Jornada de formación continua:

“Reprogramant el cervell contra els ciberatacs”

El passat 19 de setembre va tenir lloc la jornada mensual de formació al Citilab de Cornallà. La jornada va versar sobre la manera d'afrontar els riscos dels ciberatacs. Sota el títol de "Reprogramant el cervell contra els ciberatacs" Juan Carlos Ruiloba, CCEO-CTO Scientific Intelligence Team 1, S.L. ens va introduir en la manera de fer front a aquests atacs.

La Jornada va ser patrocinada per Deloitte, Auren, Prosegur, Víntegris, Andornet, OptimumTIC, BNFIX i amb el suport 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.

Joan Carles va plantejar que els cibercriminals s'adapten a les nostres defenses per vulnerar dinàmicament a mesura que les implementem. Les nostres estratègies de defensa han de canviar d'acord a les possibles amenaces i no n'hi ha prou amb solucions estàndard i globals, hem d'estar sempre un pas per davant del proper atac per evitar l'efectivitat del mateix.

Es va fer la següent pregunta, Quina és la solució ?: Adquirir i implementar les mesures tradicionals, actualitzant els pegats servits pels fabricants de programari, implementant les últimes versions dels antivirus i antimalware, etc. però la millor manera de defensar-nos, la nova tecnologia en la nostra defensa és el cervell.

Hem de tenir la capacitat per trobar a aquestes persones que saben posar-se en la ment dels atacants, també podem i hem d'actualitzar a aquelles persones que ja treballen amb nosaltres. El nostre nou antimalware comença amb la "Reprogramació del cervell contra els Ciberatacs" començant amb el nostre cervell.

Basant-se en aquest concepte de saber actuar anticipant-se als atacs, Juan Carlos Ruiloba ens va posar al corrent de les noves maneres de antimalware, antivirus i com l'enginyeria social està danyant als usuaris de les noves tecnologies.

Va parlar de la utilització dels smartphones, tauletes i per descomptat, ordinadors, que s'utilitzen per a executar els atacs, sense que els propietaris d'aquests elements, cada vegada més potents, coneguin l'ús fraudulent que realitzen.

També es va comentar l'impacte que té Internet of Things, per la seva expansió que està tenint i la seva falta de seguretat en el disseny.

Finalment es va obrir torn per al debat en el qual es van suscitar múltiples qüestions i va acabar amb un refrigeri a les mateixes instal·lacions.

Barcelona 27 setiembre 2017