

El retorno de la inversión de los proyectos y tecnologías de Seguridad

- Febrero 2013
- Vicente Gozalbo, WW Security Tiger Team, LATAM Sales
- IBM Security Solutions
- vgozalbo@co.ibm.com

Retos actuales de los clientes en Seguridad

CIO & Team



Prioridades del Negocio

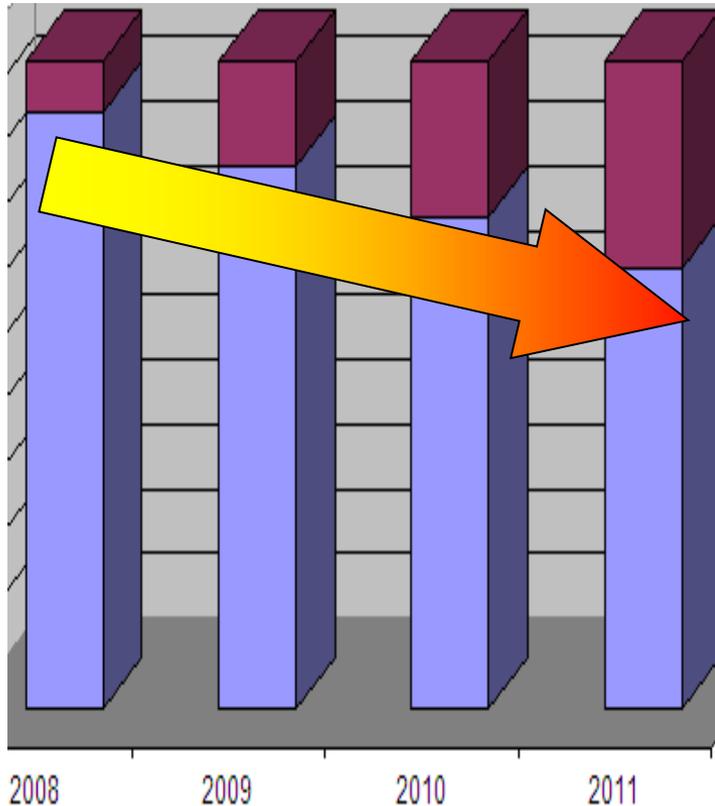
1. La Seguridad IT es un tema de gerencia
2. El negocio pide la mejor práctica global.
3. Crecimiento a través de adquisiciones
4. Incremento de las regulaciones a cumplir,
5. Aumento a la tendencia de consolidación IT
6. Hacer foco en el valor

Technical & Threat Priorities

1. Mobile / SmartPhone
2. Las redes Sociales realimentan los otros riesgos
3. Cloud
4. Incremento de la sofisticación en los ataques
5. Más vulnerabilidades en las aplicaciones
6. Ataques internos
7. Protección de datos y BBDD
8. Protección de Infraestructuras (e.g. Stuxnet)
9. Big Data Security



Debo disminuir los costes asociados a la infraestructura y gestión de la seguridad IT (TCO).



- Mantener seguros los activos tecnológicos e información me supone **un 10% del presupuesto** IT y va creciendo año a año.
- Esos gastos **restan presupuesto** a otras inversiones de más valor para la compañía

- Encontrar un balance entre la seguridad efectiva y el coste de la misma
 - No deberíamos invertir 100 € en un cercado para proteger una sola oveja que cuesta 10 €
- Existen muchos estudios que indican que la regla de Pareto (regla del 80-20) aplica perfectamente a los procesos de seguridad IT
 - EL 87% de los incidentes de seguridad IT fueron considerados evitables mediante controles razonables.
- Un pequeño conjunto de controles nos entregan una gran cantidad de cobertura ante incidentes
 - Hay que seleccionar controles críticos que contengan riesgos en todos los niveles de la empresa. P.ej. Contraseñas.
 - Las organizaciones que utilizan controles de seguridad eficientes también tienen una productividad significativamente superior*



*Fuentes: W.H. Baker, C.D. Hylender, J.A. Valentine, 2008 Data Breach Investigations Report, Verizon Business, June 2008
ITPI: IT Process Institute, EMA December 2008

Tivoli software



Tivoli Business Value Analyst Product Savings for Security

Version 3.7.4

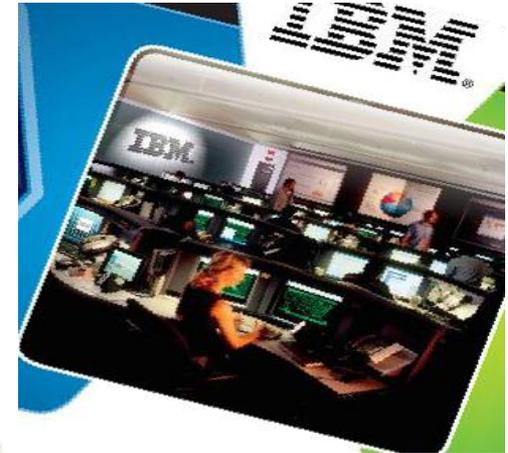
Rubros de Ahorro en seguridad

- _ Factor trabajo en Gestión de la Seguridad.
- _ Ahorro en Desarrollo de la seguridad de las aplicaciones.
- _ Reinicio de usuario/contraseña
- _ Acceso de Usuarios más rápidos.
- _ Time to Market más corto.
- _ Ahorro en/mediante/con integraciones.
- _ Ahorros en contratos de soporte.
- _ Evitar costes en tecnología de seguridad actual.
- _ Ahorros en Auditorias de Sistemas.
- _ Mejora de la productividad por centralización.
- _ Ahorros en capacitación y certificación.
- _ Incremento de la productividad del usuario final.
- _ Evitar penalizaciones del nivel de servicio.
- _ Evitar riesgos de seguridad



Casos de Ejemplo

FOROS ISIS



Caso 1: Gestión segura de procesos una nueva manera de servir a los ciudadanos

Cómo IBM y un Business Partner ayudan a hacer reingeniería de procesos de emisión de documentos, asegurándolos desde el diseño..

