סיכונים מרכזיים בעת עבודה עם פלטפורמות פגישות וידאו דיגיטליות

סיכונים מרכזיים בעת עבודה עם פלטפורמות פגישות וידאו דיגיטליות (פלטפורמות שת"פ)

כתבו: עינן ליכטרמן, יובל סיני, מרץ 2020
@

תוכן עניינים

רקע ותקציר מנהלים

פלטפורמות פגישות וידאו דיגיטליות (ידועות גם כפלטפורמות קולבורציה, Unified Communications, web conferencing meetings, Meeting Solutions - להלן במסמך זה **פלטפורמות שת"פ)** משמשות ארגונים רבים לשם ייעול הפעילות על ידי העברת פעילות מפגש בין מספר אנשים לפלטפורמה דיגיטלית, בין פעילויות אלו ניתן למנות פגישות בין מספר משתתפים, פעילויות הדרכה ואפילו כנסים מרובי משתמשים. הפלטפורמות מאפשרות שיחות קול ווידאו בין המשתתפים, שיתוף מסכים, שליחת הודעות, וכן שמירה של תכני הפגישה[1].

שימוש בפלטפורמות אלו עם היתרונות שלהן, טומן בחובו אתגרים אבטחתיים המיוחדים לו והנובעים ממספר שינויים מרכזיים:

- העברת פעולה ממרחב פיזי למרחב דיגיטלי.
- התלות הגוברת של הארגון בקיום תשתית דיגיטלית ראויה לביצוע פעולות שגרה.
- גורם שלישי (בעל הפלטפורמה) המקבל אחריות על אבטחת העברת ידע המתבצע במהלך השיחות.
- עצם הדיגיטציה ושימוש בפלטפורמה ממוחשבת לשם החיבור פותח את כלל היכולות של הפלטפורמות הדיגיטליות ובפרט את פלטפורמות השת"פ ויכולות המיוחדות לה.
- חציית סמכויות שיפוט באופן ה"שקוף" למשתמשים, כאשר כל סמכות משפטית עשויה לדרוש עמידה בדרישות אבטחה ופרטיות שונות, ולעיתים אף מתנגשות.

כפי שמתארת חוקרת אבטחת מידע:

"The main takeaway for online conference platforms is that these companies are in charge of the security of their users and they need to work to secure these environments[2]."

הסיכון הגלום בפלטפורמות אלו חל בשעת פגישה, אבל גם מעצם העובדה כי הפלטפורמות מותקנות בציוד הארגון ומאפשרות גישה למידע בסביבת העבודה של המשתמש (מידע טכני, ומידע אנושי), ובכך הפלטפורמות עצמן מהוות כלי רגיש. בנוסף, חלק מן הפלטפורמות מאפשרות אינטגרציה עם

[1] סקירת חברת גרטנר על השחקנים בשוק - https://www.uctoday.com/collaboration/gartner-magic-quadrant-meeting-solutions-2018/

[2] https://threatpost.com/video-zoom-web-conference-security-risks/152337/

מערכות נוספות הנמצאות בארגון או מחוצה לו וכך בפועל יורשות אתגרי אבטחה מרובי פלטפורמות.
ההבדל בין שימוש בפלטפורמות אלו לבין שיחת טלפון רגילה מבוססת נתונים (או אפילו משולבת וידאו) הינו המושג 'פגישה', כלומר, תהליך מתוכנן של התכנסות לחלל (וירטואלי) אחד לשם דיון בתוכן מוגדר.

המסמך ממוקד בניתוח אבטחתי של קיום פגישות עבודה בארגונים מסחריים או ציבוריים, תוך שימוש בפלטפורמות. אין ספק כי הניתוח האבטחתי לשימושים אחרים של הפלטפורמה (כגון הרצאות) דומה, אך יתכנו שינויים מסוימים.

מטרת המסמך

להציג מודל סיכונים מול השימוש במערכות אלו על מנת לאפשר למקבל ההחלטות לבצע ניהול סיכונים מושכל בהטמעה ושימוש במערכות אלו.

