OWASP AppSec
Aguascalientes 2011

The OWASP Foundation
http://www.owasp.org

La seguridad 2.0

Pablo Lugo G

@pablolugog

Citas

- La seguridad no es un producto, es un proceso. Bruce Schneier. Experto en seguridad.
- La seguridad no es un problema de tecnología, es un problema de gente y de administración. Kevin Mitnick.
- Cuando se trata de seguridad digital, no existe algo como una defensa impenetrable. Pero se pueden mitigar los riesgos siguiendo sólidas practicas operativas. @Stake

Seguridad

- ✓ La seguridad de Información debe soportar la misión del negocio
- ✓ Los dueños de recursos de información tienen responsabilidades relacionadas con seguridad dentro y fuera de su propia organización
- ✓ La responsabilidad y la asignación de la seguridad de la información debe ser establecida claramente
- ✓ Requiere de un enfoque integral y completo
- ✓ La seguridad de información debe ser re-evaluada periódicamente

- ✓ La seguridad de información esta caracterizada por la preservación de:

Confidencialidad, Integridad y Disponibilidad

- ✓ Para ello, se requiere de:
  - ➢ Metodología (Métodos, procesos, políticas)
  - ➢ Antropología (Gente)
  - ➢ Tecnología

Tendencias

Symantec en la XV edición de su reporte Internet Security Threat Report (ISTR). Comenta que la tendencia para los próximos años es clara: a medida que la tecnología se expande, los ciberataques avanzados únicamente requerirán de dinero, no de conocimientos informáticos.

Tendencias

En los últimos 12 meses el cibercrimen han enfocado sus ataques y buscan información con alto valor para sus dueños. Ya no se trata de cantidad sino de calidad de los datos.

Existen una gran cantidad de "novatos", ellos tienen la facilidad para comprar "kits" en espacios clandestinos en la Red, lo que ha provocado que hasta el delincuente más "neófito" en tecnología pueda convertirse en un cibercriminal, capaz de comprometer identidades o robar datos.

Tendencias

Durante 2009 60% del total de las fugas de información en las organizaciones fueron debido a ciberataques o intentos. Un crecimiento de casi 300% al compararse con los datos del 2008.

El sector financiero fue uno de los más afectados, 60% de los ataques fueron a este sector durante 2009, dos veces más que los reportados en 2008, cuando solo se presentaron el 29% de los casos de identidades o información comprometida.

Cibercrimen para neófitos

Existe un crecimiento del cibercrimen alrededor de todo el mundo, no hay más expertos informáticos desarrollando software malicioso, se tiene una facilidad por la venta de "kits".

El troyano-botnet Zeus, se detectaron más 90,000 variantes distribuidas en la red a un precio de $700 UDS. De hecho, se estima que 57% de todos los ciberataques a usuarios el año pasado fueron generador por cibercriminales simples, no profesionales ni organizados.

Cibercrimen para neófitos

Lo kits de malware facilitan que cualquiera puede ejecutar un ciberataque sin tener conocimiento alguno de informática.

De acuerdo a reportes 98% el malware detectado contiene capacidades de acceso remoto, 89% permite la exportación de datos de usuarios infectados, 86% contiene programas tipo keylogger y 78% exporta datos del sistema.

Y si bien, el número de ataques de phishing y botnet detectado por día sigue a la baja , se han detectó más de 50,000 bot nuevos todos los días. Se estima, que a la fecha hay más de 7 millones de PC zombis o bot en todo el mundo.

Cibercrimen para neófitos

Hoy hay menos hackers por el puro gusto de informarse en materia de seguridad informática, hoy son simples criminales.

Además paradójicamente a los pronósticos de hace años, no fue la empresa la que adoptara la vida en la nube, fue el usuario final. Facebook, Twitter, Linkedin, Google+, iTunes

La nube es algo que ya nos alcanzo

Cibercrimen para neófitos

Si la red y los usuarios ya no tienen fronteras ¿cuáles son los nuevos paradigmas que enfrenta la seguridad?.

El modelo para abordar la seguridad en las empresas se tiene que modificar y en muchas casos va a costar años pensar que la seguridad debe ser tratada de manera distinta.

Dentro de esta nueva visión de seguridad se debe contemplar tres puntos esenciales: Gobierno corporativo, reforzamiento de políticas y auditorías de servicios, que hoy están en cualquier lugar.

