Plan de trabajo del Grupo de Seguridad de RedCUDI

M. Farias-Elinos
Tecnológico de Monterrey
Grupo de Seguridad de RedCUDI

August 8, 2012

Contents

1 Antecedentes

Uno de los grandes retos que se enfrenta la Seguridad en Tecnologías de informaci'on y Comunicación tiene que ver directamente con la falta de personal especilizado en esta área, esto se puede observar en la figura 1 donde el 71% del sector educativo presenta vulnerabilidades permanentes, algo que afecta a las instituciones educativas considerablemente y que consume tiempo del personal técnico dia a dia en cosas que se pueden mejorar y tener control desde un principio. Esto tiene que ver principalmente, por un lado con la falta de conocimiento al configurar la infraestructura desde el punto de vista de la seguridad, y por el otro lado, la falta del conocimiento de los desarrolladores de aplicaciones, tal como se puede ver en la

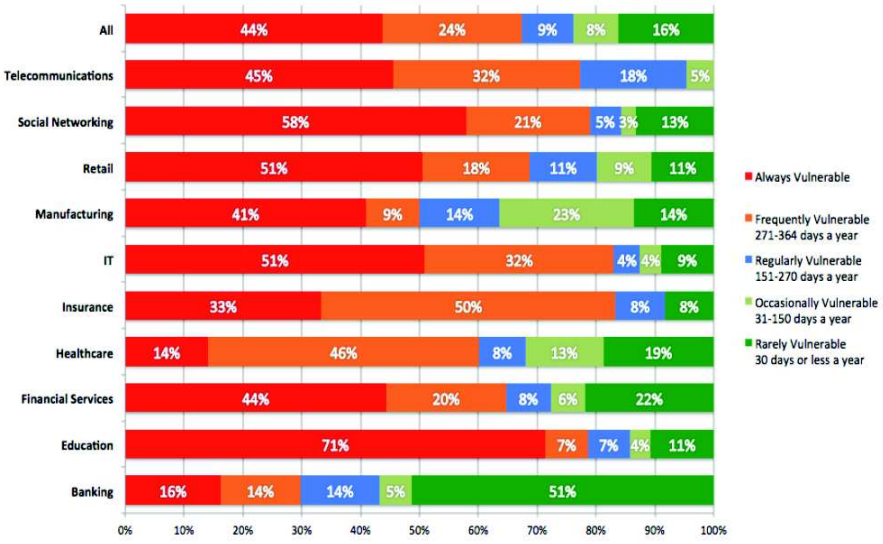

Figure 1: Vulnerabilidades por sector

figura 2 donde el 85% de los desarrollos internos (también llamados desarrollos caseros) no siguien ninguna metodología de seguridad en el desarrollos de las aplicaciones.

De por si los productos comerciales y que se conocen a nivel mundial (Windows, MacOS X, IOS (sistema operativo de los prodictos CISCO), iPhoneOS, Android, MS-SQL Server, MySQL, etc) prsentan vulnerabilidades constantemente, tanto que en promedio se boletinan 280 vulnerabilidades a la semana del software conocido, tal como se observa en la figura 3. Otro factor que es importante mencionar, es que hoy en día se tiene un deficit de 10,000 especilistas en el área de la seguridad informática.

Estos factores, por citar algunos hacen indispensable que exista un plan de capacitación para la gente técnica y de aplicaciones miembros de CUDI, con el fin de tene una red lo mas saludable posible; así como una red interna en cada institución donde los riesgos de seguridad en Tecnologías de Información y Comunicación sean reducidos a una condicón de aceptabilidad.

2 Objetivo

- Establecer un mecanismo de capacitación que permita formar a los miembros de CUDI dentro del área de la Seguridad de las Tecnologías de Información y comunicación.
- Conformar un repositorio de herramientas de seguridad para la comunidad CUDI.

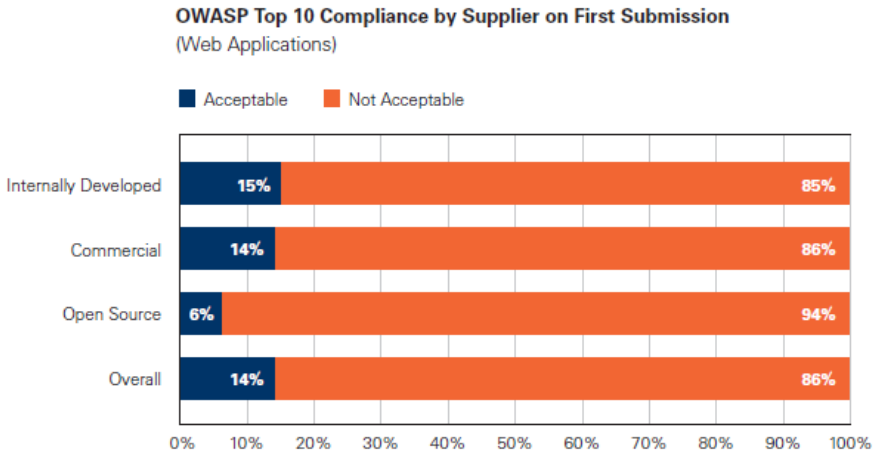

Figure 2: Vulnerabilidades por sector

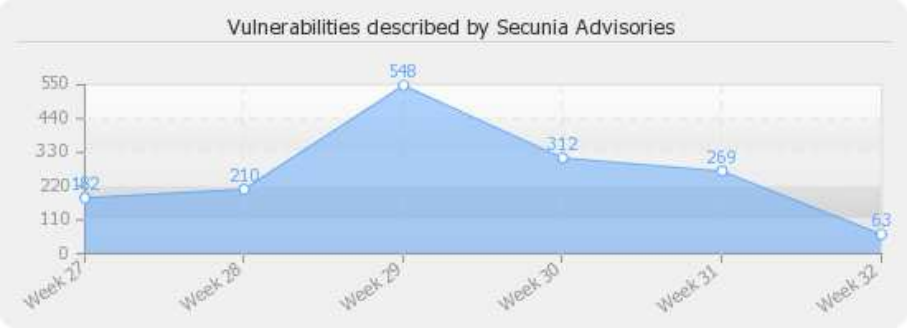

Figure 3: Vulnerabilidades por sector

3 Metas

- Tener un acercamiento con alguna organización certificadora del area de la seguridad (SANS, EC-Council, etc) con el cual se pueda obtener cursos de certificación a precios accesibles
- Definir los cursos necesarios para la comunidad CUDI.
- Establecer un calendario de cursos de seguridad.
- Instalar en algún servidor el reppositorio de herramientas de seguridad para que la comunidad CUDI pueda hacer uso de este.

4 Metodología

Establecer un canal de comunicación con algún organismo certificador del área de la seguridad en las Tecnologías de Información y comunicación que quiera participar en la capacitación de los miembros de CUDI, bajo algun esquema que permita la reducción de costos para hacelos accesibles; además de conseguir las certificaciones en el área.

Entablar una comunicación con los miembros de CUDI para detectar las prioridades y problematicas de seguridad con el fin de definir los cursos prioritarios para la capacitación de los mismos.

Definir un calendario de cursos a un año con el fin de crear un plan de carrera para los miembros de CUDI que decidan tomar los cursos; con el objetivo de crear especialidas en seguridad.

Dar acceso a la comunidad CUDI, principalmente a aquellos que tomen los cursos de capacitacion en seguridad, a las herramientas de seguridad que el grupo ha estado trabajando y que permiten probar la seguridad de la infraestructura tecnológica.