מבנה המסמך

- פרק הגדרות - מניח את היסוד למונחים המשמשים במהלך המסמך.
- פרקים המנתחים סיכונים שונים בשימוש בפלטפורמות, עבור כל פרק מופיעים מספר סיכונים הקשורים לפרק וכן את סוגי היריבים הרלוונטים לאיום זה.
- פרק המלצות.

תיחום

- המסמך בוחן את פלטפורמות השת"פ כולן - ללא התמקדות בתוכנה זו או אחרת.
- המסמך בוחן את העקרונות הטמונים בבסיס פלטפורמות אלו ולא פערים טכנולוגיים הנובעים מפיתוח שאינו נכון או מושלם של תוכנות אלו.
- המסמך בוחן את השימוש בתוכנות עצמן ולא ככלי להפצת פישינג או להתקנת תוכנות זדוניות (על ידי הפצת קישורים או זימונים שאינם נכונים).

קהל יעד

- מנהלי מערכות מחשוב וגורמי הגנה ארגוניים.

הערה: המסמך נכתב על סמך מקורות גלויים, ללא התקנה בפועל של התוכנות וללא ביצוע של מבדקי חדירות מול מערכות אלו.

נכסים מרכזיים להגנה

פרק זה סוקר את הנכסים המשמעותיים הקיימים בשימוש פלטפורמות השת"פ.

- עצם קיום פעילות השת"פ - שימור עצם היכולות לבצע פעולות שת"פ בהיקף הנדרש תוך שימוש בתקשורת ובהסכמים שחתמה החברה.
- מידע על (מטה-דאטה) - מערכות אלו כוללות מידע רב המשמש כעוטף לשיחות כגון רשימת משתתפים, פרטיהם ועוד.
- תוכן - תוכן של פגישה או חומרים ששותפו במהלך השיחה (קבצים, צ'ט).
- מידע צד - מידע מוצג במהלך הפגישה אך אינו חלק מהפגישה, כגון מהי מערכת ההפעלה, אילו תוכנות מותקנות על המחשב, ועוד.
- שימוש כערוץ לתקיפות נוספות - לנוכח העובדה כי מדובר בערוץ מוצפן המאפשר העברת תכנים (קול, תמונה) ובמקרים רבים אף קבצים, הרי שניתן להשתמש בפלטפורמות ככלי למימוש תקיפה קלאסית.
- ערוץ הזלגה ופיקוד - מכיוון שאפליקציות אלו הופכות להיות לגיטימיות במרחב העבודה ובמרחב התקשורתי, תוקף יכול להשתמש בתוכנות אלו ככלי הזלגה או פיקוד בין "מחשב האם" לבין יחידות הקצה.

סוגי יריבים מרכזיים

הבנת סוגי היריבים חיונית להשוואה בין היכולות והמטרות של היריב כחלק מתהליך ניהול הסיכונים בשימוש במערכות אלו.

- תוקף חיצוני לתהליך - יריב זה ממוקם מחוץ לתהליך התקשורת עצמו ולא מעוניין להשיג מידע על התהליך או על עצם קיומו. תוקף זה יפעל להשבית את הפעילות עצמה או לגנוב כסף (על ידי מיצוי כספי גבוה) ממשתמשים לגיטימיים.
- תוקף מבחוץ - יריב זה הינו גורם הנמצא בשגרה מחוץ למעגל ספקי / מקבלי השירות מהמערכת, אך מבקש להשיג את יעדיו, כאשר פלטפורמת השת"פ משמשת עבורו תשתית להשגת יעדיו. יתכן כי תוקף זה יתמקד בתקיפת ספק השירות (על מנת להשיג פגיעה בספק השירות או על מנת להשיג נגישות רוחבית לכל המשתמשים בשירות), או שיבחר לתקוף ישירות את הארגון.
- בעלי הפלטפורמה - ספק המאפשר שימוש בפלטפורמה במודלים כלכליים שונים. בפועל, בידי בעל הפלטפורמה קיים מידע הנוגע למשתמשים ולשיחות. יריב זה נגיש באופן מובנה לפלטפורמה. מעבר לשימושים קלאסיים שניתן לבצע במידע, היריב יכול להשתמש במידע לצורך שיווק (עצמאית או על ידי העברתו לגורם נוסף).