¿Dónde está el reto?

- Muchos ejecutivos, consideran a la seguridad de información como un problema de tecnología y no un problema de negocio.
- El software de uso común sigue teniendo huecos de seguridad (por ejemplo: Adobe Reader)
- Según cifras de Gartner, 60% de los exempleados de una corporación se llevan información confidencial, 80% admitió usarla en algún momento para nuevas oportunidades de empleo
- El cibercrímen sigue creciendo, está saludable y hoy algunos se disfrazan de hacktivistas

¿Dónde está el reto?

- La seguridad por si misma no ofrece valor de negocio, típicamente reduce la pérdida de valor de negocio.
- Factores económicos: Masificación, economías de escala. Es rentable explotar software altamente usado.
- Las áreas de seguridad responsables del desarrollo de las estrategias para proteger la información de la organización, no se comunican con otras áreas del negocio.

Que problemas hay?

La seguridad sigue ligada con las áreas de tecnología, sin embargo es un asunto que debe asumirse en toda la organización.

¿Porqué la Seguridad de Información en los procesos de Negocio?

- Existe una mayor dependencia de la tecnología de información en sus procesos críticos
- Internet se ha convertido en pieza fundamental en las operaciones de un negocio.
- Si no elevamos la seguridad de información a un rol ligado a las actividades de negocio, el impacto adverso seguirá en las organizaciones y continuaremos con problemas para justificar el costo de la seguridad de información.

Procesos y Cultura

La **Seguridad de la Información** no debe ser vista como un producto o paquete. Son una **serie de procesos** que en combinación con la **educación** y concientización del personal que labora dentro de la empresa, permite alcanzar el **nivel mínimo de riesgo** aceptado por la alta dirección.

Algunos Criterios, modelos de seguridad y Marcos de Referencia

Marcos de Referencia de Seguridad

Cobit

GITBPM

ISO 27002/ ISO 17799

Modelos de Madurez

SSE-CMM (Systems Security Engineering-CMM)

Information Security Program Matrurity Grid (ISPMG)

Software Security Metrics (SSM)

Security Maturity Model (SMM)

Modelos: ALE, SooHoo, CBA, OCTAVE

Por donde Empezar

Identificar los niveles de criticidad de procesos – eventos que ocurren en los procesos particularmente importantes dentro del negocio que ocasionarían un impacto a la empresa.

Definición de objetivos y requerimientos de seguridad. Adherencia a los objetivos y requerimientos de seguridad de los datos usados en estos procesos en un momento dado – la no adherencia conducirá a eventos que ocasionen daño. Si los objetivos y requerimientos de seguridad se cumplen entonces los impactos implícitos de los eventos son mitigados debido a que existen las medidas

La capacidad de los procesos de seguridad de TI para tratar con los eventos de seguridad – la detección y prevención de eventos.

Marco de Referencia

Valuar las medidas de Seguridad basados en el valor de los procesos núcleo de negocio

- Esto permite integrar Procesos corporativos al núcleo de negocio que deberían ser protegidos

Marcos de referencia que permitan la definición de niveles de seguridad y procesos de TI

Marco de Referencia

Se debe considerar la pérdida de valor de negocio debido a la falta de disponibilidad de un sistema (costos indirectos / de oportunidad)

Pérdida de utilidades que resultan de que se detenga un proceso de negocio

Costos de empleados

Otros costos indirectos como los intangibles (pérdida de clientes, o pérdida de reputación).

Enfoque basado en Procesos

La aplicación de un sistema de procesos dentro de la organización, junto con la identificación e interacciones de estos procesos, así como su gestión, puede denominarse como "enfoque basado en procesos".

Una ventaja del enfoque basado en procesos es el control continuo que proporciona sobre los vínculos entre los procesos individuales dentro del sistema, así como sobre su combinación e interacción.

Para que una organización funcione de manera eficaz, tiene que identificar y gestionar numerosas actividades relacionadas entre sí. Una actividad que utiliza recursos, y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados es un proceso. Frecuentemente su resultado constituye directamente el elemento de otro proceso.

¿Cuáles son los beneficios?

