Reforzando la seguridad

El proceso de mantener una efectiva arquitectura de seguridad

Seguridad no es una iniciativa sino un proceso que debe responder a las necesidades de la organización y debe ser mantenida mediante una continua evaluación"

Primera Parte

Resúmen Ejecutivo

El mundo se ha convertido en un lugar más pequeño debido en gran parte a los avances en tecnología. La explosión de Internet y la relativa facilidad para accederlo ha creado un entorno donde la comunicación entre los continentes puede establecerse en segundos. Negocios, universidades, hospitales, gobiernos, militares y ciudadanos tienen acceso a este recurso y a su poder, el cual es restringido sólo por políticas corporativas y/o sus estándares de ética. El atractivo de INTERNET radica no sólo en la abundante información que puede encontrarse a través de él, sino también el bajo costo de acceso al mismo, razón por la cual esta herramienta se ha entrelazado en la red global de comercio. Lo cual ¡es una hazaña significativa para un recurso tecnológico que no es poseído o controlado por una organización multinacional, negocio o gobierno!

Nunca antes tanta gente tuvo acceso a tanta información y capacidad. La conectividad global puede ser alcanzada simplemente mediante un módem conectado a un teléfono o mediante una tarjeta inalámbrica dentro de una computadora personal o asistente de datos personales (PDA). Los usuarios demandan acceso a mayor cantidad de información en forma remota. Las corporaciones están tomando conocimiento de sus vulnerabilidades en relación con el mal uso de información y recursos tecnológicos. Sin embargo, la gerencia es consciente de la relación entre accesibilidad y productividad. La pregunta sería ¿cuál es el balance apropiado entre flexibilidad y disponibilidad para asegurar un control sin perder productividad?

Este trabajo trata sobre la necesidad de desarrollar y mantener un proyecto efectivo de arquitectura de seguridad y definir cómo CTG Entorno de Arquitectura de Seguridad MR (SAF) puede ayudar en esta integración entre la organización y las operaciones.

El problema: Demasiada disponibilidad y Demasiados Recursos

Nos hemos convertido en un mundo de consumidores demandantes que requieren una inmediata gratificación ya sea en el trabajo, el hogar o el juego. Cuando queremos o necesitamos información, bienes consumibles, servicios u otros, esperamos una respuesta inmediata. Esto sucede tanto en el trabajo como en nuestras vidas personales. Necesitamos teléfonos celulares para mantenernos en contacto, teléfonos con cámara para capturar los momentos compartidos con familia y amigos. Agendas personales para mantener nuestros cronogramas de tareas, contactos, responder urgentemente a los mensajes a través de correos electrónicos, computadoras portátiles para mantenernos en contacto con la oficina central mientras estamos en camino de regreso, hoteles con banda ancha, aeropuertos, hoteles, clubes, restaurantes y cafés que tienen conectividad a INTERNET sin cable, para poder estar conectados. Pero, ¿cuán seguro se encuentra usted mientras está conectado? ¿Cuán seguro necesita estar? ¿Cuáles son los temas relativos a seguridad y privacidad en la información que usted está enviando y recibiendo y cómo está asegurando que sólo los supuestos receptores lo están recibiendo? Estas son preguntas que se están realizando en entidades corporativas y agencias gubernamentales, que preocupadas por la protección, integridad y exactitud de la información sensitiva.

Seguridad: ¿cuánto es suficiente?

La presión de las organizaciones para construir o contratar una seguridad en la información robusta se está incrementando. Razones para incentivar esta necesidad son los mandatos legislativos, la responsabilidad de las empresas y las amenazas crecientes. En esta nueva era, las soluciones tecnológicas tradicionales en seguridad no son más suficientes para un adecuado manejo del riesgo.

Las organizaciones enfrentan nuevas regulaciones, tales como:

- Ley Patriot
- Ley Gramm-Leach-Bliley (GLBA)
- Ley de Información de seguridad y responsabilidad (HIPAA)
- California SB 1386
- FDA 21 CFR Parte 11
- Ley del 2003 sobre transacciones de crédito justas y precisas
- Acuerdo de Capital de Basilea II
- Directiva de la Unión Europea 95/46/EC
- Programa de seguridad de la información a los tenedores de tarjeta VISA
- Programa de protección de datos del sitio Mastercard
- Programa de estándares de seguridad de datos de American Express
- Ley Sarbanes Oxley

Reguladas o no, todas las organizaciones tienen la responsabilidad de proteger a los activos en posesión de sus inversores, los datos personales y financieros obtenidos de consumidores y ciudadanos e información confidencial compartida con socios del negocio. Además, las organizaciones con componentes de la infraestructura crítica de los Estados unidos (telecomunicaciones, sistemas de electricidad, gas y almacenamiento y transporte de petróleo, banca, finanzas, transporte, sistemas de provisión de agua, servicios de emergencia (incluyendo medicina, policía, fuego y rescate) y continuidad en el gobierno) tienen la obligación de proteger sus activos por el bien de la Nación.

