Jornada de formació contínua:

“Principals tendències en matèria de ciberseguretat”

El passat 19 d'octubre va tenir lloc la jornada de formació que ISACA Barcelona ofereix tots els mesos i de nou va haver-hi una gran participació. En la conferència, a càrrec de Santiago Romeu, responsable del Servei de Prospectiva i Anàlisi de Tendències de l'Agència de Ciberseguretat de Catalunya ens va parlar de les principals amenaces detectades en l'àmbit de la ciberseguretat.

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

Santiago Romeu, va fer una introducció de les actuals tendències en matèria de ciberseguretat fent un repàs de l'evolució del ciberdelicte i com aquest, amb la transformació digital de la societat, s'ha anat especialitzant i guanyant en experiència.

El ponent va dedicar una part de la seva exposició a explicar la importància dels atacs de ransomware i com s'ha mantingut actiu i renovat contínuament, passant de xifrar les dades exigint un rescat per a recuperar la informació, fins a robar les dades i amenaçar amb vendre'ls o publicar-les, en el que s'ha anomenat doble i triple extorsió.

A continuació, va parlar sobre els atacs a la cadena de subministrament, especialment als atacs a les empreses de serveis TIC explotant la confiança que els clients dipositen en aquesta mena de proveïdors. Un atac a un proveïdor de serveis, desenvolupador de programari o que monitora la xarxa, els ciberdelinqüents poden accedir a tots els seus clients i difondre el seu programa maligne.

Santiago va posar l'accent sobre com la ciberdelinqüència s'ha aprofitat del teletreball i de l'activitat en Internet en general, veient en això una oportunitat per a comprometre a organitzacions a través de les tecnologies del treball a distància, com poden ser les VPN, RPD, correu electrònic o plataformes de videoconferència, explotant les vulnerabilitats d'aquestes.

Va comentar com, la ciberdelinqüència aprofita la fugida i robatori de dades, per a extorquir a empreses i particulars amb l'amenaça de fer pública la informació, realitzar phishing dirigit o posant a la darkweb les dades personals robades.

Finalment, Santiago va esmentar les diferents mesures policials i governamentals que tracten de lluitar contra aquesta xacra explicant alguns èxits com són les detencions de grups organitzats i tancament de webs dedicades el ciberdelicte.

Barcelona 25 d'octubre 2021