- ארגון מקביל המשתמש בשירות - משתמש לגיטימי נוסף בשירות יכול לשמש גורם תוקף ולהיות חשוף למידע. תוקף זה יכול להיות מאותה חברה כמו משתתפי השיחה המקורית או לקוח מקביל של הפלטפורמה.
- חבר בארגון אך לא שותף בפגישה - תוקף זה הוא עובד בארגון הנתקף, אך אינו שותף בקיום כלל הישיבות. תוקף זה יכול להיות חשוף למידע ארגוני שאינו אמור להיות חשוף אליו.
- שותף בפגישות אך לא חבר בארגון - תוקף זה הוא גורם החיצוני לארגון אך זומן להשתתף בפגישה מסוימת ויוכל לנצל נגישות חד פעמית זו להשגת מידע רב (תוכן הפגישה אליה זומן אינו מוגדר כמידע שהושג בתקיפה, אך תיכן ומידע על המשתתפים יוגדר כך, וכן מידע על פעילויות אחרות של הארגון במסגרת הפלטפורמה).
- **במהלך הפגישה**
  - תקיפה על ידי משתמש בפגישה - משתתף בפגישה יכול להוות תוקף, המשתתף יכול להיות מהחברה היוזמת, משתתף לגיטימי בישיבה או משתתף סמוי.
  - תקיפה על ידי מוביל פגישה - משתתף מיוחד בפגישה הוא מוביל הפגישה שלזכותו עומדות לרוב הרשאות רבות יותר ולכן הוא מהווה שחקן תוקף נוסף. במרבית המקרים, גורם זה הוא גם מארגן הפגישה אך יתכן שסמכות המוביל הועברה לו מהמארגן.

חשיפת מטה-דאטה (מידע-על)

מטה-דאטה (להלן במסמך מידע-על) הוא מידע מעבר לתוכן עצמו. עבור פלטפורמות שת"פ, התוכן עצמו מוגדר כתוכן המועבר בפגישה, סוגי מידע העל הניתנים למיצוי מתוך עולם התוכן הם:

- מידע על הפגישה עצמה - כגון נושאי הפגישה, מועד, משך, צורת החיבור, האם שותפו קבצים ומצגות ועוד.
- משתתפים (פנימיים וחיצונים) - לעיתים עצם שמות המשתתפים בפגישה יכול להוות מידע בעל ערך ליריב, כגון גיוס של עובדים לחברה או אוסף הספקים והלקוחות. במקרים רבים, גורמים אלו ישתתפו בפגישות וידרשו להזין פרטי זיהוי כחלק מהשתתפותם.
- נתונים אישיים - לשם כניסה, המשתתף מספק (כחובה או רשות) מספר פרטים אישים כגון: שם (כינוי), כתובת דואר אלקטרוני וטלפון.
- נתונים טכנולוגיים - כחלק מתהליך ההתחברות ושימוש בפגישה נחשפים נתונים טכנולוגים על פלטפורמת החיבור כגון: כתובת IP, מיקום, סוג פלטפורמה דיגיטלית, מערכת הפעלה ועוד.
- רשימת אנשי קשר - ארגון הנרשם לשירות מתבקש לייצא את רשימת העובדים לפלטפורמה לטובת מתן הרשאות או פתיחת ספר טלפונים קבוצתי, ובכך חושף את המידע על כלל העובדים לתוקף פוטנציאלי.
- מידע מתכלל - הבנת משכי הפגישות ותדירותן, תוך תכלול המידע לאורך זמן, עלול להביא להבנה על תהליכים ושינויים בארגון, כגון:
  - שינויים במבנה הארגון (יאופיין בריבוי פגישות תכופות דרגים בכירים לעיתים בשילוב ייעוץ ארגוני).
  - עזיבת גורם את הארגון (יאופיין בירידת מספר הפגישות ובאינטנסיביות שלהן על ידי גורם זה).

