Jornada de formación continua:

“Reprogramando el cerebro contra los ciberataques”

El pasado 19 de setiembre tuvo lugar la jornada mensual de formación en el Citilab de Cornallà. La jornada versó sobre la manera de afrontar los riesgos de los ciberataques. Bajo el título de “Reprogramando el cerebro contra los ciberataques” Juan Carlos Ruiloba, CCEO-CTO Scienti¬fic Intelligence Team 1, S.L. nos introdujo en la manera de hacer frente a estos ataques.

La Jornada fué patrocinada por Deloitte, Auren, Prosegur, Víntegris, Andornet, OptimumTIC, BNFIX y con el suporte institucional de Coettc, COEINF, Consejo General de Economistas, IAITG, ISMS, itSMF, UAB, ATI, Telecos.cat, CCJCC, CESICAT , BQB, Andorra Telecom i l'Institut Municipal d'Informàtica Hàbitat Urbà - Ajuntament de Barcelona.

Juan Carlos planteó que los cibercriminales se adaptan a nuestras defensas para vulnerarlas dinámicamente a medida que las implementamos. Nuestras estrategias de defensa deben cambiar acorde a las posibles amenazas y no es suficiente con soluciones estándar y globales, debemos de estar siempre un paso por delante del próximo ataque para evitar la efectividad del mismo.

Se hizo la siguiente pregunta, ¿Cuál es la solución?: Adquirir e implementar las medidas tradicionales, actualizando los parches servidos por los fabricantes de software, implementando las últimas versiones de los antivirus y antimalware, etc. pero la mejor manera de defendernos, la nueva tecnología en nuestra defensa es el cerebro.

Debemos de tener la capacidad para encontrar a esas personas que saben ponerse en la mente de los atacantes, también podemos y debemos actualizar a aquellas personas que ya trabajan con nosotros. Nuestro nuevo antimalware comienza con la "Reprogramación del cerebro contra los Ciberataques" empezando con el nuestro cerebro.

Basándose en este concepto de saber actuar anticipándose a los ataques, Juan Carlos Ruiloba nos puso al corriente de las nuevas maneras de antimalware, antivirus y como la ingeniería social está dañando a los usuarios de las nuevas tecnologías.

Habló de la utilización de los smartphones, tabletas y por supuesto, ordenadores, que se utilizan para ejecutar los ataques, sin que los propietarios de estos elementos, cada vez más potentes, conozcan el uso fraudulento que realizan.

También se comentó el impacto que tiene la Internet of Things, por su expansión que está teniendo y su falta de seguridad en el diseño.

Finalmente se abrió turno para el debate en el que se suscitaron múltiples cuestiones y terminó con un refrigerio en las mismas instalaciones.

Barcelona 27 setiembre 2017