2 אפריל, 2025

========== מבזק מיוחד לתעשייה ==========

מסמך המלצה להגברת חומות לקראת מתקפת OpIsrael

רחוב בנק ישראל 7, בניין ג'נרי 2, ירושלים 9195024 טל: 074-7675850/1/4 cyber_industry@sviva.gov.il

רקע

כמדי שנה בשנה, בתאריך 7 באפריל ובמספר ימים שלפניו ואחריו מתקיימת פעילות תקיפות סייבר מרחבי העולם כנגד ישראל המוכרת בשם OpIsrael .

פעילות זו מתבצעת מזה מספר שנים (שנה אחר שנה בהתמדה) על ידי קבוצות אקטיביסטים המזדהים כקבוצת **אנונימוס** מרחבי העולם ובעיקר ממדינות ערב ומדינות אסלאמיות נוספות, אשר חרטו על דגלם פגיעה בגופים ישראלים בתגובה לסכסוך הישראלי-פלשתיני אך גם ממדינות מערביות וידידותיות שדרכם פועלים אותם אקטיביסטים.

יעדים פוטנציאליים לתקיפה הינם: אתרים של גופים ממשלתיים, אתרים של ארגוני בריאות רשמיים, מפעלי תעשייה ובתוכם מפעלי חומרים מסוכנים, רשתות קמעונאיות, אתרים פיננסיים, אתרי תקשורת, חברות אחסון ישראליות, אתרי עיריות ומועצות, אתרי אקדמיה ועוד.

בתקיפה צפויות לפעול מספר קבוצות האקרים שונות המזוהות עם אנונימוס, אשר משתפות אחריהן ציבור תומכים רחב בעזרת כלי תקיפה אוטומטיים המפורסמים ברשתות תומכי אנונימוס.

הרשתות החברתיות השונות כמו גם פורומים ייעודיים משמשים לרתימת האקרים, תקשורת עמם והעלאת כלים ויעדים לתקיפה.

תקיפות "רועשות" אלה עלולות גם להוות מיסוך להתקפות יותר ממוקדות ויותר חכמות , ויתכן שגם תחנות פנימיות הנמצאות בתוך המפעלים שבהם קיימים בוטים יפעלו כנגדנו ביום פקודה ולא רק פעילות חיצונית ממרחב האינטרנט.

משנה לשנה ההערכות למתקפות בקרב גופים בישראל עולה מדרגה עקב המודעות הרבה לתקיפת זו והגבהת חומות וערנות טרם התקיפה

מטרות מתקפת הסייבר:

- יצירת הד תקשורתי וקידום אג'נדה פוליטית.
- זריעת פחד בקרב הציבור הישראלי.
- השבתת / שיבוש פעילות תעשייתית כולל תעשיית החומרים מסוכנים
- פגיעה באמון הציבור באתרים ממשלתיים ופיננסיים.
- מניעת אספקת שירותים אינטרנטיים (לדוגמא: גישה לשירותים בנקאיים, שירותי ממשל זמין ועוד).
- מניעת שירותים רפואיים.
- חשיפת פרטים אישיים ופיננסיים (לדוגמא: כרטיסי אשראי וכדומה).
- תקיפות למטרות כופר.

רחוב בנק ישראל 7, בניין ג'נרי 2, ירושלים 9195024 טל: 074-7675850/1/4 cyber_industry@sviva.gov.il

שיטות פעולה שננקטו ע"י התוקפים בשנים קודמות וצפויות גם השנה:

- התקפות מניעת שירות (DoS (Denial of Service ותקיפת מניעת שירות מבוזרת DDOS (Distributed Denial of Service)
- נסיון חדירה לכתובות פתוחות לעולם כולל מערכות OT המכילות מערכות בקרה המנהלות / מבקרות חומרים מסוכנים, שיבוש הפעילות ונסיון לגרימת נזק משמעותי.
- נסיון לשיבוש מערכות ייצור ובתוכם מערכות המבקרות / מנהלות חומרים מסוכנים דרך האיום הפנימי (בוטים / נוזקות השתולים בתחנות עבודה ברשת הפנימית)
- מתקפות פישינג – ניסיון לגניבת מידע אישי ו/או חסוי ממשתמש ע"י התחזות לאתר או לגורם לגיטימי כגון: אתרי קניות, אתרי בנקים ועוד באמצעות שליחת דואר מתחזה המכיל צרופה נגועה בקוד זדוני או שליחת דואר אלקטרוני הכולל בתוכו קישור לאתר זדוני.
- הכנסת נוזקות ורוגלות למפעל לצורך גניבת מידע.
- חדירה למאגרי נתונים ושיבושם או הדלפת מידע.
- הדבקה בתוכנות כופרה.
- השחתת אתרי אינטרנט.
- פריצה לשרתי ארגונים /חברות /ספקי שירות ודרכם לגופים נוספים.

