05 אפריל 2020
י"א ניסן תש"פ
סימוכין:ב-ס-1049

המלצות לשימוש בתוכנת Zoom

תקציר

לאור מגפת הקורונה ומעבר של ארגונים רבים לעבודה מרוחקת מהבית, רבים מהם עושים שימוש בתוכנות שת"פ (collaboration) שונות.
תוכנת Zoom בולטת בימים אלו בשימוש אינטנסיבי על ידי ארגונים רבים. מטרת מסמך זה, מתן המלצות לשימוש בטוח יותר בתוכנה זו.

פרטים

1. לאור השימוש המוגבר בתוכנה זו בימים אלו, גם תוקפים החלו לנסות ולתקוף משתמשים העושים שימוש במערכת זו.
2. התקיפות נעות מוונדליזם ומניעת שירות, דרך ניסיונות לתקוף את משתמשי המערכת ולגנוב נתוני הזדהות, או אף להתקין פוגען על עמדת המשתמש.
3. הוצפו מספר נושאים העוסקים בתוכנה, ביניהם:
   1. היכולת של תוקפים להתפרץ לשיחות Zoom שלא הוזמנו אליהן, ולהפריע למהלך התקין של השיחה.
   2. דיווח על פגיעות המאפשרת לתוקף משלוח קישור לשרת חיצוני העושה שימוש בפרוטוקול SMB. הפעלת הקישור גורמת למערכת ההפעלה לנסות לתקשר עם השרת, ולכן פרטי ההזדהות של המשתמש מועברים אליו באופן אוטומטי ועלולים להיתפס בידי התוקף. פגיעות זו הינה למעשה התנהגות ברירת המחדל של

מערכת ההפעלה, וקיימת גם כאשר הקישור מועבר במסמכי אופיס וכד'. לא מדובר בפגיעות ספציפית לתוכנת Zoom.

3. דיווחים לגבי ההצפנה של התוכנה, והאם היא מוצפנת מקצה לקצה. פורסמו דיווחים כי בניגוד לנטען בידי החברה, הצפנת השיחה אינה מקצה לקצה. החברה פרסמה הבהרה, ובה מודגש כי כאשר כל משתתפי השיחה עושים שימוש בתוכנות קליינט עדכניות, **והשיחה אינה מוקלטת**, השיחה אכן מוצפנת מקצה לקצה. אך אם חלק מהמשתתפים עושים שימוש בממשקים אחרים, החל משיחת טלפון וכלה בהקלטת השיחה, ההצפנה אינה מקצה לקצה.
4. נושאים נוספים שאינם קשורים ישירות לתוכנה:
   1. שימוש בדומיינים הכוללים את שם התוכנה במתקפות פישינג וכד'.
   2. שימוש בתוכנות זדוניות המתחזות לקליינט של Zoom ועידוד המשתמשים להתקינן.

דרכי התמודדות

1. על מנת למנוע מגורמים זרים להתפרץ ולהפריע לשיחות ZOOM, מומלץ לנקוט בצעדים הבאים:
   1. לפרסם את קיום הפגישה באמצעים פנים ארגוניים ולא פומביים.
   2. להגדיר סיסמה לפגישה.
   3. לנעול את הפגישה לאחר שכל המשתתפים הצטרפו, כך שלא ניתן לצרף משתמשים חדשים.
2. על מנת למנוע מנתוני הזדהות לדלוף, מומלץ לנקוט בצעדים הבאים:
   1. להימנע מלהפעיל קישורים המועלים על ידי משתתפים לפגישה.
   2. לעדכן הקליינט למערכת הפעלה Windows לגרסה 4.6.9 שמונעת הפעלת קישורים מסוג זה. קישור בסעיף "מקורות".
   3. להגדיר ב-Firewall מניעת תעבורה יוצאת בפורט 445 (SMB).

3. על מנת להימנע מדלף מידע המועבר בשיחות, מומלץ לנקוט בצעדים הבאים:
   1. להגביל השיחות רק למשתמשים שיש להם קליינטים עדכניים הפועלים על גבי מחשב או סמארטפון, ולא להקליט את השיחה.
   2. מלכתחילה להגביל סיווג השיחה כך שגם אם ידלוף מידע, הוא לא יהיה מסווג.
4. מומלץ להתקין התוכנה אך ורק מחנויות היישומים הרשמיות (AppStore, Google Play), או מהאתר הרשמי של החברה.
5. מומלץ לצרוך מידע לגבי התוכנה רק מאתרים מוכרים ורשמיים.
6. ראו בסעיף "מקורות", המלצות החברה בנוגע לאבטחת השיחות.

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

מקורות

1. https://zoom.us/security
2. https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/
3. https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
4. https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/
5. https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows