היערכות לתקיפות האקטיביסטים במרחב הישראלי

30/03/2026
י"ב ניסן תשפ"ו

[תקציר]

1. מידי שנה עולה האפשרות לתקיפות במרחב האינטרנט הישראלי סביב ימי ציון ואזכור קבועים החוזרים מידי שנה כדוגמת OPIsrael החל ב-7/4/26, חגי האביב וימי הציון הלאומיים – יום השואה, יום הזיכרון ויום העצמאות.
2. בימים אלו, פועלים האקרים המזוהים עם קהילת ההאקטיביסטים Anonymous, וגורמים פרו-פלסטינים נוספים, על מנת לייצר נזק תדמיתי ופרסומי למדינת ישראל. בשונה משנים קודמות, בשנה זו תתקיים פעילות זו במקביל למבצע "שאגת הארי" כנגד איראן, והלחימה מול חיזבאללה בצפון.

[פעולות מידיות לביצוע]

- הצטיידות מראש בשירות להגנה מפני מתקפות מניעת שירות מבוזרות (DDoS).
- וידוא כי הגיבויים של הארגון תקינים, ולפחות עותק אחד מהם נשמר בכל עת באופן שאינו מקוון.
- שימוש ב-VPN או ZTNA לגישה מרחוק למערכות הארגון מרשת האינטרנט.
- חיוב כלל משתמשי הארגון, ובפרט מנהלנים של מערכות הנגישות מהאינטרנט, בהזדהות חזקה (2FA), רצוי כזו החסינה למתקפות דיוג.

[פרטים]

1. שיטות פעולה (TTPs) עיקריות:
   1. התחזות למשתמש מורשה באמצעות
      1. ניחוש נתוני הזדהות (Brute Force or Dictionary Attack, Credential Stuffing);
      2. שימוש בנתוני הזדהות גנובים;
      3. שימוש בנתונים שדלפו בעבר ונקנו ברשת האפלה וכד';
      על מנת להשיג נגישות למערכות.
   2. מתקפות מניעת שירות מבוזרות (DDoS).
   3. תקיפות השחתה (Defacement).
   4. הדהוד מידע כוזב (Fake News).

[דרכי התמודדות]

1. כלקח מתקיפות דומות בשנים קודמות, אנו ממליצים להיערך מראש הגנתית באופנים הבאים:
   1. ארכיטקטורה מאובטחת – מומלץ להטמיע את מערכות האבטחה הנדרשות בסביבת ה-Perimeter הארגונית, ו/או כשירות מחוץ לארגון (כדוגמת שירות ענן של ספק מתמחה).
   2. רכישה מראש של פתרונות הגנה נגד DDoS, תוך מתן דגש על מניעת התקיפה במיקום המרוחק ביותר רשתית מהרשת הארגונית (עדיפות לעצירת התקיפה באמצעות תשתיות ייעודיות בחו"ל, לאחר מכן בתשתיות ספק האינטרנט ורק לבסוף בחצרי הארגון).

3. שימוש במערכות כגון VPN או ZTNA, עם הצפנה והזדהות חזקה מתאימה (2FA), עבור גישה מרשת האינטרנט לממשקים של מערכות כגון CMS, WebMail וכד', בפרט עבור משתמשים עם הרשאות מנהלן, אך מומלץ מאד לכל המשתמשים.
4. חסימת גישה לא רצויה מחוץ לישראל (GEO Protection). מדובר בפתרון חלקי בלבד, שתוקפים מתקדמים יודעים כיצד לעקוף.
5. הגברת מודעות עובדים, היערכות, מוכנות וכוננות של צוותי SOC, צוותי IR ובעלי עניין.
6. יש לוודא קיום גיבויים תקינים ואמינים של כל המידע החיוני לרציפות העסקית של הארגון. רצוי שלפחות עותק גיבוי אחד יישמר בכל עת באופן לא מקוון.
7. יש להקפיד על דיווח מיידי לממונה אבטחת המידע הארגוני, בכל חשד לפעילות חריגה או פגיעה בשירות.

עיקר הפעילות בימים אלו מבוססת על שיח המתנהל ברשת, בעיקר ברשתות החברתיות, וכן על אירועים במרחב אשר מלבים את השיח הניצי והפרו-פלסטיני וגורמים בסופו של דבר לעליה במספר התקיפות.

השנה, ההתפתחויות האזוריות מגבירות את המתיחות הקיימת ממילא, ועלולות להגביר את כמות התקיפות ומבצעי ההשפעה במהלך תקופה זו ובפרט בימי הציון/אזכור.

מערך הסייבר הלאומי יעדכן התרעה זו ככל שיידרש, לצורך הערכות מתאימה.

⚠

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.