, reducir el impacto de forma apreciable) la amenaza proveniente de un hacker contra sus sistemas de información.

Amenazas a la Seguridad de la Información

El reto, dentro de este contexto, consiste pues en asegurar una protección adecuada sin malgastar recursos. En la tabla que se presenta a continuación se enumeran las amenazas más comunes, de cara a los recursos tecnológicos de la organización.

Amenaza	¿Qué hace?	Impacto
Hackers/Crackers	Personas dentro o fuera de la organización que intentan penetrar en la red con el objeto de tener acceso a información confidencial o para entorpecer la operación de los servicios	Imagine el daño que puede causar que las historias médicas de los pacientes sean envíadas por e-mail a un períodico, o que sea alterada la información en el sistema farmaceútico
Virus	Estos son programas que infectan los ordenadores en la red y se distribuyen de forma automática de una máquina a otra. Dependiendo del tipo de virus, este puede destruir la información, apagar equipos o interferir de forma general con la operación del sistema	Una vez que un virus está activo en el sistema, puede dañar cualquier fichero del mismo, borrar cualquier cosa que este almacenada y entorpecer la operación del equipo. En algunos casos, un virus puede bloquear la operación de un segmento crítico de la red simplemente envíando muchas copias de un mensaje.
Troyanos	Es un programa (similar a un virus) que infecta maquinas en la red. La diferencia radica en que estos programas permiten el acceso a la máquina fuera del control del dueño del sistema	Utilizando troyanos, un atacante puede acceder a cualquier cosa que quiera. Riesgos potenciales de un Troyano incluye: enviar correos electrónicos falsos utilizando el nombre del dueño del sistema, acceder o alterar documentos sensibles o, comprometer sistemas críticos en la red
Negación de Servicio	Servidores críticos y recursos de la red pueden resultar desabilitados, de forma tal que los usuarios no tienen acceso a los mismos	En caso de que el sistema de admisión, o el de farmacia no estuviera disponible durante 24 horas, ¿Cuál sería el impacto en su organización?
Errores del usuario	Nunca atribuya a la malicia lo que puede ser atribuido a la incompetencia o a errores. La gran mayoría de los problemas en los sistemas vienen dados por errores que cometen las personas	Un administrador de sistemas tiene, de hecho, un poder sin restricciones para alterar o modificar un sistema en producción. Si esa capacidad no está controlada, no existe limite al daño que se puede generar en un sistema
Pérdida de la Propiedad Intelectual	Cualquier cosa que pueda ser hecha, también puede ser robada.	En muchos ambientes de la economía este es la mayor de las amenazas, pues representa la pérdida del conocimiento desarrollado a expensas de las organizaciones.

Una vez identificados las amenazas más comunes, el siguiente reto lo constituye el entender que se puede hacer para protegerse de ellos.

¿Qué es la Seguridad?

Dentro de este contexto es importante destacar que Seguridad no es igual que Secreto. La Seguridad debe ser entendida como una combinación de Confidencialidad, Disponibilidad e Integridad. La Confidencialidad es la posibilidad de revelar información clasificada en completa confianza. Disponibilidad constituye la posiblidad de proveer acceso bajo completa confianza, nuevamente, a ciertos recursos cuando es requerido. Integridad, es trabajar en una condición sana, inalterada.

¿Dónde Comenzar?

Uno de los problemas con la Seguridad consiste en determinar donde comenzar. El común de las organizaciones hoy en día no posee un entendimiento cabal de lo que puede haber instalado en la red, de que forma está protegido, o si se está sufriendo un ataque. Para aliviar esta situación es necesario un programa de seguridad.

Un buen nivel de seguridad se consigue planificando de antemano e implantando servicios de seguridad comunes. La realidad de hoy en día es que las aplicaciones, y las transacciones que realizan los usuarios abarcan un abánico muy amplio de programas que operan en varias plataformas. Con esta proliferación multi-plataforma, las organizaciones enfrentan el reto de vencer un entorno de seguridad heterogeneo que, por lo general, conduce a una seguridad inefectiva, construida sobre implantaciones disimiles. Por otro lado, el administrador de sistemas no puede desperdiciar su tiempo en gestionar las siempre cambiantes necesidades de seguridad. Por lo tanto, la infraestructura de seguridad de cualquier organización debe ser los suficientemente amplia como para soportor ambientes heterogeneos.

El concepto fundamental detrás de un programa de seguridad es el de ser capaz de construir un conjunto de servicios y recursos que, trabajando en forma acompasada, conforman una infraestructura de red altamente segura. Y, el primer paso, en implantar una infraestructura integral de seguridad es realizar una valoración de la realidad actual de la organización.

Utilizando inspeciones en el sitio, así como pruebas, un grupo de ingenieros puede hacer una revisión completa dela seguridad en la red de una organización determinada. Al final del período de valoración, esta organización tendrá una idea muy acertada de que tan vulnerable es y de que puede hacer para correjir los problemas encontrados.

Aunque no hay ningún program de segurida 100% efectivo, el objetivo del programa de seguridad de una organización debe ser el de ayudar a mantener unas defensas lo suficientemente sólidas, así como el riesgo de detección y prosesamiento criminal a un nivel tan alto, que aquellos que pensasen en amenzarla prefieran buscar una presa más fácil.