תוקפים רלוונטים לסוג איום זה							
במהלך פגישה							
תוקף חיצוני לתהליך	תוקף מבחוץ	בעלי הפלטפורמה	ארגון מקביל המשתמש בשירות	חבר בארגון אך לא שותף בפגישה	שותף בפגישות אך לא חבר בארגון	תקיפה על ידי משתתף בפגישה	תקיפה על ידי מוביל פגישה
X	V	V	X	V	X	V	V

הזדהות והשתתפות בפגישות

פלטפורמות השת"פ מאפשרת קיום של פגישות בין גורמים שונים על סמך הזדהות דיגיטלית (להבדיל מהזדהות פיזית בפגישות "קלאסיות"). מרכיב ההזדהות מהווה את יחידת היסוד בשימוש בפלטפורמות אלו, ושיבוש של רכיב זה מהווה תקיפת יסוד של השימוש בפלטפורמה. את המושג הזדהות בהקשר השימוש בפלטפורמות ניתן לחלק לשני חלקים:

- הזדהות המשתמש כחלק מהארגון.
- השם המוצג של המשתמש בפלטפורמה (נבחר על ידי המשתמש).

ניתן לזהות מספר מרכיבי איום הנובעים מעולם תוכן זה:

- אמצעי הזדהות ופגיעויות מוכרות בהם - מרבית הפלטפורמות פועלות על פי הזמנה, או חיבור לאפליקציות נוספות לשם זיהוי המשתמש, כך שבפועל, זיהוי המשתמש הוא זיהוי חלש, לא מתבצע אימות של המשתתפים מעבר למוצהר על ידם.
- נתונים המוצגים בתוכנה אינם מאומתים - שמות המשתמשים שהתוכנה מציגה אינם מאומתים ונובעים ישירות ממידע שהמשתמש הזין ולכן נתונים אלו הם בעלי רמת אמינות נמוכה.
- השתתפות סמויה - המשתתפים בפגישה מנוהלים על ידי הפלטפורמה ולכן יתכן כי קיימים משתתפים שאינם מוצגים בפלטפורמה אך בפועל משתתפים בפגישה.
- זיהוי ישיבה מעבר להגדרת חדר - התחברות לפגישה מתאפשרת לאחר הזנת מספר החדר (קוד גישה). בפועל, יתכן ומשתמשים יתחברו לחדרים בהם לא אמורים להיות בצורה רנדומלית או מכוונת.
- כניסה לישיבה ללא הזמנה - המנגנון אינו חוסם כניסה לפגישה ללא הזמנה, ובכך, בפועל יתכן ובפגישה ישתתפו גורמים נוספים מעבר לאלו שהוזמנו.
- אוטונומיית המשתתף - בחלק מן המקרים משתתפים בפגישה יכולים להוסיף באופן עצמאי מוזמנים נוספים לפגישה, וזאת ללא אישורו/ידיעתו של מוביל הפגישה.

תוקפים רלוונטיים לסוג איום זה							
במהלך פגישה							
תקיפה על ידי מוביל פגישה	תקיפה על ידי משתתף בפגישה	שותף בפגישות אך לא חבר בארגון	חבר בארגון אך לא שותף בפגישה	ארגון מקביל המשתמש בשירות	בעלי הפלטפורמה	תוקף מבחוץ	תוקף חיצוני לתהליך
X	X	V	V	V	X	V	X

הרשאות

הפלטפורמות השונות יוצרות מדרג של תפקידים בניהול הפלטפורמה מצד הארגון, ובניהול הפגישות עצמן. תפקידים של הרשאות אלו הוא להתיר או להגביל פעולות הניתנות לביצוע על ידי שחקנים שונים במערכות. פגיעה במערכות הרשאות אלו עלולה להביא לכדי ביצוע פעולות על ידי בלתי מורשים ובכך לפגוע בשירות בדרכים הבאות:

