16 ביוני 2016
י' בסיוון התשע"ו
סימוכין: ב-מפ-0363

הנדון: <u>פנייה מוקדמת לקבלת מידע לתשתיות ושירותים למעבדת בדיקות סייבר לאומית "ספקטרום" – התייחסות לשאלות הבהרה – גרסה מעודכנת</u>

1. במסגרת הפנייה שבנדון ניתנה אפשרות להעברת שאלות הבהרה בטרם הגשת ההצעות.
2. להלן התייחסותנו לשאלות ולבקשות ההבהרה שהתקבלו:

א. **שאלה:** בהתייחס ל-50 מכונות וירטואליות/פיזיות (מענה לבקשה – סעיף 1). כמה מכל סוג? ולמה?
התייחסות: ניתן להניח כי הרשת לניסוי תורכב ברובה ממכונות וירטואליות. ייתכן חיבור של מכונות פיזיות היכן שהדבר מתחייב, לדוגמא עבור ציוד חומרה ייחודי (שאינו גנרי ושלא ניתן להריצו מעל תשתית הווירטואליזציה), או לצרכים ייחודיים של הבדיקה.

ב. **שאלה:** מה הכוונה בתשתית בסיסית (עקרונות ודגשים למימוש – סעיף 7א')?
התייחסות: הכוונה בהקמה של הפלטפורמה הנדרשת להפעלה של המעבדה תוך חשיבה על יכולות הרחבה, והוספת יכולות החל משלב ההפעלה. כלומר, קיימת עדיפות לכך שהמעבדה תוקם בפרק זמן מהיר יחסית ועם ציוד בסיסי ותוכל להתרחב בתשתיות וביכולות בהתאם לצרכים האופרטיביים והתו"ל המתגבש החל מהפעלתה.

ג. **שאלה:** OPEN SOURCE – באיזו רמה (עקרונות ודגשים למימוש – סעיף 7ב')?
התייחסות:

1) מוצרי קוד פתוח יכולים להשתלב ברמות שונות כגון תשתית להקמת רשת הניסוי, כלים להזרמת התעבורה, כחלק מסט מוצרי ההגנה ברשת ומערכות הניטור והבקרה של הניסויים עצמם.
2) אנו בוחנים את החלופות השונות גם במסגרת בקשה זו לקבלת מידע.

ד. **שאלה:** תעבורת רשת לגיטימית – מה הגדרה של לגיטימי? האם פקטה ללא יעד היא לגיטימית או לא? כנ"ל לפקטה חסרה.
התייחסות: הכוונה ליכולת לייצר תעבורת רקע (רעש) נוסף על התעבורה הלא לגיטימית (עוינת), ומטרתה לדמות פעילות שגרתית ברשת הניסוי, אשר תבוא לביטוי בחיווים של המערכות והשירותים המותקנים בה. מצב של פקטה לא תקינה או חסרה יכול להיות כחלק מהתעבורה הלגיטימית או הלא לגיטימית כתלות במטרת הניסוי.

ה. **שאלה:** בנושא תעבורת רשת זדונית – האם רוצים להריץ נוזקה אמיתית או רק לדמות תעבורה זדונית (או לדמות את הנוזקה עצמה)?
התייחסות:

1) באופן כללי על המעבדה לאפשר את שני המקרים – הן דימוי של הרושעה והן הרצת הרושעה האמיתית (יתכנו מקרים מיוחדים כתלות במאפייני הרושעה עצמה).

2) היכולת לדמות פעילות של רושעה הינה חלק מהיכולת להוספה ועדכון תרחישי איום חדשים המבוקשת.

ו. **שאלה:** אופן השימוש במעבדה במתודולוגיות ותקינה מקובלת בעולם, כדוגמת NIAP ו-Common Criteria העוסקות בנושא.

התייחסות: פעילות המעבדה המיועדת הינה שילוב הן של מתודולוגיות וסטנדרטיים מקובלים בעולם (דוגמת Common Criteria ופרסומים שונים של NIST) היכן שישימים, והן של ידע פנימי בהתאם לייעוד המעבדה, שאינו עבור המגזר האזרחי וכמפורט בפנייה.