Jornada de formación continua:

# “Nuevas Técnicas de Ataque”

El pasado 10 de diciembre 2019 tuvo lugar la jornada mensual de formación en el Auditorio del Citilab de Cornellà del Llobregat. La jornada versó sobre la seguridad en la nube con el título de "**Nuevas tácnicas de ataque**", y contó con la participación, como ponente, de **Mario Díaz Caldera**, Security Consultant de E&Y.

La Jornada fue patrocinada por Deloitte, Auren, s21sec, Víntegris, Andornet, OptimumTIC, ITACA 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.

En el transcurso de la jornada de formación organizada por No cON Name e ISACA Barcelona, **José Nicolas Castellano y Joan Barceló** en representación de sus respectivas organizaciones, firmaron un **convenio marco de colaboración** entre las dos entidades.

**Mario Díaz** hizo una introducción sobre distintos tipos de ataques cibernéticos y sus consecuencias económicas y pérdida de reputación. En su exposición se centro en tres tipos de ataque fraude del **CEO, Sextorsión y Warranty Exploitation**.

Explicó como los ciberdelincuentes **utilizan el phishing** y la ingeniería social para realizar el ataque del CEO. Este consiste en que los atacantes utilizan el nombre de una persona o de un departamento y envían correos a otro usuario de un departamento **pidiendo información** sobre una **TRANSACCIÓN o PROCEDIMIENTO**. Si consiguen recibir respuesta esta viene con documentos adjuntos que los utilizan para
seguir pidiendo información. El atacante se hace un experto en **PROCEDIMIENTOS y WORKFLOWS**.

Seguidamente **Mario** nos hizo una exposición del ataque denominado **sextorsión** que consiste en amenazar al receptor de un correo en divulgar contenido sexual, aunque este no exista. El contenido si puede ser real si se **han visitado webs con este tipo de contenido o simplemente haya habido conversaciones con íntimas con otras personas** que no se quiera que se divulguen. El hecho de recibir una amenaza de este tipo hace que las víctimas, ante la incertidumbre caigan en manos de este tipo de ataques.

Por último, nos habló del **Warranty Exploitation**, en este tipo de ataque, Se basa en explotar grandes compañías para recibir productos de manera gratuita sin pagar por ellos. Cuando los consiguen los venden obteniendo grandes beneficios que se traducen en pérdidas pequeñas para las compañías dado su gran tamaño. Entre otras formas de engaño, **falsifican los números de serie de los productos** y reclaman el envío de del material. Un claro ejemplo es el de un joven que **estafó a Amazon devolviendo las cajas llenas de papel**.

Al final de la ponencia se estableció un interesante debate de cómo hay que tomar medidas de seguridad para no hacer fácil el trabajo a los delincuentes.

Barcelona 20 de diciembre 2019