Jornada de formació continua:

“Ciberamenaces, estem realment preparats?”

El proppassat 3 de Març va tenir lloc la Jornada de Formació mensual d’ISACA Barcelona que va tractar sobre **“Ciberamenaces, estem realment preparats?”** a mans del Carles Solé, Information Security Director de “CaixaBank”**.**

La Jornada va ser patrocinada per **Deloitte, Auren, Innevis, Víntegris, Cloudjacket, ItAdvisory, Andornet, OptimumTIC** i amb el suport 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 **vicepresident de ISACA Barcelona, Joaquim Altafaja**, va introduir la jornada comentant les activitats de l'associació, anunciant els nous cursos de preparació als exàmens del mes de juny, les noves iniciatives de convenis amb **PMI i CIS Fòrum**. Va anunciar el proper Congrés **gigaTIC 2015**, conjuntament amb **itSMF, el pròxim 16 d'abril**.

El Sr. Carles Solé va començar amb una referència a l’elevat increment del nombre de vulnerabilitats i on al 2011 es referenciaven per anys (http://hackmageddon.com/) ara es compten per dies, i això representa un gran canvi en poc temps.

El Sr. Carles Solé comentà que hi ha amb tres paradigmes a tenir en compte:

a) **L'outsourcing** com a porta d'entrada a la nostra organització per incidents de seguretat, ja que disposa d'uns nivells de seguretat diferents als nostres, i nosaltres tenim una certa limitació de control.
b**) El Cloud** com a solució, hi ha una clara millora continua en l'evolució dels serveis cloud, així com una millora en els costos per proveir els nostres serveis interns, però al mateix temps també es produeix una pèrdua de control sobre la infraestructura quan és de tercers.
c) **El BYOD**, te riscos inherents, tot i que hi ha una evolució de millora, cal poder aïllar, en qualsevol cas, el que és personal del que és corporatiu, però la part personal també s'ha de controlar ja que hi ha una gran quantitat d'apps a l'abast dels usuaris que gaudeixen d'un excés de drets sobre la informació que resideix en el terminal i això s'ha d'evitar.

El ponent va continuar fent-se aquesta pregunta: **I ara?**

Hem de posar-nos al costat dels atacants, **entendre què poden voler fer i com**, per estar el més preparats possible a allò que encara no ens ha passat.
Hem de tenir ulls per tot arreu, **disposar de monitoratge permanent**, SIEM, IPS, SSL, … tot centralitzat i mirar tot el que passa.

En temes de **ciberintel·ligència**, estem a les beceroles, en un estat molt primari, i és imprescindible que millorem en aquest sentit. **Aprendre a compartir**, en punts neutres bidireccionals que permetin aprofitar la feina feta per una organització i que la resta ja puguin disposar d'aquest coneixement al més aviat possible, **pel benefici de tots**.

Però ens hem d'enfocar en el futur, **en allò predictiu,** o Big Data, … aprendre quin és el funcionament habitual i que entengui que hi ha hagut un canvi. Això és el que ens ajudarà en el futur pròxim de la ciberseguretat, **estar preparats pels ciberatacs**.

Com els Espartans, o s'estan defensant o es **preparen per a la defensa permanentment**. Ens hem de preparar mitjançant simulacions d'escenaris coneguts o imaginats per tot allò que se'ns pugui presentar.

Després de la presentació, es van suscitar algunes preguntes per part dels assistents. Es va emfatitzar en la **necessitat de cooperació entre les organitzacions** i la dificultat de portar-lo a terme. També es va comentar que, en el futur, serà necessari continuar amb la **seguretat perimetral**, però que cada vegada més, **l'anàlisi de comportament** serà més important.

Barcelona 3 de març 2015