המלצות להגברת חומות

להלן מספר המלצות לביצוע לקראת ה-7.4.2025 :

- ביצוע עדכוני אבטחה במערכות הפעלה בתחנות עבודה ובפרט בשרתים לסגירת חולשות ידועות.
- ביצוע עדכונים בכל רכיבי אבטחת המידע לסגירת חולשות קיימות וידועות (רכיבי חומת אש, סינון תוכן, הגנה על עמדות הקצה, הגנה אפליקטיבית, הגנה על בסיסי הנתונים ועוד)
- הורדת שירותים ומשתמשים מיותרים שלא בתוקף ממערכות אבטחת המידע, תחנות עבודה בדגש על תחנות אדם מכונה (HMI) והשרתים השונים בדגש על שרתי SCADA שרתי ERP ושרתי MES וכל שרת / שירות להם נגיעה לפעילות הייצור ופעילות ניהול / בקרה של חומרים מסוכנים .
- הורדת הרשאות לא נחוצות במערכות ההפעלה במערכות ה-HMI , בשרתים , ובמערכות הבקרה
- החלפת סיסמאות בשירותים קריטיים (עמדות HMI , בקרים, שרתי ERP , שרתי MES וכל שירות קריטי אחר)
- ביצוע ווידוי הפצת הגנה על תחנות הקצה ושרתים (אנטי-וירוס, EDR וכדומה) כולל ביצוע עדכוני אבטחה אחרונים
- ביצוע פעילות יזומה של ניקוי ווירוסים בתחנות עבודה ובשרתים בדגש על רשתות OT (גם אם אינן חשופות לאינטרנט)

רחוב בנק ישראל 7, בניין ג'נרי 2, ירושלים 9195024 טל: 074-7675850/1/4 cyber_industry@sviva.gov.il

- צפיה מוגברת ורציפה בלוגים במערכות השונות של אבטחת המידע וניטור תקשורת חשודה
- במידה וקיים סוק – הנחייה למפעילי הסוק להגברת הערנות מול התראות קופצות.
- מתן תשומת לב מיוחדת לשרשרת האספקה ולפעילותה בימים אלה (התחברויות מרחוק, הגעת טכנאים לאתר ועוד)
- קיום כוננות צוותים לקריאה מיידית במקרה אירוע סייבר לצורך הכלה ותגובה לכל פעילות תקיפה ברשת
- רענון תהליכי מעבר לפעילות ידנית וניטרול מערכות ממוחשבות עקב פגיעה במערכות בקרה המנהלות / מבקרות חומרים מסוכנים
- ביצוע בדיקה מדגמית של שחזור מגיבוי בייחוד במערכות הבקרה המנהלות / מבקרות חומרים מסוכנים.
- סריקות חיצוניות לבדיקת חולשות (שרתים ושירותים מוחצנים)
- סריקות פנימיות לבדיקת חולשות ברכיבים קריטיים (שרתי SCADA, שרתי DC, שרתי DB , שרתי ERP ו -MES וכל שירות קריטי אחר)
- טיוב חוקים בחומות האש ובמוצרי האבטחה השונים המכילים חוקים.
- חסימת GEO LOCATION ככל האפשר לאזורים שלא אמורה להגיע תקשורת מהם (מבלי לפגוע בהמשכיות עסקית)
- הקפאת תצורה ושינויים בתקופה של כיומיים לפני ויומיים לאחר ה-7.4

הערה:

מסמך זה נכתב לצורך סיוע תעשיית החומרים המסוכנים בהגבהת חומות כ**המלצה בלבד ואינו מחייב**.
המסמך לא בא במקום פעילות שכבר מתקיימת במפעלים אלא בנוסף.

בכל שאלה בנושא או במקרה אירוע שהתרחש ניתן לפנות ישירות טלפונית לאחד הגורמים הבאים:

יוסי שביט – ר' יחידת הסייבר בתעשייה, המערך הלאומי לחירום וחומ"ס 058-6662242

אתי רזניק – מנהלת סוק סביבה, המערך הלאומי לחירום וחומ"ס 052-5215367

יוסי שביט

========== מבזק מיוחד לתעשייה ==========

רחוב בנק ישראל 7, בניין ג'נרי 2, ירושלים 9195024 טל: 074-7675850/1/4 cyber_industry@sviva.gov.il