- קיום חלוקת תפקידים בפלטפורמה - קיימת חשיבות בעצם קיום של חלוקת הרשאות ותפקידים שונים במערכת, בין תפקידים אלו ניתן למנות:
  - מנהל (ADMIN) הפלטפורמה מצד הלקוח - נציג הלקוח בניהול הפלטפורמה, אחראי על חשבון הלקוח (מרכיב כספי), אחראי להגדרת משתמשים ומתן הרשאות שונות.
  - מוביל שיחה - גורם המוביל פגישה (לרוב המארגן), יכול לשלוט על פעילות המשתתפים בשיחה (החל ממצב אמצעי הקלט ועד לשיתוף, נידוי אנשים מהשיחה).
  - משתתף בפגישה (חבר בארגון האם).
  - משתתף בפגישה (חיצוני לארגון האם).
- הרשאות בעל הפלטפורמה - לבעל הפלטפורמה קיימות הרשאות שהן מעל להרשאות של ארגונים ובכך הוא הגורם החזק במערכת.
- "חטיפת" ניהול פגישה - למנהל הפגישה קיימות הרשאות עודפות על המשתתפים האחרים (ניהול משתתפים, הצגת חומרים ועוד), חטיפת הרשאה זו מהווה סיכון.
- שינוי הקשר בין המשתמש לפגישה - קביעה כי המשתמש:
  - לא יכול להשתתף בפגישה מסוימת.
  - הוצאה מפגישה לאחר שהחלה.
  - נידוי משימוש בפלטפורמה.
  - לא יכול לעזוב את הפגישה (ללא כיבוי פיזי של המחשב).
- הרשאות לשמירת תוכן הפגישה - הפלטפורמות מאפשרת הקלטה של שיחה ושמירה של התוכן המועבר בשיחה (הקלטות ומידע נוסף) בפלטפורמה, הרשאה זו כוללת את:
  - שמירת נתוני הפגישה (בצורה גורפת של כלל הפגישות או פגישה פרטנית).
  - מתן גישה לצדדים שלישיים (שאינם שותפים בפגישה) לנתוני הפגישה לאורך זמן.
  - הרשאות מחיקה של פגישות.

תוקפים רלוונטיים לסוג איום זה							
במהלך פגישה							
תוקף חיצוני לתהליך	תוקף מבחוץ	בעלי הפלטפורמה	ארגון מקביל המשתמש בשירות	חבר בארגון אך לא שותף בפגישה	שותף בפגישות אך לא חבר ארגון	תקיפה על ידי משתתף בפגישה	תקיפה על ידי מוביל פגישה
X	X	V	X	V	V	V	V

בפגישות מועבר תוכן בצורה ישירה או בצורה עקיפה ("מידע צד"), שלעתים יכול להיות רגיש. בנוסף, הפלטפורמות המותקנות במחשב יכולות להוות ערוץ הזלגת מידע גם בשעה שהפלטפורמות אינן פעילות. בין סוגי התוכן המועברים ניתן למנות:

- דיונים של המשתתפים במהלך הפגישה - (קול/ווידאו) של הדיון עצמו.
- חומרים המוצגים במהלך הפגישה - במהלך הפגישה הפלטפורמות מאפשרות הצגת חומרים בצורות שונות:
  - שיתוף קבצים (מצגות וקבצים נוספים).
  - שיתוף שולחן עבודה.
- תכני צ'אט כתוב שנוהל במהלך הפגישה - יתכן כי הצ'אט יתנהל בין כלל המשתתפים או חלקם.
- נגישות לתכנים שמורים של שיחות עבר - לנוכח העובדה כי הפלטפורמות מאפשרות שמירת המידע, הרי שנגישות לפגישות עבר, או לכל חלק שלהם (הפגישה עצמה, קבצים שהועברו, צ'אטים), מהווים מידע רגיש.
- "מידע צד" - מבנה שולחן עבודה, אפליקציות נוספות פועלות ברקע משותף - בפגישה בה משותף או מוצג מסך המשתתף, תוקף יכול לדלות מידע על שולחן העבודה. במקרים מסוימים ניתן גם לקבל מידע על ציוד החיבור ועוד.
- הקלטת תכנים על ידי אפליקציה חיצונית - אם בפגישה מועברים תכנים רגישים, ניתן להשתמש בפלטפורמה הדיגיטלית ולהפעיל תוכנת הקלטה (הפועלת מחוץ לפלטפורמת הקישור) ובכך לפגוע בפרטיות תוכן הפגישה.
- מידע על המשתמש במהלך פגישה - הפלטפורמה יכולה לעקוב במידה מסויימת על פעילות המשתמש במהלך הפגישה (האם חלון הפגישה פעיל וכדומה).
- מידע מסביבת העבודה של המשתמש שלא בזמן פגישה - לפלטפורמות עומדות יכולות והרשאות משמעותיות, ולכן הן יכולות לשמש כלי תקיפה עצמאי המעביר מידע גם שלא בזמן פגישה.

