ניטרול האפשרות להזדהות חזקה
למטרת גניבת נתוני הזדהות

20/04/2026
ג' אייר תשפ"ו

[תקציר]

1. לאחרונה דווח למערך הסייבר הלאומי על תקיפת סייבר בה התוקף ביצע מתקפת מניעת שירות כנגד השרת האחראי להזדהות החזקה בארגון המותקף, במטרה להפעיל מנגנון הזדהות חלש יותר המשמש כגיבוי למנגנון ההזדהות הראשי.
2. מטרת התרעה זו, הכרת שיטת פעולה זו ודרכים להתמודדות עימה.

[פעולות מידיות לביצוע]

- היערכו מראש עם מספר שיטות לביצוע הזדהות חזקה.
- הימנעו ככל האפשר משימוש בהזדהות המבוססת על רכיב בודד כגון סיסמה.
- העבירו את כל המשתמשים, **ובפרט המנהלנים של כל המערכות הארגוניות**, להזדהות החסינה בפני דיוג (Phishing resistant MFA).
- יישמו מנגנון Throttling עבור ניסיונות הזדהות כושלים רציפים.

[פרטים]

1. התוקף ביצע מתקפת מניעת שירות כנגד השרת האחראי להזדהות החזקה בארגון המותקף.
2. בשל חוסר היכולת לבצע הזדהות באמצעות שרת זה, הופעל מנגנון הזדהות שהוגדר מראש כגיבוי, המבוסס על שם משתמש וסיסמה בלבד.
3. התוקף נערך לכך מראש וניצל את שנמוך מנגנון ההזדהות להזדהות המבוססת על רכיב בודד (Something You Know), באמצעות הפניית המשתמש לאתר מתחזה שמטרתו השגת נתוני ההזדהות של המשתמשים.

[דרכי התמודדות]

1. מומלץ מאד להיערך מראש עם יותר מאפשרות אחת למימוש הזדהות חזקה, ואם עולה צורך להפסיק שימוש באפשרות המועדפת מכל סיבה שהיא - בין אם תקלה ובין אם בעקבות תקיפה, עיברו למנגנון MFA חלופי. לדוגמה, אם מנגנון הזיהוי הראשי שלכם מבוסס על סיסמה וכרטיס חכם, היערכו מראש עם מנגנון זיהוי חלופי באמצעות סיסמה ויישומון Authenticator בסמארטפון. מומלץ מאד לא לעבור למנגנון זיהוי הכולל רכיב בודד כדוגמת שם משתמש וסיסמה.
2. מומלץ מאד לחייב את כל המשתמשים, **ובפרט את כל מנהלני המערכות השונות**, בשימוש במנגנון הזדהות חזקה חסין לניסיונות דיוג (Phishing Resistant MFA).
3. וודאו כי מוגדרת עבור מנגנוני ההזדהות השונים הגבלה של האפשרות להזדהות לפרק זמן מסוים, לאחר מספר ניסיונות הזדהות כושלים. מומלץ להגדיר מספר נמוך יחסית של ניסיונות הזדהות טרם חסימה (לדוגמה – 5 עד 10) ופרק זמן גדל והולך לחסימה ככל שניסיונות ההזדהות הכושלים נמשכים.
4. וודאו כי המשתמשים מודעים לשיטת תקיפה זו, והנחו אותם כי בכל מקרה של שנמוך אופן ההזדהות יש לוודא (באמצעות בדיקת התעודה הדיגיטלית של אתר ההזדהות) כי אכן הם מחוברים לשרת הנכון.