Nota de l'Agència de Ciberseguretat de Catalunya en relació a l'ús d'aplicacions de videoconferència

10 d'abril de 2020

En l'actual estat de confinament s'està fent un **ús intensiu de diferents plataformes de videoconferència per finalitats personals i professionals**.

En aquest sentit, en les ultimes setmanes s'han publicat algunes noticies sobre suposats problemes de seguretat d'algunes d'aquestes eines de videoconferència, com és el cas de Zoom o Jitsi.

Pel que fa a **Zoom**, el propi fabricant va publicar el passat 2 d'abril una nova actualització per als sistemes operatius Microsoft Windows on es resolien les vulnerabilitats de seguretat que permetrien obtenir les claus d'accés de l'usuari d'aquest sistema.

Pel que fa les informacions aparegudes sobre **Jitsi**, a l'Agència de Ciberseguretat no li consten vulnerabilitats recents. La darrera de la qual se'n té constància és de fa 3 anys i ja va quedar resolta.

És per això que des de l'Agència de Ciberseguretat de Catalunya es recomana actualitzar les aplicacions i el programari que utilitzem, tant a nivell personal com professional, cada cop que els fabricants publiquen una nova versió per evitar així ser exposats a riscos de ciberseguretat.

D'altra banda, insistir també en el fet que actualment existeixen diferents solucions i fabricants que disposen **de mesures i nivells de seguretat diferents**. Per això, és important determinar quin és el nivell de seguretat que requerim per a cada ús, ja sigui professional o particular per tal de poder destriar la plataforma de videoconferencia amb **els estàndards de seguretat més adequats per a la seva finalitat** (fer una reunió familiar o amb els amics, reunions de treball, visites mèdiques no presencials, etc.).

En resum, en relació amb les eines de videoconferència **recomanem que**:

- Es mantingui la **versió del programari actualitzada i** que es **configurin els elements de seguretat** segons les indicacions del mateix fabricant, que es poden obtenir a través dels enllaços oficials del seu llocs web (veure nota peu de pàgina[1]).
- Es descarreguin sempre de **Markets oficials o d'enllaços provinents de les pàgines oficials** (actualment hi ha força campanyes de Phishing per suplantar aquest tipus d'eines).

[1] ZOOM: https://zoom.us/docs/en-us/privacy-and-security.html.
JITSI: https://jitsi.org/

Salvador Espriu, 45-51
08908 L'Hospitalet de Llobregat
Tel. 93 557 42 40

- Verificar i valorar els usos que volem fer de cada aplicació (ja siguin lúdics, professionals, o d'altres) i els **estàndards de seguretat de les solucions** segons la rellevància de la informació que vulguem transmetre.
- Analitzar i verificar les **condicions de privacitat** de les solucions, ja que en molts casos la seva gratuïtat es justifica pel tractament de les dades personals de l'usuari.
- **Evitar difondre informacions falses** sobre possibles riscos de seguretat que no provinguin de fonts fiables i/o oficials.

L'Agència de Ciberseguretat de Catalunya és l'entitat encarregada d'executar el servei públic de ciberseguretat i treballa per augmentar el nivell de seguretat de les xarxes i els sistemes d'informació a Catalunya, així com fomentar la **confiança digital** dels ciutadans.

Per a més informació podeu consultar les recomanacions als webs de l'Agència de Ciberseguretat de Catalunya (www.ciberseguretat.cat o www.internetsegura.cat) o als canals oficials de la Generalitat de Catalunya.