

12 באוקטובר 2023
כ"ז בתשרי תשפ"ד
סימוכין: ב-ס-1632

אבטחת מערכות למידה/עבודה מרחוק

תקציר

1. מערכות שת"פ (Collaboration) כגון Zoom, Teams, Webex, Skype, Google Meet וכד', משמשות בזמן לחימה כאמצעי ללמידה מרחוק, ולשיתוף פעולה וקיום פגישות בין עובדים המנועים מלהגיע פיזית למשרדים.
2. להלן הנחיות לשיפור אבטחת מערכות אלו.

פרטים

1. בשימוש בכלים אלו מספר סיכונים עיקריים:
 1. העברת קישורים זדוניים או צרופות במטרה להדביק בפוגען את עמדות/ציוד המשתתפים.
 2. גניבת נתוני הזדהות.
 3. התפרצות של גורמים לא מורשים לפגישה.
 4. דלף מידע המועבר בפגישה.
 5. מתקפת מניעת שירות המונעת קיום הפגישה.

דרכי התמודדות

ההנחיות הן כלליות לסוג תוכנה/שירות זה. יש לבחון ולהפעיל את ההגדרות הרלוונטיות על פי תיעוד היצרן למערכת שבשימושכם.

1. על מנת למנוע מגורמים זרים להתפרץ ולהפריע לשיחות, או למנוע את עצם קיום הפגישה, מומלץ לנקוט בצעדים הבאים:
 1. לפרסם את קיום הפגישה באמצעים פנים ארגוניים ולא פומביים.
 2. להגדיר סיסמה ארוכה, מורכבת וקשה לניחוש לפגישה.

ניתן לשתף מידע המסווג **TLP:CLEAR** עם כל קבוצת נמענים, לרבות ערוצים פומביים

3. אם התוכנה תומכת וניתן להתנות גישה לפגישה בשימוש בהזדהות חזקה, מומלץ להפעיל אפשרות זו.
 4. להגדיר שמצטרפים לפגישה ימתינו בחדר הכניסה (Waiting Room) עד שיוכנסו אליה על ידי מנהל הפגישה לאחר שאימת את זהותם.
 5. אם אפשרי, לנעול את הפגישה (Lock Meeting) לאחר שכל המשתתפים הצטרפו, כך שלא ניתן לצרף משתמשים חדשים.
 6. וודאו כי מנהל הפגישה יודע כיצד באפשרותו להוציא משתמשים מתוך הפגישה במקרה הצורך.
 7. הגדירו כי משתמשים שהוצאו באופן יזום מהפגישה לא יוכלו להצטרף מחדש.
 8. הגדירו כי מנהל הפגישה יכול למנוע שיתוף מסך על ידי המשתתפים (Disable desktop screen sharing for meetings you host).
 9. בתום הפגישה, מנהל השיחה יודא כי השיחה נעולה וכל המשתמשים התנתקו.
2. על מנת למנוע מנתוני הזדהות לדלוף, או הדבקה של עמדת המשתמש באמצעות קישור או צרופה, מומלץ לנקוט בצעדים הבאים:
1. יש להימנע מלהפעיל קישורים/צרופות המועלים על ידי משתתפים לפגישה. יש לבדוק טרם הפתיחה בדרכים התואמות את מדיניות הארגון.
 2. הגבילו את סוגי הקבצים/צרופות שניתן לשתף למינימום הנדרש. אם הדבר אפשרי נטרלו אפשרות העברת ושיתוף קבצים לחלוטין.
 3. יש להימנע מלהפעיל קישורים לשרתי SMB, מאחר וכברירת מחדל, מערכת ההפעלה משדרת עם הפעלת קישור כזה את נתוני ההזדהות של המשתמש, והם עלולים להיתפס על ידי התוקף. כאמצעי הגנה נוסף ניתן לחסום פורט 445 ב-Firewall לתעבורה יוצאת.
 4. על מנת לשמור על פרטיות המשתתפים בפגישה, מומלץ לוודא שהאפשרות לביצוע Attention Tracking מנוטרלת.
3. על מנת להימנע מדלף מידע המועבר בשיחות, מומלץ לנקוט בצעדים הבאים:
1. לוודא כי השיחה מוגדרת כמוצפנת מקצה לקצה (End to End Encryption) בהגדרות התוכנה.

ניתן לשתף מידע המסווג TLP:CLEAR עם כל קבוצת נמענים, לרבות ערוצים פומביים

2. להימנע מהקלטת השיחה, אלא אם היא חייבת להיות מוקלטת מסיבות עסקיות או ארגוניות. אם הפגישה מוקלטת, יש לוודא כי ההקלטה מתבצעת על ידי מנהל הפגישה בלבד, לוודא כי המשתתפים מודעים להקלטה, ולהחליט מראש על אופן האחסון המאובטח של ההקלטה.
3. מלכתחילה להגביל סיווג השיחה כך שגם אם ידלוף מידע, הוא לא יהיה מסווג.
4. וודאו כי הרקע מאחורי המשתמשים, או שולחן העבודה, אינם חושפים מידע רגיש.
4. מומלץ להתקין התוכנות השונות המשמשות לגישה לפגישות אך ורק מחנויות היישומים הרשמיות (AppStore, Google Play), או מהאתר הרשמי של היצרן. וודאו באופן עיתי כי ברשותכם גרסת התוכנה העדכנית ביותר הכוללת את כל עדכוני האבטחה שפרסם היצרן.

מקורות

1. <https://www.gov.il/he/departments/news/safezoom>
2. <https://www.gov.il/he/departments/publications/reports/videoplatform>
3. <https://explore.zoom.us/en/trust/security/>
4. <https://explore.zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf>
5. <https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings>
6. <https://help.webex.com/en-us/article/sf4sh1/Webex-App-%7C-Security-Best-Practices>
7. <https://help.webex.com/en-us/article/8zi8tq/Best-practices-for-secure-meetings:-hosts>
8. <https://help.webex.com/en-us/article/nwh2wlx/Enable-End-to-End-Encryption-Using-End-to-End-Encryption-Session-Types>
9. <https://learn.microsoft.com/en-us/microsoftteams/teams-security-guide>
10. <https://www.lepide.com/blog/microsoft-teams-security-tips-and-best-practices/>
11. <https://learn.microsoft.com/en-us/microsoftteams/teams-security-best-practices-for-safer-messaging>
12. <https://gatlabs.com/blogpost/make-google-meet-meetings-more-secure/>

ניתן לשתף מידע המסווג TLP:CLEAR עם כל קבוצת נמענים, לרבות ערוצים פומביים

13. <https://support.google.com/meet/answer/9852160?hl=en>
14. <https://support.google.com/a/answer/7582940?hl=en>
15. <https://blog.google/outreach-initiatives/education/connect-confidently-google-meet-security-features/>
16. <https://support.skype.com/en/faq/FA34649/protecting-your-online-safety-security-and-privacy>
17. <https://learn.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/security/best-practices>

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.



ניתן לשתף מידע המסווג TLP:CLEAR עם כל קבוצת נמענים, לרבות ערוצים פומביים