Securizarea Conferințelor video

- Riscuri de securitate
- Bune practici

OCTOMBRIE 2020

Introducere

În contextul pandemiei actuale COVID-19 mai multe organizații din sectorul public, privat și mediul academic au fost nevoite să-și reevalueze formatul de activitate și modul de comunicare, implementând operarea de la distanță prin intermediul platformelor pentru conferințele video (de exemplu: Zoom, Microsoft Teams, Cisco Webex). În această conjunctură este foarte importantă evaluarea corectă a riscurilor de securitate asociate utilizării acestor platforme și respectiv, este necesar să fie respectate, nemijlocit, anumite cerințe pentru asigurarea securității cibernetice în timpul conferințelor video.

Prezentul document conține informații cu privire la cele mai frecvente riscuri de securitate cibernetică ce vizează platformele pentru conferințele video și un set de bune practici pentru securizarea conferințelor video.

Riscuri de securitate frecvente ce vizează platformele pentru conferințele video

- **Atacuri de tip Distributed Denial of Service (DDoS)** - atacurile respective suprasolicită serviciul, astfel pot provoca perturbarea sau blocarea acestuia. Conferințele video respective pot fi întrerupte sau chiar blocate.

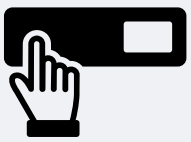
- **Phishing și Domain Spoofing** - persoanele rău intenționate adesea creează unele replici ale site-urilor oficiale pentru descărcarea software-ului pentru conferințe video prin falsificarea numelui de domeniu a site-ului, cu intenția de a induce în eroare utilizatorii să acceseze pagini de phishing. Acestea urmăresc colectarea informațiilor confidențiale, cum ar fi numere de carduri sau conturi PIN, parole și utilizarea acestora pentru a sustrage bani.

- **Atașamente/link-uri malițioase în chat -** odată ce persoanele rău-intenționate/terțe au acces la conferința dvs., acestea pot distribui atașamente sau link-uri malițioase pentru a înșela participanții la confeință să le acceseze.

- **Compromiterea link-urilor conferințelor** - reutilizarea link-urilor conferințelor video facilitează accesul neautorizat din partea persoanelor rău-intenționate.

- **Dezvăluiri de informații** - în cazul în care participanții la conferința video partajează informații sensibile în cadrul acestora, însă nu cunosc dacă sesiunea este înregistrată din exterior sau are participanți terți, utilizatorii respectivi se expun riscului înalt de divulgare a informațiilor sensibile.

BUNE PRACTICI
pentru securizarea conferințelor video



- **Activați funcția "Waiting Room" (Camera de așteptare**)- setarea unei săli de așteptare virtuală pentru participanții la conferința video oferă mai mult control și posibilitate gazdei de a admite doar participanții invitați la conferință, astfel persoanle nedorite nu vor avea acces la conferință.

- **Implementați o politică puternică de parole** - securizați-vă contul folosind o parolă puternică și unică, sau utilizați Generatorul de parole pentru a crea parole securizate ce sunt dificil de spart. În cazul în care utilizați mai multe aplicații pentru conferințele video, utilizați parole unice pentru fiecare cont formate din minim 8 caractere ce includ atât litere majuscule, cât și minuscule, cifre și caractere speciale. De asemenea, dacă este posibil activați autentificarea cu 2 pași (2FA).

- **Solicitați o parolă nouă pentru fiecare conferință video** - prin intermediul acesta participanții vor fi nevoiți să introducă parola pentru a se alătura la conferință, iar în acest mod, chiar dacă link-ul conferinței este identificat de către alte persoane terțe acestea nu se vor putea alătura conferinței fără parolă.

- **Generați un ID unic pentru fiecare conferință video** - în acest mod ID-ul îl vor cunoaște doar persoanele invitate la conferință, de asemenea evitați să-l faceți public pentru alte peroane terțe.

- **Nu distribuiți link-ul, ID-ul sau parola conferinței prin intermediul rețelelor de socializare sau a formurilor publice** - oricne deține aceste informații poate participa la confeințele video fără permisiune.

- **Activați funcția "Automatic Update" (Actualizare automată)** - astfel vă asigurați că aplicația pentru conferințele video este actualizată în mod continuu.

- **Dacă este posibil încercați să nu împărtășiți date sensibile în timpul conferințelor video** - chiar dacă alegeți să nu înregistrați conferința, fiți conștienți că oricine din participanți poate utiliza instrumente externe de înregistrare a conferinței, fără ca să cunoașteți despre acest lucru.

ATENȚIE!

Dacă utilizați software pentru conferințele video independent descărcați-l doar din surse oficiale și de încredere (de exemplu: Apple App Store, Google Play) sau de pe site-ul oficial al furnizorului de servicii.

I.P. Serviciul Tehnologia Informației și Securitate Cibernetică
MD-2012, or. Chișinău, Republica Moldova
Piața Marii Adunări Naționale 1

www.stisc.gov.md

(022)820 911

stisc@stisc.gov.md
info@cert.gov.md