תוקפים רלוונטים לסוג איום זה							
במהלך פגישה							
תוקף חיצוני לתהליך	תוקף מבחוץ	בעלי הפלטפורמה	ארגון מקביל המשתמש בשירות	חבר בארגון אך לא שותף בפגישה	שותף בפגישות אך לא חבר בארגון	תקיפה על ידי משתתף בפגישה	תקיפה על ידי מוביל פגישה
X	X	V	X	V	V	V	V

שימוש בפגישה או בפלטפורמה כבסיס לתקיפה

מעבר לתקיפה של הפגישה עצמה (בתוכן או כמידע-על), קיום הפלטפורמות והשימוש בהן מהווה אפשרות לתוקף לביצוע תקיפות המשתמשות בפלטפורמה ככלי. להלן חלק מתקיפות אלו:

- מניעת שירות (DoS) - תקיפה מסוג זה יכולה להביא לכדי מניעת שירות של הגורמים הבאים:
  - הפגישה עצמה - על ידי הרעשה מכוונת של התוכן, השמעת רעש לבן או כל אמצעי אחר המונע אפקטיבית את מימוש הפגישה.
  - שימוש בפלטפורמה - על ידי תקיפת החיבור של הארגון לפלטפורמה, מספר המשתמשים המורשים, מספר המחוברים לפגישה, איכות החיבור, או כל רכיב אחר (טכני או ניהול-הרשאתי), ובכך למנוע בפועל קיום של פגישות נוספות בפלטפורמות אלו.
  - השבתה של נקודת קצה / חיבור רישתי (פנימי או חיצוני) - פלטפורמת אלו מטיבן, דורשות משאבי מחשוב מרובים (רוחב פס, משאבי ביצוע וזיכרון) וזאת לאור הצורך להעביר וידאו באיכות טובה לאורך זמן לכמות גדולה של משתתפים, הנעת פגישות מרובות או טכניקות שונות יכולות להביא לידי השבתת הקישור הרשתי של הארגון (פנימי /חיצוני) או של תחנת קצה פרטנית.
- ניצול הפלטפורמה כערוץ סמוי (COVERT CHANNEL) - הפלטפורמה משמשת כערוץ תקשורת מוצפן בין משתמשים דרך נקודה מרכזית ומעבירה כמות גדולה של נתונים, תוקף יכול להשתמש בקישור לטובת תקיפה אחרת, התוקף יכול להזליג מידע או להעביר פיקודים באמצעות ערוץ זה.
- תקיפת תוכנות מקבילות - לנוכח העובדה כי הפלטפורמה פועלת תחת הרשאות גבוהות, התקנתה (או שימוש בכלי וב) מאפשרת מיצוי מידע ותקיפה של אפליקציות אחרות הפועלות במקביל.
- ניצול להאזנה נפחית/חוזי - וזאת על ידי הפעלת המערכת ברקע ככלי האזנה.
- תקיפה כלכלית - אם קיים חיוב על פי שיחה או לפי כמות משתמשים, תוקף יכול למצות כספית את משאבי הארגון על ידי יצירת חיוב בפלטפורמה.
- אתגר משפטי - לאור העובדה כי פלטפורמות השת"פ ברובן מבוססות שרת, הנמצא לא בהכרח במדינת האם של המשתמשים, יתכן ויחולו חבות משפטיות או תנאים משפטיים מאתגרים.

תוקפים רלוונטים לסוג איום זה							
		במהלך פגישה					
תוקף חיצוני לתהליך	תוקף מבחוץ	בעלי הפלטפורמה	ארגון מקביל המשתמש בשירות	חבר בארגון אך לא שותף בפגישה	שותף בפגישות אך לא חבר בארגון	תקיפה על ידי משתתף בפגישה	תקיפה על ידי מוביל פגישה
X	V	V	X	X	X	X	X

הפרק יסקור נקודות שונות בהן תוקף יכול לגרום להטיה מחשבתית של שימוש הוגן בפלטפורמה, בעוד בפועל מתרחש שימוש זדוני:

- פרסום פגישה מזויפת - פרסום של פגישה כוזבת או פגישה בשם אדם למרות שלא יזם אותה, לשם תפיסת הזמן של המשתמש וקיבועו לנגישות למכשיר דיגיטלי או לשם הורדת התוכנה.
- קיום פגישה מזויפת - קיום של פגישה מלאה ביוזמת גורם אחר. זיוף הפגישה יכול לכלול את עצם הזימון ואפילו את המשתתפים, וזאת לנוכח העובדה כי יכולת המשתתף לזהות את הנמצאים בפגישה בצורה מלאה (מעבר להצהרותיהם) נמוכה.
- זיוף משתתף (התחזות) - לנוכח העובדה כי לא קיימת מערכת הזדהות אפקטיבית בפלטפורמה, והשתתפות בפגישה מובנית על מידע המוזן על ידי המשתתף, הרי שניתן לזייף משתתף (שינוי שם או שינוי עמוק - deep fake) ובכך להשתתף בפגישה בצורה זדונית.
- "חטיפת משתמש" - גניבה דיגיטלית של זהות המשתמש על ידי גניבת המזהים הדיגטלים של המשתמש אם לפני השיחה או במהלכה (גניבת סשן).
- טיפול בדיעבד בתוצרי הפגישה - שינוי קובץ הווידאו של הקלטה, הצ'אט או רשימת המשתתפים.

תוקפים רלוונטים לסוג איום זה							
במהלך פגישה							
תוקף חיצוני לתהליך	תוקף מבחוץ	בעלי הפלטפורמה	ארגון מקביל המשתמש בשירות	חבר בארגון אך לא שותף בפגישה	שותף בפגישות אך לא חבר בארגון	תקיפה על ידי משתתף בפגישה	תקיפה על ידי מוביל פגישה
V	V	X	V	V	V	X	X

כפי שמצוין במסמך, שימוש בפלטפורמות שיתוף אלו טומן בחובו מרחב חדש של איומים פוטנציאלים על הארגון ועל התכנים המועברים. להלן מספר המלצות לשימוש בטוח יותר בפלטפורמות שיתוף אלו. ההמלצות מחולקות לשני חלקים:

- בחירת פלטפורמות שיתוף - בחלק זה יופיעו מספר יכולות שיש לוודא כי הפלטפורמה תומכת בהן, על מנת לאפשר לארגון לפעול בצורה מיטבית.
- שימוש נכון בפלטפורמות - בחלק זה יוצגו מספר תהליכי יסוד בשימוש בפלטפורמות ומספר התנהגויות מונעות לשם מיטוב השימוש המוגן בפלטפורמות אלו.

בחירת פלטפורמות שיתוף

- אישור ודגשים מהלשכה המשפטית המתייחסים לפלטפורמה הפרטנית.
- במקרים רבים קיים פער ביכולות (אבטחתיות ואחרות) בין גרסאות שונות של הפלטפורמה (תלוי תשלום). יש לבחור בגרסה המאפשרת יכולות אבטחה ראויות.
- פלטפורמה המאפשרת העברה של מינימום מידע מהארגון לבעל הפלטפורמה.
- הגבלת מידע על קיום ישיבות לפי הרשאות.
- אי שמירת "ספרי טלפונים" בשרת בעל הפלטפורמה - אלא התחברות חיצונית.
- אי קיום של יכולת משתתפים נסתרים בפגישה.
- אינדיקציה ברורה לכניסת משתמש חדש לפגישה. על האינדיקציה להיות ברורה עבור כלל סוגי עמדות הקצה של המשתתפים (מחשב, סלולר) ולהיות מלווה הן באינדיקציה קולית והן באינדיקציה חזותית.
- קיום של חלוקת תפקידים (הרשאות) בין מנהל השימוש מטעם הארגון, מוביל פגישה, ומשתתף בפגישה.
- הגנה על הרשאת מנהל הלקוח ומוביל פגישה - אפשרות להזדהות חזקה (MFA) לפחות לבעלי תפקידים אלו.
- אינדיקציה ברורה לכלל משתתפי הפגישה כי הפגישה מוקלטת, על האינדיקציה להופיע במשך כל הפגישה.
- הצפנה של פגישות השמורות בפלטפורמה ובקרת גישה מחמירה על פגישות אלו, תוך הודעה לבעל הפגישה על נגישות גורם לתוכן זה.
- מתן נגישות למנהל הלקוח לרשימת הפגישות השמורות ואפשרות לניהול רשימה זו (מחיקה והגבלת תפוצה), אך ללא אפשרות להקלת הרשאות (הסרת סיסמה או מניעת הודעה למוביל הפגישה).