Test rápido de Valoración de Seguridad

Como una guía, es posible hacer una valoración rápida que, de forma inmediata, identifique áreas de preocupación. Este puede ser el primer paso en reconozer vulnerabilidades potenciales. Esta valoración rápida debe poseer unas preguntas básicas/genéricas y las respuestas documentadas a las mismas:

1. ¿Tiene mi organización alguna política corporativa de seguridad?
2. ¿Con qué frecuencia se revisan las políticas de seguridad?
3. ¿En qué forma educamos a nuestros funcionarios en las políticas corporativas de seguridad?
4. ¿Existe documentación sobre los mecánismos de contro de acceso?
5. ¿Se ha presentado, en alguna oportuindad, ataques de virus, scans, etc en mi organización?
6. ¿Cómo trata mi organización a sus empleados?
7. ¿Se hace cumplir la política corporativa de seguridad?
8. ¿Qué tan relevante es la política corporativa de seguridad?
9. ¿Se audita la Red de forma recurrente?

Formas avanzadas de Valoración de la Seguridad

Uno de los errores más comunes en los que caen las organizaciones es en el de la falsa sensación de seguridad. Con mucha frecuencia, una organización cualquiera despliega alguna tecnología o aplicación que se supone es la panacea y que provee el nivel de seguridad absoluto. Todo esto, solo para verlo fallar en un momento crítico. En realidad, no exis-

te un único producto, o una tecnología particular que pueda proveer una protección integral ella sola. La única forma de poder establecer un mecánismo de seguridad real es aplicando el concepto de "Defensa en Profundidad"

La estrategía de "Defensa en Profundidad" reconoce que la la verdadera seguridad de la información requiere una aproximación integral que analize los riesgos y que diseñe recursos que permitan proteger los sistemas contra estos. Por ejemplo, en un supermercado el poner una cerradura a la puerta no constituye una solución total. Una estrategia integral que incluya camaras de seguridad, procedimientos de auditoría financiera y un sistema sofisticado de alarma contra robos son elementos requeridos para establecer una seguridad integral.

Esta estrategía también reconoce que establecer una sola capa de protección, en la mayoría de las organizaciones, tiene una utilidad limitada. En consecuencia, para realmente establecer la seguridad de la información es necesario desplegar una arquitectura multicapa.

Los niveles indispensables a considerar son los siguientes:

Debe existir un mecánismo para restrigir el acceso. La primera línea de defensa la deben constituir los mecánismos de control de acceso que permitan que solo aquellos individuos autorizados puedan acceder.

Debe existir un elemento que supervise los accesos en curso y que asegure que cumplen las normas. La supervisión provee una mecánismos de alerta frente a un intento de violación de la seguridad (sea este exitoso o no)

Debe existir un recurso que registre que elementos han sido vulnerados. Una vez que la decisión de dar acceso a alguien, la actividad de ese usuario debe ser registrada de forma tal que se pueda generar un log completo de las actividades del usuario en cuestión. Este es un recurso invalorable de forma que se pueda entender que ocurrio después de un fallo en un sistema.

Debe existir una metodología para recuperarse de un fallo de seguridad. Aunque múltiples niveles de seguridad reducen la probabilidad de un fallo en el sistema, es también cierto que en un momento determinado del tiempo un fallo siempre ocurrirá. En ese caso, es de vital importancia que exista un mecánismo que permta recuperar el sistema de un fallo catastrófico.

La combinación de distintas capas hace posible que se pueda reducir de forma dramática la posibilidad de que un fallo relacionado con la seguridad ocurra en un sistema tecnológico. Dado que cada capa se construye sobre la capa anterior, la probabilidad de un fallo total es mínima. Y, aún cuando un fallo ocurra, la organización contará con los mecá-

nismos que permitiran recuperarlo. El reto consite en enterder como estos componentes se relacionan enter si, con el ambiente específico de la organización y con las necesidades de seguridad.

Para poder abordar una tarea de estas características utilizando una herramienta de inspección y prueba, un equipo de expertos puede realizar una valoración de la seguridad para cualquier organización. Al final del período de valoración, se puede tener una visión golbar de donde se encuentran las vulnerabilidades y que se puede hacer para corregirlas.

Es importante tomar conciencia que la seguirdad en una organización es un proceso que no tiene fin, por lo tanto una vez completada la valoración inicial y establecidos los pasos a seguir para mejorar la situación presente, hay que certificar que dichos cambios han sido aplicados con éxito y que no se presentan nuevos huecos en la seguridad del sistema.

Aplicando la estrategia de, consistentemente, subsanar las vulnerabilidades detectadas, supervisar que se mantienen sin alteraciones una vez correjidas y analizar las causas por las que se presentan las vulnerabilidades recurrentes; se garantiza estar en un modo de mejoramiento continuo. La realimentación que este proceso genera provee la información necesaria para establecer los mecánismos de mejora que requiere el proceso de seguridad y, por ende, garantizar que se mantiene constantemente actualizado y garante de la prtotección de los sistemas de información.