- Facilita el establecimiento de una metodología para la Administración de la Seguridad clara y estructurada.
- Reduce el riesgo de pérdida, robo o corrupción de información.
- Proporciona a los usuarios acceso a la información a través de procesos seguros.
- Facilita el monitoreo continuo y los controles para el manejo de la información.
- Genera confianza en clientes y socios debido a la garantía de calidad y confidencialidad de la información manejada.
- En el caso de emplearse como referencia en la realización de auditorías, ayuda a identificar las vulnerabilidades.
- Facilita la integración con otros sistemas de gestión, como pueden ser ISO 9001 e ISO 14001.

¿Qué necesidades deben satisfacer?

Administración.- buscar un estándar desarrollado con la finalidad de proporcionar un modelo para establecer, implementar, operar, monitorear, mantener y mejorar la Seguridad de la Información de la empresa.

Regulación.- Los marcos de referencia al ser adoptados ayudan a dar cumplimiento a regulaciones aplicables a la empresa, como Sarbanes Oxley y PCI-DSS, para garantizar la veracidad, confidencialidad, disponibilidad e integridad de la información, obteniendo entre otros beneficios, el cumplimiento con la regulación aplicable.

Control.- Los marcos de referencia ayudan a mantener un ambiente de control en materia de Seguridad de la Información; ya que una de sus premisas es brindar recomendaciones a los responsables de planear, implantar o mantener controles para garantizar la Seguridad de la Información. Proveen una base común para el desarrollo de estándares de control de seguridad, aplicables a una empresa en particular tomando como referencia un conjunto de prácticas que han probado su efectividad.

¿Qué necesidades deben satisfacer?

Seguridad.- Al trabajar con un estándar desarrollado proporciona un modelo para establecer, implementar, monitorear, revisar, mantener y mejorar un Sistema de Administración de Seguridad de Información (ISMS). Así mismo, enfatiza que el diseño y la implementación de un Sistema de Administración de Seguridad de Información debe satisfacer las necesidades, objetivos estratégicos y requerimientos en materia de seguridad.

Estrategia.- La adopción de un marco de referencia debe ser una decisión tomada a nivel estratégico, ya que se definen objetivos estratégicos, que satisfagan los requerimientos de seguridad de los procesos sustantivos del negocio.

Que existe ?

BSC (Balanced Scorecard) contempla un sistema de administración del desempeño que permite a las empresas conducir su estrategia acorde a lo planeado mediante el monitoreo continuo, complementando los indicadores financieros tradicionales con criterios de medición de desempeño orientados a: "Clientes", "Procesos Internos" y "Aprendizaje y Crecimiento".

La técnica BSC es complementaria, ya que puede ser empleada para definir la estrategia requerida para la ejecución de los programas y proyectos asociados con la implantación y mejora de los Sistema de Administración de Seguridad de Información

Que existe ?

COBIT (Control Objectives for Information and Related Technology) es un compendio de objetivos de control para la Tecnología de Información que incluye herramientas de soporte que permiten a la administración cubrir la brecha entre los requerimientos de control, los aspectos tecnológicos y los riesgos de negocio.

Que existe ?

IT Governance es un conjunto de mecanismos utilizados por la administración de una organización para dirigir y controlar su desarrollo tecnológico, asegurando que las metas del negocio sean alcanzadas de forma efectiva mediante la detección y control de los riesgos asociados.

Una parte esencial del Gobierno de TI (IT Governance) es el Gobierno de Seguridad de Información (Information Security Governance), el cual se encarga de garantizar la integridad de la información, continuidad de servicios y protección de los activos de información.

En resumen

- Reto: Encontrar como Dar Valor de Negocio a la Seguridad de Información en un mundo como el actual.
- Es necesario ligar la seguridad con los procesos de negocio de la organización, si desde un inicio no se considera la seguridad, el agregarla después será más costoso.
- La seguridad de información y las tres logias:
  - Metodología, Antropología, Tecnología

Bibliografía

- ISO e IEC, **"BS ISO/IEC 27001:2005 BS 7799-2:2005, Information technology — Security techniques — Information security management systems — Requirements"**
- IT Governance Institute, **"COBIT Mapping"**.

Referencias Electrónicas

- http://www.27001-online.com
- http://www.ISO 27000.es
- http://www.bsistandards.co.uk
- http://www.isaca.org

Preguntas

¡Gracias!

Pablo Lugo G
pablolugog@gmail.com