אירוע סייבר בחברה בינלאומית לציוד רפואי

12/03/2026
כ"ג אדר תשפ"ו

[תקציר]

1. לאחרונה פורסם מידע ראשוני על אירוע סייבר בחברה בינלאומית לציוד רפואי.
2. על פי דיווחים פומביים, התוקפים נטרלו מספר רב מאד של עמדות קצה של החברה והעובדים (BYOD), בפרט ציוד נייד כגון סמארטפונים ומחשבים ניידים, באמצעות גישה בלתי מורשית למערכת הניהול של ציוד זה.

[פעולות מידיות לביצוע]

- אם ארגונכם מנהל באמצעות מערכת UEM – Unified Endpoint Management, את ציוד הקצה של המשתמשים, וודאו כי פעולות בעלות פוטנציאל פגיעה רחב בפעילות החברה, כגון מחיקה (Wipe) של מספר רב של עמדות קצה וציוד נייד, **נאכפות אך ורק אם אושרו על ידי 2 מנהלנים מורשים**.
- המערכת שככל הנראה מנהלת את ציוד החברה שהותקפה, מאפשרת לאכוף זאת באמצעות מנגנון בשם Multi-Admin Approval.
- אם קיים בארגונכם מנגנון דומה, וודאו כי הוא מוגדר בהתאם. היעזרו בתיעוד או בנציגי היצרן על מנת לבחון כיצד ניתן לממש זאת.

[פרטים]

1. על פי הפרסומים הפומביים, החברה משתמשת בתוכנת InTune של מיקרוסופט לניהול ציוד קצה.
2. התוכנה כוללת יכולת מחיקה מרחוק של עמדות הקצה, עם מספר **רמות חומרה** למימוש המחיקה.
3. ככל הנראה, התוקפים השיגו נגישות בדרך שטרם פורטה אל המערכת, והפעילו פקודה למחיקה ברמת החומרה הגבוהה ביותר, של כלל הציוד המנוהל באמצעותה.

[דרכי התמודדות]

1. הגבילו למינימום הנדרש את הכתובות המורשות לגשת למערכת ניהול ציוד הקצה, ואת מספר המנהלנים המפעילים אותה.
2. וודאו כי הגישה למערכת מחייבת הזדהות חזקה, רצוי באמצעי זיהוי החסין למתקפות דיוג כגון FIDO Keys.
3. אם מערכת ניהול ציוד הקצה תומכת בכך, הפעילו מנגנון כדוגמת Multi-Admin Approval, המחייב אישור של 2 מנהלנים בטרם ביצוע פעולות קריטיות כגון מחיקה גורפת של ציוד.
4. אם מערכת ניהול ציוד הקצה תומכת בכך, הגבילו מראש האפשרות למחיקה גורפת של פריטי ציוד למספר פריטים מוגבל. תוקף שירצה למחוק חלקים נרחבים של הציוד הארגוני, ייאלץ לבצע את פקודת המחיקה מספר פעמים. לדוגמה, בארגון עם 10,000 פריטים מנוהלים והגבלה של מקסימום 100 פריטים לכל פקודת מחיקה, התוקף יצטרך להפעיל את הפקודה 100 פעמים, באופן שיכול לסייע לזיהוי הפעילות החריגה.