Finalmente, para simplemente ser un buen ciudadano de Internet y evitar que la corriente lo empuje, las organizaciones deben asegurar que no se convierten en una base de lanzamiento para ataque contra otras organizaciones.

El constante incremento de simplificación y sofisticación de ataques contra servidores de red, bases de datos, servidores de redes internas y sistemas de compañías telefónicas implican que las empresas deben tener sistemas de seguridad pro-activos y procesos para detectar y manejar nuevos riesgos.

Bases para el proyecto amplio de arquitectura de seguridad

Una arquitectura de seguridad efectiva permite a una organización desarrollar o mantener sus ventajas estratégicas y competitivas. La información, tecnologías y personal son recursos con una misión crítica distribuidos a través de la organización y son la base de su infraestructura operacional. El rápido desarrollo y las nuevas tecnologías y su expansión dentro de la organización han proveído ventajas competitivas, incrementado la productividad y la exposición a mercados desconocidos. Esta rápida expansión ha creado también nuevos riesgos en el manejo de los cuales la gerencia tiene poca experiencia y en algunas instancias han evitado su expansión en esos mercados desconocidos. Para mantenerse competitivas, las compañías deben estar preparadas para expandir sus zonas de confianza. Para considerar

adecuadamente los mayores riesgos, la gerencia necesita encarar el control y la seguridad de los recursos críticos con un enfoque que abarque toda la empresa.

Durante los últimos años, hubo una corrida para contar con los detectores de intrusos para controlar y evaluar la seguridad de Internet en la organización. Mientras esto produjo algunas historias interesantes, también creo en las organizaciones un falso sentido de seguridad y confort. Hay algo más que simplemente tener una conexión segura de Internet. Hay aspectos como acceso interno, políticas, procedimientos y estándares, monitoreo de actividad, control de activos, integridad de datos, confidencialidad, educación y concientización, cumplimiento, obligación y privacidad para citar algunos de los aspectos a tener en cuenta. Hay cada vez más productos que están siendo ofrecidos para proveer control de acceso, capacidad de control de actividad, administración centralizada de recursos, etc. Muchas organizaciones no tienen ni el tiempo ni los recursos para mantenerse a tono con estos avances y no entienden completamente los beneficios o impacto de contar con estos recursos. Debido a los desafortunados acontecimientos del 11 de Setiembre, ha habido y hay un fuerte compromiso de seguridad tanto en el sector público como el privado. El Departamento de Defensa de la Nacionalidad ha dicho varias veces que Internet no es lo suficientemente seguro ni confiable para procesar las comunicaciones gubernamentales. Además, los esfuerzos de la Defensa de la Nacionalidad federal, de los estados y gobiernos locales deben estar concentrados en seguridad física y lógica. Esta movida del gobierno federal tiene impacto a la vez en los negocios de la comunidad.

Estar en la autopista de la información no es más una extravagancia sino una necesidad en la economía actual. Sin embargo, muchos negocios han integrado nuevas tecnologías y capacidades con poca o nula conciencia en la seguridad. Además, muchos negocios han adquirido tecnologías relacionadas con seguridad y no las han instalado, integrado o mantenido apropiadamente, ubicándolos en una posición vulnerable en su infraestructura de seguridad tecnológica. Esto ha derivado en que muchos negocios tienen un nivel de confort de seguridad que los protege de daño o abuso. Nada más alejado de la realidad. Durante los años pasados, hubo una corrida de fusiones y adquisiciones en el mundo. Muchas veces, el negocio adquirido fue dejado solo para continuar sus operaciones con una pequeña supervisión de su compañía controlante, en particular en el área de tecnología de la información. Como consecuencia, hay muchas redes internas y externas no documentadas ni controladas. Además, mientras la compañía controlante provee conectividad a través de su red interna, proveen poca guía al negocio adquirido sobre cómo controlar los accesos y su propia red. Esta situación ha creado una vulnerabilidad potencial donde la compañía controlante tiene una infraestructura segura, pero da acceso a un entorno inseguro. Comprometiendo el entorno inseguro (el negocio adquirido) pone en riesgo a la compañía adquirente.

