טיוטת נוסח להגדרת מוצרים וידע לפיקוח בתחום הסייבר

טקסט המסומן בצהוב מציין תוספת על הקבוע ברשימת ה–dual-use של הסדר ואסנאר

הגדרות

"תוכנת חדירה" (Intrusion Software) – תוכנה אשר תוכננה או שהותאמה במיוחד לצורך מניעת גילוי על–ידי כלי ניטור (monitoring tools), או על מנת להתגבר (to defeat) על מערכות או אמצעי הגנה (protective countermeasure) של מחשב או מכשיר בעל יכולת קישור לרשת, ואשר מבצעת אחד מהבאים:

א. מיצוי/משיכת (extraction) מידע ממחשב או ממכשיר בעל יכולת קישור לרשת, או שינוי מידע של מערכת או של משתמש; או

ב. שינוי נתיב ריצה (execution path) סטנדרטי של תכנית או תהליך על מנת לאפשר ביצוע של הוראות חיצוניות.

ג. שיבוש של יכולות פונקציונאליות של המערכת או גרימת נזק פיזי למערכת.

ואינה כוללת את אחד מהבאים:

א. היפרוויזורים (תוכנה להרצה וניהול מכונות וירטואליות), כלי תיקון שגיאות או תוכנות לביצוע הנדסה הפוכה;

ב. תוכנה לניהול זכויות יוצרים דיגיטליות (DRM);

ג. תוכנה שתוכננה להתקנה על ידי היצרן, האדמיניסטרטור או המשתמש על מנת לעקוב אחר נכסים או שחזורם.

"מכשיר בעל יכולת קישור לרשת" – כולל מכשירים ניידים ומונים חכמים.

"כלי ניטור" – תוכנה או חומרה אשר מנטרת את התנהגות המערכת או התהליכים אשר רצים על מכשיר, לרבות, מוצרי אנטי וירוס, מוצרי הגנה על נקודות קצה, מוצרי הגנה אישית (PSP), מערכות לזיהוי חדירה (IDS), מערכות למניעת חדירה (IPS) או חומות אש (Firewall).

"מערכות/אמצעי הגנה" – טכניקות שתוכננו להבטיח הרצה בטוחה של קוד, כגון מניעת ביצוע הרצת תוכנה (DEP), שינוי אקראי של כתובות (ASLR) או שימוש ב"ארגז חול" (מנגנון להרצת תכניות בצורה בטוחה).

"חולשה" – חוסר שלמות בקוד או בפרוטוקול, אשר ניתן לניצול לפגיעה במערכת או בתוכנה.

"פורנזיקה דיגיטלית" – השגת, ניתוח או שחזור מידע באמצעות ממשק פיזי לציוד מחשוב או אחסון כגון מחשבים, מכשירי טלפון סלולריים, דיסקים קשיחים, מכשירי ניווט לווייניים, רכיבי USB, כרטיסים חכמים וכרטיסי SIM.

"מידע סטטי" – מידע אשר נשמר בדיסק קשיח או ציוד אחסון אחר, שאינו דורש מקור מתח חשמלי לצורך שמירה על המידע.

"מידע נדיף" – מידע אשר נשמר בציוד, שדורש מתח חשמלי לצורך שמירה על המידע.

תוספת לרשימת הפיקוח

מערכות ציוד ואביזרים:

1. תוכנות חדירה ומערכות הכוללות תוכנות חדירה.
2. מערכות, ציוד ורכיביהם, אשר תוכננו או שהותאמו במיוחד ליצירת, הפעלה, העברה (הדבקה) או תקשורת עם תוכנות חדירה, לרבות מערכות ציוד ואביזרים שתוכננו או הותאמו במיוחד לדמות שימוש, הפעלה או תקשורת עם תוכנת חדירה כנגד אחר, ולמעט מתן שירותים לבדיקות חסינות מערכות מפני תקיפה (PT).
3. מערכות ציוד ורכיבים שתוכננו או הותאמו במיוחד להגנה על מערכות ביטחוניות אסטרטגיות או להגנה על ציוד לחימה מפני תוכנת חדירה.
4. מערכות ציוד ורכיבים שתוכננו או הותאמו במיוחד לטובת הגנה או ניטור של עורקי תקשורת ברמה הלאומית.
5. ציוד, רכיבים ותוכנה לביצוע פורנזיקה דיגיטלית או לביצוע הדמיה של פורנזיקה דיגיטלית אשר:
   א. תוכננו במיוחד לבצע או להשתמש בטכניקות למניעת אפשרות שינוי המידע, על מנת להעתיק את המידע בשלמותו; או
   ב. תוכננו במיוחד לבצע אנליזה של המידע לשם:
      1) שחזור מידע סטטי שנוצר ע"י המערכת או המשתמש;
      2) זיהוי או ניתוח של מידע נדיף שנוצר על ידי המערכת או המשתמש.

תוכנה:

6. תוכנה אשר תוכננה או שהותאמה במיוחד ליצירה, הפעלה, העברה (הדבקה) או תקשורת עם תוכנות חדירה, לרבות תוכנה שתוכננה או הותאמה במיוחד לדמות שימוש, הפעלה או תקשורת עם תוכנת חדירה כנגד אחר, ולמעט מתן שירותים לבדיקת חסינות מערכות מפני תקיפה (PT).
7. תוכנה שתוכננה או הותאמה במיוחד להגנה על מערכות ביטחוניות אסטרטגיות או להגנה על ציוד לחימה מפני תוכנת חדירה.
8. תוכנה שתוכננה או הותאמה במיוחד לטובת הגנה או ניטור של עורקי תקשורת ברמה הלאומית.

טכנולוגיה וידע:

9. טכנולוגיה וידע לפיתוח של תוכנת חדירה.
10. חולשה, למעט אחת מאלה:
    א. חולשות הנמסרות באופן בלעדי למי שפיתח את הקוד או הפרוטוקול, או למי מטעמו;
    ב. חולשות המוצאות לנחלת הכלל;
    ג. חולשות המיועדות לשימוש במוצרי הגנה בלבד, המיוצרים בחברה המחזיקה בחולשה או בחברה. בסעיף זה "חברה" – לרבות חברה שהיא חברה-בת או שיש לה חברה-בת כהגדרתה בחוק ניירות ערך, התשכ"ח-1968.
11. מערכת או תוכנה שתוכננה או הותאמה במיוחד לאיתור חולשות אוטומטי, לשם ביצוע שימוש בהן בתוכנת חדירה כנגד אחר.