El forense informàtic Bruno Pérez desvetlla a Figueres la tàctica dels hackers

En la seva conferència, ha alertat de les amenaces actuals de ciberatacs si no prenem mesures



Bruno Pérez, amb les representants de la XEC a Figueres.

L'altempordanès Bruno Pérez, expert en ciberseguretat, ha fet una ponència recentment a Figueres, al Museu de la Tècnica de l'Empordà, i ha desvetllat quines són les amenaces actuals i realsa les quals tots estem exposats si no prenem mesures de protecció davant dels ciberatacs. Bruno Pérez està especialitzat com a perit judicial informàtic forense, a més de ser professor de la càtedra de Ciberseguretat de la UDIMA (Universidad a Distancia de Madrid).

El segrest i petició de rescat per les dades encriptades, l'espionatge, la competència deslleial, el robatori de dades personals i d'informació rellevant per a les empreses són situacions que s'estan produint a dia d'avui i són, alhora, causants de danys molt greus.

La XEC Empordà (Xarxa d'Emprenedores Competents) ha volgut incloure, en el seu programa de conferències i tallers divulgatius, un tema tan candent com és la delinqüència computacional. A partir de la ponència de Bruno Pérez, les integrants d'aquesta entitat han elaborat un llistat de conclusions:

Bruno Pérez ha detallat, en la seva xerrada, com pensa un hacker i quines pautes segueix per realitzar un bon atac i aconseguir el seu objectiu. Aquest és, segons l'expert en ciberseguretat, l'esquema que seguiria un hacker informàtic per perpetrar un atac:

Per arribar al seu objectiu, confecciona un pla d'atac mètodic, estudiant tota la informació que es troba a la xarxa i sempre aprofitant errors informàtics i esquerdes que s'hagin produït per poder entrar.

La tasca del forense informàtic és, segons Bruno Pérez, buscar les empremtes de l'atacant. Aquests professionals, sempre han d'anar molt en compte amb la llei de protecció de dades(LPD).

El hacker té al seu abast tota una sèrie d'eines de les quals es pot servir per fer un atac:

Google:Amb impressores connectades a internet. Inclús es pot veure què s'imprimeix.
Càmeres de vigilància: La configuració és molt important. Poden arribar a visualitzar l'interior d'un habitatge.
Directoris de discs compartits: Les carpetes que s'utilitzen.
I també:Webcams, Routers, Iphones, Pen Drive...

Bruno Pérez ha alertat que el hacker, a més, pot acabar infectant amb virus milions de persones quan la seva intenció és atacar un únic objectiu.

El ponent ha parlat també de la Deep Web,"aquella zona fosca d'Internet on es mou tot el que és il·legal, on és couen el ciberatacs. Una part oculta del web en la qual és molt recomanable no endinsar-t'hi perquè és realment molt complexa i perillosa".

Entre les recomanacions que dóna l'expert en ciberseguretat als assistents a la seva ponència, tot plegat per intentar estar "una mica protegits davant dels possibles atacs", cal prendre nota dels següents:

Bruno Pérez ha fet una extensa conferència per donar una visió àmplia de la seva feina. Ha parlat de l'Enginyeria Social enfocada cap als grups de persones que generen estafes. "Una de les portes d'entrada més ràpides que utilitzen per guanyar-se la confiança de les persones i robar-los les dades", adverteix. I també comenta: "Vam descobrir que hi ha Granges de Persones que es dediquen, a canvi del seu temps, a buscar debilitats a Internet per robar dades. Si obtenen resultats hi ha recompensa."

Els grups cibercriminals (els dolents), com explica Bruno Pérez, estan molt ben organitzats a escala internacional, i fins i tot han aconseguit blanquejar diners. Un exemple n'és l'estafa Nigeriana.

"Els forenses informàtics (els bons) treballem molt per poder col·laborar de la millor manera en l'àmbit internacional, però degut a lleis poc clares o bé per falta de comunicació entre països no ho aconsegueixen de manera àgil i eficient", assenyala l'expert.

Les representants de la XEC han volgut destacarles cares de sorpresa dels assistentsa l'acte a mesura de la

descoberta de les tàctiques i estafes que Bruno Pérez ha relatat, una a una. Entre aquestes, l'estafa del CEO, A man-in-the-middle attack, la Sextorsió...

"La seguretat depèn de nosaltres i cada vegada més, ja que estem exposats a patir atacs que ens arribin per molts canals diferents. No afecta únicament les empreses, tots nosaltres podem arribar a ser una font d'ingressos per als cibercriminals."

Font del document:
http://www.emporda.info/tecnologia/2017/03/02/forense-informatic-bruno-perez-desvetlla/347147.html?utm_source=rss