Por años, las empresas han contratado consultores externos para proveer la comparación con otros negocios en materia de seguridad y operaciones de tecnología. Como parte de esos servicios, los consultores proveían un plan de acción para implementar medidas correctivas. En la mayoría de las oportunidades, estos planes de acción fueron archivados y nunca implementados. Para ser efectiva, la seguridad debe estar en una constante adaptación. La solución de hoy es el riesgo de mañana. Muchas organizaciones no tienen la habilidad de dedicar recursos para mantenerse actualizados y conscientes de los cambios constantes en el área de tecnología y seguridad. Ahora más que nunca, hay una confianza en los recursos externos para proveer soluciones a las organizaciones, brindando el talento y experiencia que pueda asegurar que la tecnología y la estrategia son adecuadas e integradas con las necesidades estratégicas y tácticas del negocio.

La Solución: Entorno de Arquitectura de Seguridad (SAF) MR

La seguridad en la actualidad es más que contraseñas, “firewalls” y pistas de auditoría. Ahora implica entrenamiento del personal que no solo entiendan las tecnologías instaladas sino también su integración e impacto en las operaciones del negocio. Para llegar allí, las organizaciones necesitan asesores confiables para identificar faltantes y debilidades, diseñar mejoras en los sistemas y procesos e integrar soluciones efectivas. CTG’s Soluciones en Seguridad Informática ofrece soluciones prácticas y soluciones que cumplen con las necesidades de los clientes. A través de nuestra metodología de entorno de arquitectura de seguridad, facilidad de seguridad virtual, software de herramientas para evaluar seguridad y

portales de conocimientos gerenciales proveemos recomendaciones en forma consistente, dando respuestas consistentes y proactivas para mitigar riesgos.

La seguridad efectiva es un proceso no un evento o solución de única vez. Como la tecnología ha evolucionado, de acuerdo a lo descripto en la figura 1, también lo han hecho los riesgos y vulnerabilidades asociados con la misma. Hemos visto una rápida expansión de la tecnología a través de los últimos treinta años desde los grandes centros de cómputos a los entornos virtuales globales.

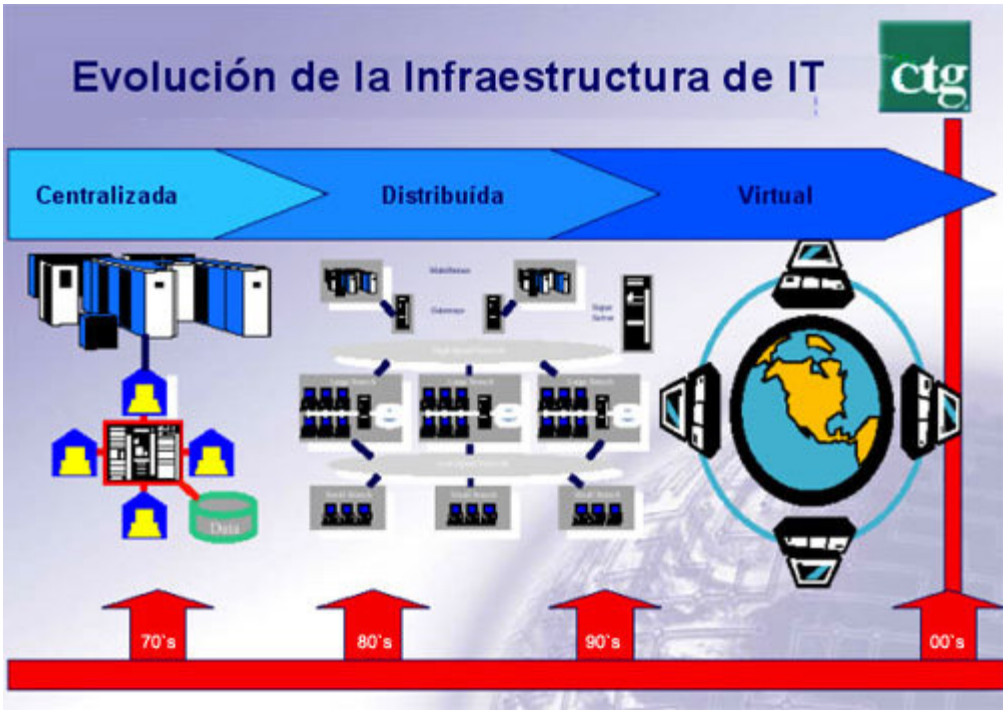

FIGURA 1

Durante los últimos 30 años la computación ha cambiado fundamentalmente desde una alta centralización, en un entorno de grandes centros de cómputos, el cual es relativamente fácil de controlar, al actual entorno virtual donde los controles, cuando existen, están en constante cambio.