תהליך התקנת פלטפורמה (במידה ונדרש)

- יש להתקין את הפלטפורמה ממקור אמין בלבד (אתר החברה הרשמי, חנות רישמית להורדת אפליקציות).
- יש לוודא כי מותקנת גרסת התוכנה האחרונה וכי התוכנה מעודכנת כנדרש.
- בשים לב להרשאות הגבוהות של הפלטפורמות והנגישות לאמצעים חיצוניים (מצלמה, מיקרופון), מומלץ לבחור על איזה ציוד להתקין את הפלטפורמה ולהניח כי היא פעילה גם בעת שלא נראית כך.
- יש לוודא זיהוי שמי של המשתמש אך לא למסור פרטים נוספים.
- יש להגדיר את הפלטפורמות בצורה מאובטחת ככל הניתן. ברמה הארגונית וברמת המשתמש (לדוגמא מניעת אינטגרציה עם כלים נוספים).
- יש לוודא כי ברירות המחדל הן כי:
  - לתוכנה אין אפשרות לפעול ברקע.
  - בכל שינוי מצב (התחברות לשיחה, הוספת משתתפים וכדומה) מצלמה וקול מנותקים.
- נדרשת הצפנה של כלל נקודות הקצה (H323 / SIP).
- השבתת האפשרות להקלטה בענן.

תהליך זימון פגישה

- אין לתת לפגישה שם משמעותי אלא שם סתמי.
- את הזימון לפגישה יש להעביר בפלטפורמה אחרת המשמשת את הארגון.
- אין לנהל יומנים בפלטפורמה, זימון אנשים לפגישה יתבצע מחוץ לפלטפורמה.
- מומלץ כי לישיבה תוגדר סיסמה שתתחלף בכל פגישה (מעבר למספר הפגישה) וכן כי הסיסמה תועבר בדרכי תקשורת חלופיים למשתתפי הפגישה.
- אין לאפשר למשתתפים בפגישה לזמן אחרים באופן עצמאי.

תהליך תחילת פגישה

- אין להניח כי השמות הרשומים בישיבה אכן נכונים, מומלץ כי זימונים יגיעו בערוץ אחר מוכר, ויש לענות רק להם (ולא זימונים המגיעים בפלטפורמה).
- מומלץ שכולם יעלו בווידאו (לפחות לרגע ראשון) על מנת לוודא כי כל המשתתפים אכן מוכרים.
- יש לוודא כי מחוברים אך ורק הגורמים הרלוונטיים (אחריות מוביל הפגישה) - וזאת לאורך כל משך הפגישה.
- אם משתנה "מוביל" הפגישה ללא ידוע המשתתפים, בצעו ניתוק מידי של הפגישה.
- יש לוודא כי לא מוצג "מידע צד" במהלך וידאו או שיתוף מסך - לסגור כל דבר שאינו רלוונטי ולהפנות את המצלמה אל קיר לבן כרקע.

תהליך סיום ישיבה

- יש לוודא ניתוק מהמערכת לפני תחילת פגישה חדשה.
- יש לוודא כי כלל המשתמשים התנתקו לפני סגירת הישיבה על ידי יוזם הפגישה.
- יש לנתק או להסתיר את המצלמה, וכן לנתק את המיקרופון.

ביבליוגרפיה

- Security in webex - https://www.webex.co.in/content/dam/webex/eopi/Global-en/documents/pdf/security_webex.pdf
- https://www.eztalks.com/video-conference/tips-for-secure-web-conferencing.html
- https://www.techrepublic.com/article/how-to-secure-your-zoom-conference-line-from-hackers/
- רשות המיסים - הנחיות אבטחה לשימוש באפליקציית ZOOM.
- משרד הבריאות - הנחיות אבטחת מידע לעבודה מהבית ולשימוש בכלים לשיחות וידאו.

*** סוף מסמך ***