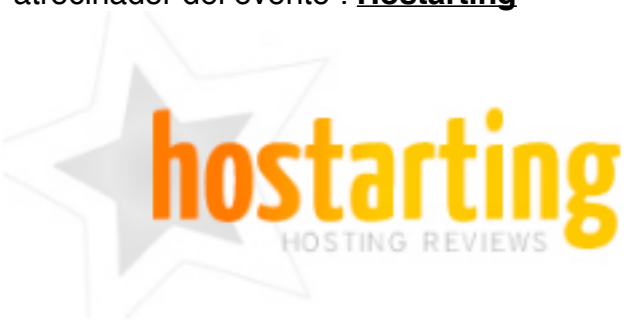
NETWORKINGACTIVO

Desayuno de trabajo **Networking Activo** sobre "**Ciber Seguridad**", celebrado el 4 de Mayo 2011 en Madrid.

Patrocinador del evento : **Hostarting**



Los Temas propuestos para el debate fueron:

- Seguridad en servicios externalizados o en la nube.
- Importancia (o no) del cumplimiento de estándares de seguridad por las empresa
- Amenazas ¿nuevas? en las redes sociales.
- Riesgos de los dispositivos móviles en las organizaciones en cuanto a fugas de información y conformidad legal
- Validez o impacto de las tecnologías actuales en la protección de los sistemas informáticos (antivirus, IDS, honeypots, firewalls, WAFs…)
- Seguridad en infraestructuras críticas (muy de moda en ambientes más técnicos, caso Stuxnet)
- Idoneidad y asimilación del Esquema Nacional de Seguridad
- Importancia del ciclo de desarrollo del software en la seguridad del mismo
- Los aspectos de seguridad relacionados con la virtualización y la "nebulización" de las aplicaciones.
- La problemática de la fuga de información digital, tan de moda gracias a Wikileaks, y contra la que ya lleva años intentando hacer algo las industrias discográficas y cinematográficas.
- La seguridad normativa y estándares contra la aplicación práctica y efectiva de medidas. La falta de formación en el factor humano.
- La explotación en el lado del cliente y la falta de conciencia sobre el alcance de este tipo de ataques.
- La autentificación de doble factor, claves de un sólo uso y sistemas de login único. ¿Avanzan las tendencias en direcciones contrarias?
- La firma electrónica, los correos electrónicos y las evidencias digitales como medio de prueba ante un tribunal.

Conclusiones del debate:

Plan de seguridad

Un responsable tiene que hacer seguro el negocio, sin hacer que este negocio se ralentice, que conozca cómo funciona la empresa. En una pyme es el informático de cabecera. En una gran empresa si debe haber un especialista de seguridad que pida cosas que no tiene por qué gustar al responsable de IT.

El plan de seguridad tiene que hacerse al principio del proyecto. El plan de seguridad de la información debe existir en la mayor parte de las empresas, independientemente de su tamaño, eso sí, según su tamaño y complejidad, así será su plan de seguridad.

Al subcontratar delegamos que nos realicen tareas, no nos eximen de "responsabilidades"

La seguridad informática en las empresas, erróneamente, resulta que no es un detalle prioritario.

Los profesionales de la ciber seguridad en España se conocen bien y hay bastante buen rollo.

Si un prestador de servicios no admite auditorias, da mala señal.

Las empresas se defienden a futuro sobre problemas de seguridad que ya les han ocurrido.

Amenazas nuevas y comunes

La gran lacra de la ciber seguridad está en las filtraciones de información por parte de los trabajadores de la empresa.

Nuevas amenazas: Los iPad & iPhone.

El riesgo de los dispositivos móviles ante seguridad es muy alto.

La creación de Apps con troyanos será cada vez más habitual y el control de las empresas para publicar Apps no es 100% rigurosa.

El cibercrimen crece mucho más que otras actividades delictivas cómo las drogas y se le suman motivaciones tipo políticas, terroristas, etc…

La calidad de defensa cibernética de los grupos delictivos es cada vez mayor

La legislación sobre ciber seguridad no es global

Para que las pruebas "digitales" sean aprobadas ante los jueces, tienen que ser tratadas y expuestas con mucha escrupulosidad, por falta de conocimientos en dicho ámbito.

No hay una regulación para ser perito informático y por tanto estos no están obligados a estar al día de las últimas tecnologías o de la legislación.

A las empresas de seguridad les cuesta mucho conseguir rentabilidad debido a los amplios recortes de las empresas en el concepto de seguridad informática.

