Jornada de formación continua:

“Principales tendencias en materia de ciberseguridad”

El pasado 19 de octubre tuvo lugar la jornada de formación que ISACA Barcelona ofrece todos los meses y de nuevo hubo una gran participación. En la conferencia, a cargo de Santiago Romeu, responsable del Servicio de Prospectiva y Análisis de Tendencias de la Agencia de Ciberseguretat de Catalunya se habló de las principales amenazas detectadas en el ámbito de la ciberseguridad.

La Jornada fue patrocinada por Deloitte, Auren, s21sec, Víntegris, Andornet, OptimumTIC, ITACA y con el apoyo institucional de Coettc, COEINF, Consejo General de Economistas, IAITG, ISMS, itSMF, UAB, ATI, Telecos.cat, CCJCC, BQB, Andorra Telecom y el Instituto Municipal de Informática Hábitat Urbano - Ayuntamiento de Barcelona.

Santiago Romeu, hizo una introducción de las actuales tendencias en materia de ciberseguridad haciendo un repaso de la evolución del cibercrimen y como este, con la transformación digital de la sociedad, se ha ido especializando y ha ganado en experiencia.

El ponente dedicó una parte de su exposición para explicar la importancia de los ataques de ransomware y como se ha mantenido activo y renovado continuamente, pasando de cifrar los datos exigiendo un rescate para recuperar la información, hasta robar los datos y amenazar con venderlos o publicarlos, en lo que se ha llamado doble y triple extorsión.

A continuación, habló sobre los ataques a la cadena de suministro, en especial a los ataques a las empresas de servicios TIC explotando la confianza que los clientes depositan en este tipo de proveedores. Un ataque a un proveedor de servicios, desarrollador de software o que monitorea la red, los cibermalhechores pueden acceder a todos sus clientes y difundir su programa maligno.

Santiago hizo hincapié sobre como la ciberdelincuencia se ha aprovechado del teletrabajo y de la actividad en Internet en general, viendo en ello una oportunidad para comprometer a organizaciones a través de las tecnologías del trabajo a distancia, como pueden ser las VPN, RPD, correo electrónico o plataformas de videoconferencia, explotando las vulnerabilidades de estas.

Comentó como la ciberdelincuencia aprovecha la fuga y robo de datos, para extorsionar a empresas y particulares con la amenaza de hacer pública la información, realizar phishing dirigido o poniendo a la darkweb los datos personales robados.

Por último, Santiago mencionó las distintas medidas policiales y gubernamentales que tratan de luchar contra esta lacra explicando algunos éxitos como son las detenciones de grupos organizados y cierre de webs dedicadas el cibercrimen.

Barcelona 25 de octubre 2021