Jornada de formación continua:

“Noves Tècniques d’Atac”

El 10 de desembre 2019 va tenir lloc la jornada mensual de formació a l'Auditori de Citilab de Cornellà de Llobregat. La jornada va versar sobre la seguretat en el núvol amb el títol de "**Noves tècniques d'atac**", i va comptar amb la participació, com a ponent, de **Mario Díaz Caldera**, Security Consultant d'E & I.

La Jornada va ser patrocinada per Deloitte, Auren, s21sec, Víntegris, Andornet, OptimumTIC, ÍTACA i amb el suport institucional de Coettc, COEINF, Consell General d'Economistes, IAITG, ISMS, itSMF, UAB, ATI, Telecos.cat, CCJCC, CESICAT , BQB, Andorra Telecom i l'Institut Municipal d'Informàtica Hàbitat Urbà - Ajuntament de Barcelona.

En el transcurs de la jornada de formació organitzada per No cON Name i ISACA Barcelona, **José Nicolas Castellano i Joan Barceló** en representació de les seves respectives organitzacions, van signar **un conveni marc de col·laboració entre les dues entitats**.

Mario Díaz va fer una introducció sobre diferents tipus d'atacs cibernètics i les seves conseqüències econòmiques i pèrdua de reputació. En la seva exposició es va centrar en tres tipus d'atac frau de **l'CEO, sextorsió i Warranty Exploitation**.

Va explicar com els ciberdelinqüents **utilitzen el phishing** i l'enginyeria social per realitzar l'atac de l'CEO. Aquest consisteix en el fet que els atacants utilitzen el nom d'una persona o d'un departament i envien correus a un altre usuari d'un departament demanant informació sobre una **TRANSACCIÓ o PROCEDIMENT**. Si aconsegueixen rebre resposta aquesta ve amb documents adjunts que els utilitzen per seguir demanant informació. L'atacant es fa un expert en **PROCEDIMENTS i workflows**.

Seguidament **Mario** ens va fer una exposició de l'atac denominat **sextorsió** que consisteix a amenaçar el receptor d'un correu a divulgar contingut sexual, encara que aquest no existeixi. El contingut si pot ser real si s'han visitat webs amb aquest **tipus de contingut o simplement hi hagi hagut converses amb íntimes amb altres persones que no es vulgui que es divulguin**. El fet de rebre una amenaça d'aquest tipus fa que les víctimes, davant la incertesa caiguin en mans d'aquest tipus d'atacs.

Finalment, ens va parlar de **l'Warranty Exploitation**, en aquest tipus d'atac, Es basa en explotar grans companyies per rebre productes de manera gratuïta sense pagar per ells. Quan els aconsegueixen els venen obtenint grans beneficis que es tradueixen en pèrdues petites per a les companyies donat el seu gran tamany. Entre altres formes d'engany, falsifiquen els números de sèrie dels productes i reclamen l'enviament del material. Un clar exemple és el d'un jove que va estafar a **Amazon retornant les caixes plenes de paper**.

A la fi de la ponència es va establir un interessant debat de com cal prendre mesures de seguretat per no fer fàcil la feina als delinqüents.

Barcelona 20 desembre 2019