Problema:

Algunos documentos oficiales (p.ej. Pasaportes, certificados médicos, licencias de conducir) pueden ser objeto de fraude y falsificación.

Muchos de estos documentos son procesados usando controles y validaciones obsoletas que son vulnerables a falsificaciones y modificaciones con tecnología moderna..



Razones para actuar

Fraudes, terrorismo, accidentes de vehiculos.

Ineficiencias debidas a tener que rehacer los documentos en procesos no flexibles.

Alta frustración de los Ciudadanos.

Inversión extranjera se resiente

Propuesta: Citizen's ID, un proceso seguro para generar y entregar credenciales a empleados y ciudadanos.

Revisión profunda del proceso actualm analizando los fraudes existentes y las ineficiencias del mismo.

Reingeniería: Secure by Design

- Asegurar por completo el procesos de emisión de documentos oficiales
- Desde la ventanilla publica hasta los sistemas finales.
- Monitoreo de todo el proceso desde un SOC

Componentes de la solución

Biometria y Criptografía

Seguridad en BBDD y ofuscación de datos

Gestión de Identidades

Escaneo de vulnerabilidades en Aplicaciones

Security Intelligence: Monitoreo 7x24 de todo el proceso desde un SOC mediante un SIEM / Security Intelligence

Beneficios

Reduce los retrabajos y mejora la flexibilidad:

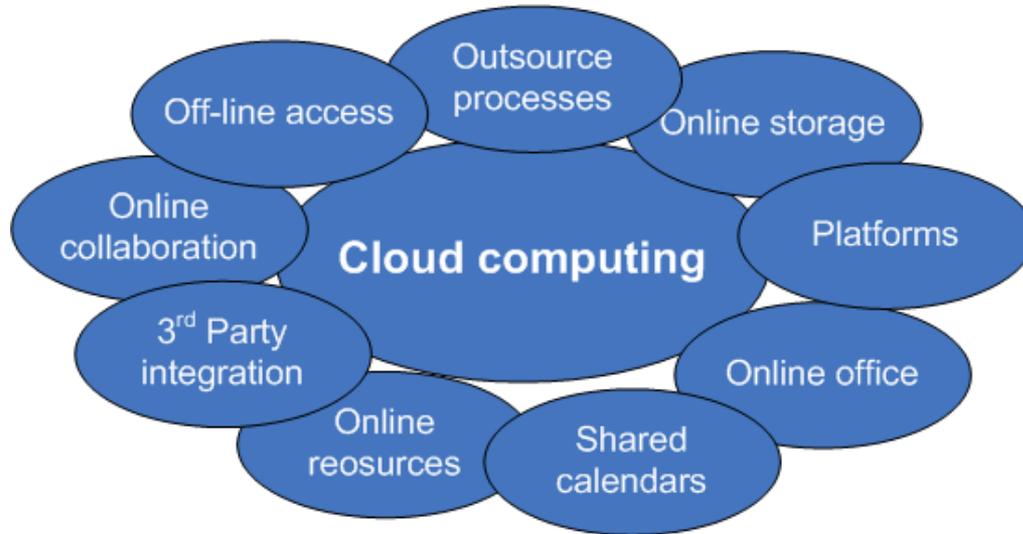
Más eficiencia

Reduce el fraude y la frustración de los ciudadnos: incrementa la confianza en las instituciones.

Disminuye las falsificaciones: Reduce los delitos, estafas y accidentes.

Más seguridad jurídica: mejora el clima de inversión extranjera.





Caso 2: Gestión de Acceso y Federación de Identidades que generan nuevos modelos de negocio



Cómo se puede crear nuevos modelos de negocio usando tecnologías de seguridad.

Problema:

Las aplicaciones Web son fáciles de desplegar y cómodas para usuarios, clientes y empleados..

Sin embargo mantener la seguridad en esas aplicaciones es difícil debido a las continuas vulnerabilidades y problemas de gestión de accesos: conforme las aplicaciones van proliferando y el número de usuarios crece, la complejidad aumenta exponencialmente.



Razones para actuar:

Las aplicaciones Web y Móviles están el core business de cualquier compañía.

La inseguridad y la complejidad detiene el desarrollo de estos nuevos canales.

Las compañías pueden ser seriamente afectadas por falta de seguridad en sus aplicaciones on-line.

Los nuevos canales que se despliegan desde una base segura son los que más probabilidad de éxito tienen.

Los modelos de negocio que no son seguros introducen riesgos y restringen las posibilidades del canal on-line.



Propuesta

Gestión de Acceso a la Web integrado que decide quien tiene acceso a qué aplicación en base a políticas.

Federación de identidades que habilita a empresas externas a autenticar a sus propios usuarios, pasando la información de las credenciales mediante estándares.



Security Intelligence.
Think Integrated.

Componentes de la Solución

Proxy Reverso integrado

Usuarios de las aplicaciones en directorio LDAP,

Gestor de identidades Federadas

Beneficios:

Ahorro en el desarrollo de aplicaciones

Mejor protección de las plicaciones

Time to Market Rápido para nuevas aplicaciones

Capacidad de gestionar centralmente quien accede a que y cuando, basado en reglas de negocio.

Escalable hasta millones de usuarios.



FOROS ISIS

Vicente Gozalbo Moragrega
IBM Security Systems
WW Security Tiger Team

vgozalbo@co.ibm.com