Jornada de formación continua:

“Ciberamenazas, ¿estamos realmente preparados?”

El pasado 3 de Marzo tuvo lugar la Jornada de Formación mensual de ISACA Barcelona que trató sobre **"ciberamenazas, estamos realmente preparados?"** En manos de **Carlos Solé**, Information Security Director de "CaixaBank".

La Jornada fue patrocinada por **Deloitte, Auren, Innevis, Víntegris, Cloudjacket, ItAdvisory, Andornet, OptimumTIC** y con el suporte institucional de **Coettc, COEINF, Consejo General de Economistas, IAITG, ISMS, itSMF, UAB, ATI, Telecos.cat, CCJCC, CESICAT y el Instituto Municipal de Informàtica Hàbitat Urbano - Ajuntament de Barcelona**.

El **vicepresidente de ISACA Barcelona, Joaquim Altafaja,** introdujo la jornada comentando las actividades de la asociación, anunciando los nuevos cursos de preparación a los exámenes del mes de junio, las nuevas iniciativas de convenios con PMI y Fórum CIS. Anunció el próximo Congreso **gigaTIC 2015**, conjuntamente con itSMF, **el próximo 16 de abril**.

El Sr. Carles Solé comenzó con una referencia al elevado incremento del número de vulnerabilidades y donde en 2011 se referenciado por años (http://hackmageddon.com/) ahora se cuentan por días, lo que representa un gran cambio en poco tiempo.

El Sr. Carlos Solé comentó que hay tres paradigmas a tener en cuenta:

a) **El outsourcing** como puerta de entrada a nuestra organización por incidentes de seguridad, ya que dispone de unos niveles de seguridad diferentes a los nuestros, y nosotros tenemos una cierta limitación de control.
b) **El Cloud** como solución, hay una clara mejora continua en la evolución de los servicios cloud, así como una mejora en los costes para proveer nuestros servicios internos, pero al mismo tiempo también se produce una pérdida de control sobre la infraestructura cuando es de terceros.
c) **El BYOD**, tiene riesgos inherentes, aunque hay una evolución de mejora, hay que poder aislar, en cualquier caso, lo que es personal de lo corporativo, pero la parte personal también debe controlarse ya que hay una gran cantidad de apps al alcance de los usuarios que disfrutan de un exceso de derechos sobre la información que reside en el terminal y esto se debe evitar.

El ponente continuó haciéndose esta pregunta: **¿Y ahora qué?**

Debemos ponernos al lado de los atacantes, entender **qué pueden querer hacer y cómo**, para estar lo más preparados posible a lo que aún no nos ha pasado.
Debemos tener ojos en todas partes, disponer de **monitorización permanente**, SIEM, IPS, SSL, ... todo centralizado y **mirar todo lo que pasa**.

En temas de **ciberintel·ligència**, estamos en pañales, en un estado muy primario, y es imprescindible que mejoremos en este sentido. **Aprender a compartir**, en puntos neutros bidireccionales que permitan aprovechar el trabajo realizado por una organización y que el resto ya puedan disponer de este conocimiento lo antes posible, **por el beneficio de todos**.

Pero nos debemos enfocar en el futuro, **en lo predictivo**, o Big Data, ... aprender cuál es el funcionamiento habitual y que se entienda que ha habido un cambio. Esto es lo que nos ayudará en el futuro próximo de la ciberseguridad, **estar preparados por los ciberataques**.

Como los **Espartanos**, o se están defendiendo o se preparan **para la defensa permanentemente**. Nos tenemos que preparar mediante simulaciones de escenarios conocidos o imaginados por todo lo que se nos pueda presentar.

Tras la presentación, se suscitaron algunas preguntas por parte de los asistentes. Se enfatizó en la necesidad de **cooperación entre las organizaciones** y la dificultad de llevarlo a cabo. También se comentó que, en el futuro, será necesario continuar con la **seguridad perimetral**, pero que cada vez más, el análisis de comportamiento será más importante.

Barcelona 3 de març 2015