

7 באוקטובר 2023
כ"ב בתשרי תשפ"ד
סימוכין: ב-ס-1625

התרעה דחופה: העלאת מצב כוננות סייבר במשק

תקציר



1. כחלק מההיערכות הכללית במשק למצב המלחמה, כלל הארגונים במשק נדרשים להעלות רמת הכוננות לאירועי סייבר באופן מיידי.
2. **הבהרה:** בשעות האחרונות רצות שמועות אודות מתקפות סייבר על ישראל, אנו מזכירים כי בחירום, כמו בשגרה, יש להימנע מכניסה לקישורים לא מזהים. אנו קוראים לציבור ולארגונים לגלות אחריות ובכל חשד למתקפת סייבר ולבירור שמועות הקשורות בסייבר, יש לחייג 119.

היערכות



1. על כל הארגונים במשק לבצע את הפעולות הבאות:
 1. רענון נהלי חירום פנימיים, דרכי תקשורת.
 2. הגברת ערנות לאירועים חריגים.
 3. בדיקת תקינות אמצעי האבטחה.
 4. תגבור פעולות לשמירת לוגים, ופעילות לניתוח לוגים והתרעות.
 5. שמירת לוגים במדיה חיצונית או נפרדת באופן יומי.
 6. וידוא ורענון מוכנות מערך ההתאוששות (DR).
 7. דחיית פעולות שאינן דחופות כגון עדכון גרסה, החלפת רכיבים וכד'.¹
 8. רענון מיפוי הטופולוגיה והתצורה של המערכות.
 9. תדרוך גורמי אבטחה ותפעול.
 10. אירועים חריגים - יש לדווח מיידי למערך הסייבר הלאומי.

שיתוף מידע עם ה-CERT 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.