Redes sociales

Amenazas ¿nuevas? en las redes sociales (también muy de moda)

Hay muy poca conciencia social respecto de los peligros de la privacidad de las redes sociales. La próxima generación ya habrá aprendido de los peligros de las redes sociales.

Dropbox, google docs… son todos servicios donde se debe dar por perdida la absoluta privacidad de nuestros datos.

"Puerto seguro" es la empresa o nación que cumple leyes tipo LOPD de su país equiparable al régimen Europeo. Normativas caras de cubrir.

Con los juzgados, siempre 3 copias, más una copia extra, que en los juzgados hay tendencias a "perderse" cosas.

En España se quiere montar la seguridad sobre el hardware ya montado y no es así.

Hay un gran problema de seguridad en las infraestructuras críticas.

Cuando cualquier proceso de seguridad acaba pasando por un usuario final, ahí se produce un fiasco.

Cloud Computing

Cualquier servicio de alojamiento remoto de documentos que no cumple expresamente con la legislación española no se puede ni plantear usar, si eres abogado.

Seguridad en servicios externalizados o en la nube (muy de moda): Para usar el mail hay que usar pgp, nadie lo usa. Para temas sensibles no se pueden usar servicios tipo nube o Google Apps.
Va a haber muchos servicios que vendrán muy bien a las empresas, pero los absolutamente críticos todavía no están seguros en la nube.

Hay oferta por llevar el mail "seguro" a la nube, pero son servicios muy caros.

Si estás dispuesto a pagar, hay servicios muy buenos de seguridad.

Cloud hosting seguro es una tendencia.

Desarrollo web: problemas y tecnología

Hay pocas barreras de entrada en la industria del desarrollo web al no ser una industria regulada, por lo que suele haber poca preocupación por la seguridad en muchas páginas web.

Muchos fallos de seguridad en la programación, viene porque hay subcontrataciones donde se exige velocidad, sin exigir documentación.

Las fechas límite obligan a acabar determinados proyectos rápido y dejar de lado la seguridad, porque no se tiene una correcta apreciación del riesgo.

Lo suyo es auditar el código y cobrar por cada vulnerabilidad encontrada al programador.

Hay formación insuficiente en la universidad sobre la seguridad informática.

Si la empresa lleva mal los temas de TI, seguro va a llevar mal la Ciber seguridad.

Ante el error humano no hay sistema de ciber seguridad que funcione adecuadamente.

Los mayoristas de hardware de seguridad mangonean libremente respecto a qué se va a comprar en las grandes empresas.

La rotación de dispositivos de tecnología en altos directivos de empresas es altísimo, dispositivos con información sensible. Se “pierden” en regalos a familiares muchos gadgets.

Para las llaves de uso único, es un problema de usabilidad el llevar encima el gestor de esas contraseñas y si se aplica que sea en todas las capas. ¿Para qué sirven si luego las empresas quieren usar sistemas Single-sign-on para evitar tener que hacer login en las aplicaciones?

Validez o impacto de las tecnologías actuales en la protección de los sistemas informáticos (antivirus, IDS, honeypots, firewalls, WAFs…): La solución que aportan es relativa pero es muy necesario tener estas herramientas.

Legal

Los expertos que publican sobre fallos de ciber seguridad están muy desprotegidos de cara a ser buscados por responsabilidad por revelar fallos de terceros.

Idoneidad y asimilación del Esquema Nacional de Seguridad: Basado en ISO27k que es bueno, pero el problema estará en ver cómo se implanta. Ni empresas ni instituciones lo van a implementar bien.

En Justicia, hay fiscales que se están formando en Ciber Seguridad, aunque la capacitación de los juristas en general está muy alejada de comprender los problemas de ciberdelincuencia.

Importancia (o no) del cumplimiento de estándares de seguridad por las empresas

El estándar de seguridad ISO 27001 es excesivo para una Pyme.

Es una falsa premisa pensar que el DNI electrónico es 100% seguro.

Desayuno de Trabajo Networking Activo sobre **Ciber Seguridad** patrocinado por **Hostarting**, comparador de precios de hosting que cuenta con la información de los planes de hosting, servidores dedicados, housing o registro de dominios de las principales empresas del país

Algunas de las empresas participantes en el Desayuno de Trabajo fueron : ESET (Nod 32), FLAG Solutions S.L., HispaSec, Hostarting, Networking Activo, Panda Security, Razona LegalTech, s21sec, Security by default, SEINHE y VaniOs.

Creador del documento: Emilio Márquez Espino CEO de Networking Activo.