En un entorno centralizado:

- El acceso está restringido a un número limitado de usuarios.
- Los procesos son primariamente de a lotes (batch), frecuentemente con largos períodos entre actividades.
- Hay controles manuales redundantes.
- Los datos son centralizadamente archivados con poco volumen.
- La introducción en 1978 de la computadora personal anunció el comienzo de la democratización de la computación, sacando el procesamiento de un área controlada hacia el espacio general de trabajo.

En el entorno distribuido:

- Hay un creciente número de usuarios, pero todos permanecen conocidos y autorizados por la organización.
- La frecuencia de procesamiento salta de diaria a horaria o a pedido.

- El entorno de LAN (local area network) permite múltiples usuarios distribuidos en una ubicación física. También con el advenimiento de WAN (wide area network) el crecimiento de los controles se incrementa a toda la organización independientemente de la ubicación.

- Sacando la computadora del área controlada, se multiplica la diversidad y éxito de la tecnología portable.

- Cuando la influencia de tecnología informática se expande a toda función operacional, financiera, recursos humanos y de venta, la necesidad de un lenguaje común en los programas se convierte en una alta prioridad para lograr eficiencia. Los sistemas que se utilizan en toda la organización, tales como SAP, Baan, Oracle Financials y Peoplesoft ofrecen esta uniformidad pero también introducen aspectos de control significativos.

Con el advenimiento de Internet/Intranet/Extranets que han habilitado el entorno virtual:

- Casí todo parámetro que existía previamente fue redefinido

- La actualización es constante.

- El entorno computarizado es ahora global.

- La tecnología de almacenamiento está permitiendo capacidad ilimitada dentro del departamento de IS a través del almacenamiento en el sitio del usuario.

- Las organizaciones no conocen más quiénes son los usuarios qué están conectados en sus sistemas en cada momento y los puntos de control cambian rápidamente.

- Los socios externos de la empresa se han integrado en el día a día de operaciones con amplio acceso a información y sistemas.

- A fin de conectarse con otros, los protocolos y estándares se estan considerando nuevamente.

- Se debe repensar cómo es utilizada y definida la información.

En algunos momentos la tecnología reemplaza la existente, pero en muchos casos, la tecnología es acumulativa. Nuevos controles y políticas deben trabajar en forma complementaria con controles y políticas ya existentes.

Así como nos introdujimos en este entorno de tecnología virtual global, los riesgos y vulnerabilidades se han incrementado también (Figura 2). Como las nuevas tecnologías han sido integradas en la infraestructura de la empresa, los riesgos y vulnerabilidades asociados con tecnologías antiguas no han sido eliminadas, a menos que esas tecnologías antiguas hayan sido retiradas. En muchos casos, las viejas tecnologías no fueron retiradas, pero sus roles fueron redefinidos, comprendiendo los riesgos de la organización.

FIGURA 2

De acuerdo a la evolución de la tecnología, junto con los cambios ha habido un cambio importante en el nivel de riesgo dentro de las organizaciones. Los riesgos operan en dos mundos:

- Uno es el de los negocios con tendencias y focalización en costos, cambios rápidos, complejidad creciente y resultados en el corto plazo.

- El segundo es el riesgo que aparece del entorno tecnológico a medida que éste evoluciona hacia un entorno abierto a más usuarios, puntos de conexión, complejidad y reduciendo el tiempo de reacción.

Hoy, el nivel de riesgo no ha sido reemplazado pero de hecho se ha ampliado a través del tiempo. Los anteriores riesgos permanecen en el mundo actual y crecen exponencialmente con los nuevos riesgos que aparecen con la nueva tecnología.

CTG ha desarrollado un enfoque a la seguridad de la arquitectura de toda la empresa basado en el principio de proteger los activos valiosos de la misma. La tríada de Gente, Proceso y Tecnología es la base alrededor de la cual la arquitectura de seguridad debe ser desarrollada. La figura 3 describe el Ciclo de Vida de la Seguridad de CTG, que visualiza el continuo proceso que involucra los componentes clave de la arquitectura de seguridad.

FIGURA 3

- **Activo**s – activos a ser asegurados y controlados contra malos usos de manera inadvertida o intencional.
- **Gobierno** – establecer políticas, procedimientos y estándares de comportamiento.
- **Perfil** – ubicar e identificar todos los activos dentro de la infraestructura.
- **Valor** – determinar el valor de los recursos para el negocio
- **Vulnerabilidades** – identificar vulnerabilidades potenciales y la habilidad de aprovecharlas
- **Amenazas** – identificar potenciales amenazas y la posibilidad de ocurrencia
- **Riesgo**– calcular el nivel de riesgo basado en exposiciones y contramediciones.
- **Soluciones** – eliminación o reducción de la posibilidad de vulnerabilidades.
- **Medidas** – establecer medidas para determinar el impacto y valor de las iniciativas de seguridad.
- **Monitoreo** – asegurar el cumplimiento con políticas, procedimientos y estándares establecidos.

