Barcelona, Spain

Jornada de formación continua:

" Vulnerabilidades y fraude en canales digitales transaccionales"

Los Sres. Joaquim Altafaja y Miguel-Angel Hervella durante la conferencia

Dentro del marco de conferencias de formación continua, se celebró el pasado 1 de abril de 2014, en la **Sala de Actos del CTiTI**, una interesante charla sobre **"Vulnerabilidades y fraude en canales digitales transaccionales"**.

La Jornada fue patrocinada por **Deloitte** , **Auren** , **Innevis** , **Víntegris** , **Cloudjacket** y **Andornet** y con el soporte institucional de **Coettc** , **COEINF** , **Consejo General de Economistas** , **IAITG** , **ISMS**, **itSMF** , **UAB , ATI**, **Telecos.cat**, **CCJCC, CESICAT y el Institut Municipal d'Informàtica Hàbitat Urbà - Ajuntament de Barcelona**.

En la presentación de la Jornada, el Sr**. Joaquim Altafaja** hizo mención de las actividades del capítulo de **ISACA Barcelona** destacando la labor de los distintos grupos de trabajo**,** hizo de nuevo mención de la celebración de **EUROCACS y Cyberlimpics en Barcelona**. También se informó de los cursos de preparación a los exámenes para la obtención de los Certificados **CISA, CISM i CGEIT** que **ISACA Barcelona** viene realizando gracias a los profesores voluntarios sin los cuales sería imposible realizarlos.

También anunció la celebración de la **Asamblea Ordinaria** que se celebrará el **10 de Junio** y donde se procederá a elegir una nueva directiva.

A continuación, tomó la palabra el **Sr. Miguel-Angel Hervella,** para hacer una exposición sobre la problemática con la utilización de distintos canales de comunicación entre **el negocio y el cliente** desde distintos aspectos donde **la usabilidad y la seguridad** tienen carácter prioritario.

El **Sr. Miguel-Angel Hervella**, hizo mención de los distintos ataques que en estos momentos está sufriendo la banca en general y los cajeros automáticos en particular con una nueva manera de acceder a ellos desde **la red de cajeros**, donde una intrusión en esta red facilita el fraude.

Comentó la importancia entre la necesidad de facilitar **el uso de las nuevas tecnologías**, las **necesidades del negocio** y las medidas contra el fraude, un equilibrio que a veces es difícil de conseguir.

Destacó que la proliferación del **malware ha crecido en un 40%** y que la utilización de las tabletas y Smartphone complica más aún la defensa contra los ataques de estos programas.

Dedicó un tiempo a explicar la importancia de la **ingeniería social** para acceder a los servidores y áreas reservadas de un alto nivel sensible y que para ello también se está utilizando las **redes sociales**.

Por último dio un repaso sobre cómo se puede **defenderse de estos ataques** con herramientas, pero sobre todo con **organización, procedimientos y protocolos** establecidos por la compañía.
Destacó el tener protocolos de **actuación ante incidencias, utilizar el hacking ético** para detectar debilidades, controlar la **calidad de las transacciones** y el **comportamiento del usuario** teniendo reglas de comportamiento.

Por último hubo un extenso debate de cómo conseguir una **mayor eficacia** contra el malware, ataques utilizando ingeniería social y a la vez, tener **aplicaciones sencillas para los usuarios** de manera que estos no rechacen estas aplicaciones. También se comentó que **la inversión en seguridad es proporcional a los ataques, a menor inversión mayor riesgo**.

A Barcelona 1 de abril 2014