mossos d'esquadra

Foment del Treball Nacional

TREBALLEM PER LA PREVENCIÓ

Els sistemes d'informació són un fonament quasi imprescindible per al desenvolupament de qualsevol activitat empresarial. Els avenços tecnològics, l'accés massiu a Internet o els usuaris amb informació i formació insuficients, han contribuït a generar noves amenaces i vulnerabilitats per a les empreses.

Darrerament s'ha detectat una nova modalitat delinqüencial relacionada amb l'ús de les noves tecnologies a les empreses:

Aquesta es detecta per un funcionament incorrecte en algun dels equips informàtics de l'empresa. A la pantalla de l'equip afectat, apareix una finestra escrita en anglès on s'explica a l'usuari que s'ha trobat arxius amb contingut pornogràfic a la memòria de l'ordinador.

El missatge continua dient que s'han vist obligats a bloquejar-lo i a codificar tots el programes que contenia. Afegeix que la solució passa per pagar una quantitat de diners.

Fan constar que una vegada fet el pagament s'enviarà un programa per desencriptar i poder recuperar la informació codificada, evidentment es faci o no el pagament l'ordinador afectat continua bloquejat.

Aquest tipus de demanda mai la fa un organisme oficial. Es tracta d'una estafa organitzada i dissenyada per grups criminals.

Es per això que des de la Policia de la Generalitat – Mossos d'Esquadra, es considera oportú i necessari fer difusió d'aquest nou tipus d'extorsió a les Petites i Mitjanes Empreses de Catalunya i al col·lectiu empresarial de manera genèrica.

Per tal de prevenir i minimitzar els efectes d'aquest tipus de virus (*ransomware)* es recomana que preneu les mesures següents:

- **Actualitzar el programari amb regularitat.** Els ordinadors personals haurien de tenir instal·lat programari antivirus, anti-malware i tallafocs que aïllin la xarxa interna d'internet. Aquests sistemes s'han d'actualitzar freqüentment per tal d'estar al dia de les noves amenaces.

- **Utilitzar antivirus.** Verifiqueu sempre els arxius descarregats amb el programari antivirus.

- **Realitzeu comunicacions segures.** Utilitzeu filtres de correu electrònic i navegació Web (spam, phishing,...). Vetlleu també per realitzar comunicacions segures en el comerç electrònic, configuració segura d'equips, xifrat de les comunicacions, etc.

- **Fer regularment còpies de seguretat** de les dades emmagatzemades en el vostre ordinador. En cas d'estar afectat pel virus abans esmentat normalment es poden accedir al seus arxius comuns de l'empresa des d'un altre terminal.

- **No respondre correus electrònics sospitosos** o enviats per entitats amb les quals no teniu relació en què us demanin dades personals o que afectin la seguretat, fins i tot si provenen d'un origen aparentment conegut, sense confirmar-los per telèfon o personalment.

- **Formar als usuaris** per evitar que les males praxis puguin contribuir a augmentar la inseguretat dels sistemes informàtics. Es important conscienciar sobre la prevenció envers els incidents de seguretat.

- **No entrar en enllaços sense conèixer el seu veritable origen**. El que sembla un anunci inofensiu en realitat ens pot redirigir a la pàgina web des d'on el programari maliciós es descarrega.

- **Desconfiar dels missatges de programari obsolet.** Fent una recerca a la xarxa amb el proveïdor oficial es pot saber si el programari està realment desactualitzat i quines són les instruccions per a actualitzar-lo.

- **No instal·lar o executar programari que no és de confiança o desconegut.** Instal·lar aplicacions en l'ordinador quan no sabem d'on provenen, pot afavorir l'aparició de programes pirates que intentaran robar dades personals.

- **Consultar amb el vostre proveïdor TIC sobre quin antivirus pot desbloquejar l'ordinador.** Existeixen nombrosos llocs web oficials i blocs amb instruccions sobre com eliminar de forma segura aquest tipus de virus del vostre equip.

Es important fer una bona anàlisi prèvia de les necessitats de seguretat a l'empresa i implentamentar les que més ens convinguin. Apostar per la seguretat preventiva sempre és una bona inversió.

Recordar que cap agència de seguretat pública demana el pagament d'una sanció en aquestes condicions. Per tant es tracta d'una estafa i el pagament de la quantitat exigida no soluciona la problemàtica generada.

En cas de ser víctima, cal presentar denúncia a qualsevol dependència de la Policia de la Generalitat - Mossos d'Esquadra, aportant el màxim de dades de les que es disposi. Aquesta informació arribarà a la Unitat Central de Delictes Informàtics per a la posterior investigació i esclariment dels fets.

Per a més informació, podeu consultar el web del Centre de Seguretat de la Informació de Catalunya (CESICAT) www.cesicat.cat