Las tres áreas de Políticas y Procedimientos, Tecnología y Recupero y Restauración son el foco del entorno de Arquitectura de Seguridad como se describe en la Figura 4. De esos tres, las políticas y procedimientos forman el fundamento ya que son las reglas a través de las cuales la organización se gobierna a sí misma. Las políticas y procedimientos establecen controles apropiados para el gobierno de los individuos dentro de una organización. Segundo, asignan clasificación a los datos para ayudar a determinar los riesgos asociados con cada uno.

El establecimiento de políticas correctas y procedimientos permiten a la organización controlar el uso y evitar el uso incorrecto de la tecnología estableciendo bases de seguridad mínima. Algunos ejemplos podrían ser la inclusión de longitud mínima de claves, políticas de seguridad periférica, configuración de sistemas operativos, estándares para la autorización y autenticación, etc.

A través de este proceso estamos viendo cómo la organización conduce su negocio y ayudando a establecer controles apropiados teniendo en cuenta los riesgos. Podemos ayudar planeando lo impensable en caso que ocurra una interrupción en la continuidad del negocio. El recupero y la restauración deben focalizarse en las funciones críticas del negocio con el fin último de lograr una total restauración de las operaciones del negocio.

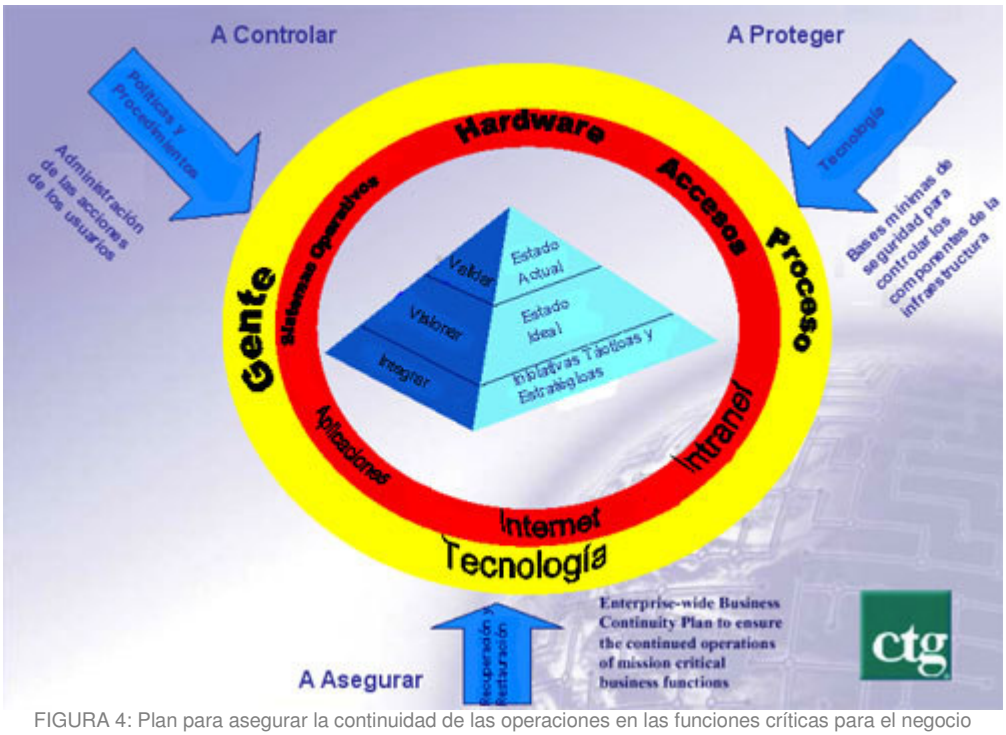

FIGURA 4: Plan para asegurar la continuidad de las operaciones en las funciones críticas para el negocio

¿Cuál es nuestra visión? Desde nuestra perspectiva hay tres fuerzas que conducen la seguridad: controlar, brindar seguridad y asegurar. Mientras algunas personas entienden que la seguridad se refiere a control y seguridad, mucha gente, incluyendo los más altos rangos, ignoran el aspecto de “mejora” de la seguridad. De este modo, la seguridad es clasificada como un costo o dotación en vez de un facilitador del negocio. Nuestra perspectiva es que la seguridad provee, además de seguridad y control en el entorno, la habilidad de mejorar e incrementar las oportunidades de negocio.