אבטחת מערכות VPN/למידה/עבודה מרחוק

15/06/2025
י"ט סיון תשפ"ה

[תקציר]

- לאור הלחימה מול איראן, אנו מפרסמים שוב הנחיות לשיפור אבטחת מערכות VPN, למידה או עבודה מרחוק.
- מערכות שת"פ (Collaboration) כגון Zoom, Teams, Webex, Google Meet וכד', משמשות בזמן לחימה כאמצעי ללמידה מרחוק, ולשיתוף פעולה וקיום פגישות בין עובדים המנועים מלהגיע פיזית למשרדים.
- מערכות מסוג VPN משמשות ארגונים רבים לגישה מרחוק לרשת הארגונית.
- להלן הנחיות לשיפור אבטחת מערכות אלו.

פעולות מידיות לביצוע:

- שינוי סיסמאות ברירת מחדל.
- וידוא שימוש בגרסה העדכנית ביותר ועדכון עיתי של התוכנה.
- שימוש בהזדהות חזקה (MFA) עבור כל המשתמשים במערכות גישה מרחוק, ובפרט המנהלנים.
- מערכות VPN – הקפדה על מניעת גישה מרשת האינטרנט לממשקי הניהול.

[פרטים]

- בשימוש בכלים לשיתוף ופגישות מרחוק מספר סיכונים עיקריים:
  - העברת קישורים זדוניים או צרופות במטרה להדביק בפוגען את עמדות/ציוד המשתתפים.
  - גניבת נתוני הזדהות.
  - התפרצות של גורמים לא מורשים לפגישה.
  - דלף מידע המועבר בפגישה.
  - מתקפת מניעת שירות המונעת קיום הפגישה.

⚠

שיתוף מידע עם מערך הסייבר 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.

[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. אם משתתפי הפגישה כוללת קבוצה מוגדרת מראש (לדוגמה, תלמידים בביתה או ישיבה שמשתתפיה כולם מוכרים), מומלץ לפתוח קבוצה ולהזמין רק את משתתפיה לפגישה.
   3. להגדיר סיסמה ארוכה, מורכבת וקשה לניחוש לפגישה.
   4. אם התוכנה תומכת וניתן להתנות גישה לפגישה בשימוש בהזדהות חזקה, מומלץ להפעיל אפשרות זו.
   5. להגדיר שמצטרפים לפגישה ימתינו בחדר הכניסה (Waiting Room) עד שיוכנסו אליה על ידי מנהל הפגישה לאחר שאימת את זהותם.
   6. אם אפשרי, לנעול את הפגישה (Lock Meeting) לאחר שכל המשתתפים הצטרפו, כך שלא ניתן לצרף משתמשים חדשים.
   7. וודאו כי מנהל הפגישה יודע כיצד באפשרותו להוציא משתמשים מתוך הפגישה במקרה הצורך.
   8. הגדירו כי משתמשים שהוצאו באופן יזום מהפגישה לא יוכלו להצטרף מחדש.
   9. הגדירו כי מנהל הפגישה יכול למנוע שיתוף מסך על ידי המשתתפים (Disable desktop screen sharing for meetings you host).
   10. בתום הפגישה, מנהל השיחה יוודא 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 לבודקם 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 ובברירת 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.
   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.

5. המלצות להגברת האבטחה של מערכות VPN:

1. מומלץ מאד לא להשתמש בהגדרות ברירת המחדל של הציוד, לעבור על כל הגדרה ולהיעזר במסמכי Best Practice של היצרן או גורמים מקצועיים מוכרים.
2. ניתן להיעזר בהמלצות אתרים כגון https://www.ssllabs.com/ssltest/ וכד', על מנת להגדיר את הציוד באופן הולם לדרישות אבטחה מודרניות (שימוש בגרסאות מתאימות של TLS, סוגי פרוטוקולי הצפנה סימטריים וא-סימטריים, אורכי מפתח וכו').

3. מומלץ לצמצם למינימום הנדרש את הפורטים והפרוטוקולים שהציוד חושף לרשת האינטרנט.
4. מומלץ להירשם לרשימת דיוור של היצרן על מנת לקבל התרעה על כל עדכון אבטחה רלוונטי. מומלץ לבחון ולהתקין עדכוני אבטחה סמוך ככל האפשר לפרסומם.
5. מומלץ לוודא שמשתמשים בציוד אינם משתמשים בסיסמאות ברירת מחדל לגישה אליו. מומלץ לוודא דרישה להגדרת סיסמה ארוכה וקשה לניחוש. מומלץ מאד לוודא שכל המשתמשים בציוד, ובפרט מנהלנים, מצוידים באמצעי להזדהות חזקה אל הציוד.
6. מומלץ לוודא שתקופת הרישום של משתמש חדש בציוד תהיה מוגבלת בזמן. אם המשתמש לא נרשם בזמן לציוד, והגדיר סיסמה והזדהות חזקה, מומלץ לחסום הגישה ולהנחות המשתמש לפנות לתמיכה הארגונית לצורך רישום.
7. מומלץ להגדיר את הציוד כך שגם לאחר הזדהות מוצלחת, הגישה של המשתמשים לרשת הארגונית תהיה מוגבלת לשירותים, לפרוטוקולים ולפורטים הדרושים להם לצורך ביצוע עבודתם בלבד.
8. מומלץ להפעיל את מנגנוני הלוג והרישום הקיימים בציוד, לגבותם מחוץ לציוד ולנתחם בכלים ארגוניים כגון SIEM.

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/
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://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
17. https://media.defense.gov/2021/Sep/16/2002855930/-1/-1/0/SECURING_IPSEC_VIRTUAL_PRIVATE_NETWORKS_EXECUTIVE_SUMMARY_2020_07_01_FINAL_RELEASE.PDF