פנייה מוקדמת לקבלת מידע לתשתיות ושירותים למעבדת בדיקות סייבר לאומית "ספקטרום"

מאי 2016

כתובת לקבלת דואר: משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450811, פקס 03-7450822

פנייה מוקדמת לקבלת מידע (RFI) לשירותים ולתשתיות למעבדת בדיקות סייבר לאומית

רקע

1. מטה הסייבר הלאומי במשרד ראש הממשלה (להלן – המטה) ומפא"ת (המנהל למחקר, פיתוח אמל"ח ותשתית טכנולוגית) במשרד הביטחון, מובילים תהליכי מחקר ופיתוח שמטרתם שיפור החוסן וקידום יכולות הגנתיות ברמה הלאומית.
2. המטה, בשיתוף עם מפא"ת, מבקש להקים סביבת בדיקות לאומית (להלן – המעבדה), שייעודה שיפור המענה לאיומי סייבר והתמודדות עמם על ידי שיפור יכולת תכנון, מוכנות מבצעית ועמידה באיכות של מערכי הגנה בהתאמה לאיומים השונים.
3. המעבדה הנה סביבה ייעודית בטוחה שתאפשר בחינה מעמיקה של טכנולוגיות ופתרונות הגנה, מוצרים אזרחיים וכן רכיבי מו"פ ייעודי/פנימי של גוף לאומי (להלן – מוצרי הגנה) המיועדים לרשתות ארגוניות רגישות. בשלב זה הבדיקות הנן לשימוש פנימי בלבד.
4. המעבדה תהווה מוקד טכנולוגי ייחודי לאומי בתחום בדיקות סייבר, הן בהיבטי המחקר והפיתוח של מתודולוגיה ותכנון בדיקות והן ביכולת מימוש ויישום על בסיס תשתית מתקדמת.

משימות

משימותיה המרכזיות של המעבדה הינן:

1. פיתוח ידע ומתודולוגיות בתחום בדיקות מוצרי הגנה – ובכלל זה פיתוח תכניות בדיקות, פיתוח תהליכי עבודה יעילים, יישום תובנות מאירועי עבר וכן שיתוף והעברת ידע למערכים אחרים, למול ידע ממקורות חוץ ולמול צרכים לאומיים.
2. ביצוע – ביצוע בדיקות באופן סדור ועל פי המתודולוגיה ותכניות הבדיקות שנכתבו במעבדה למוצרים, פתרונות וטכנולוגיות שונות בתחום הגנת רשתות וסייבר.
3. דרישות והגדרות כלליות:
   א. הבדיקות יבוצעו בסביבת בדיקות מתקדמת שבה יכולת הרצת תרחישים מורכבים ברשת הדומה לרשת מבצעית וכלים תומכים לביצוע וניהול ניסויים בצורה מבוקרת.
   ב. הבדיקות יבוצעו הן לצורך בחינת ערך הגנתי (Security Effectiveness) תוך התאמה לאופן השתלבות המוצר הנבדק במערך היעד והן לצורך בחינת היבטים של חוסן ועמידות לפעילויות שיבוש ותקיפות ערוצי צד (Security Assurance) של המוצר הנבדק.
   ג. תהליך העבודה במעבדה יורכב מתכנון של בדיקות, הכנת התשתיות הנדרשות, ביצוע בדיקות וסיכומן.
      1) שלב תכנון הבדיקה יכלול בין היתר הכרות עם המוצר ואופן השתלבותו בסביבת היעד, מיפוי הסיכונים, סקירת ידע קיים/קודם וכתיבת תכנית בדיקה בהתאמה.
      2) בשלב הכנת התשתיות יבוצעו ההכנות הנדרשות לרשת לניסוי ולתרחישי הבדיקה.

3) בשלב ביצוע הבדיקות ייבדק המוצר בקונפיגורציה מוגדרת תוך הפעלה אוטומטית ומבוקרת של תרחישי בדיקה שהינם תעבורה לגיטימיים ו/או סימולציה של פוגענים, תוך ניטור ביצועים של המוצר הנבדק ושל רשת הניסוי.

4) בשלב הסופי יבוצע ניתוח תוצאות, שמירה וסיכום של הבדיקה.

ד. דוגמאות לתרחישי שימוש במעבדה הנן: בדיקות חוסן למוצרים בארכיטקטורות שונות, תשתית בדיקה למו"פ פנימי בשלבים שונים של הפרויקט בדגש על קונספט ובדיקות התכנות ובדיקת התאמה של מוצרי הגנה אזרחיים למול מתארים מבצעיים.

ה. דוגמאות מייצגות למשפחות מוצרים אשר יבדקו במעבדה הנן: Breach Detection Systems (Behavioral / Anomaly Detection, Threat Intelligence Systems), IDS/IPS, FW/App FW, DDoS Prevention Systems, Server/Endpoint Protection Systems, Secure Mail / Web Gateways, Sanitation and Content Filtering, Access Control.

עקרונות ודגשים למימוש

1. מעבדת "ספקטרום" תמוקם במתקן של הרשות הלאומית להגנת הסייבר (להלן – הרשות) בקריית הסייבר הלאומית בבאר שבע או במרכז הארץ.
2. הרשות תהיה בעלת הסמכות והאחריות הכוללת לפעילות המעבדה ואמונה על ניהולה בפן המקצועי והניהולי.
3. המעבדה תוקם ותופעל בידי ספק או קבוצת ספקים באתר המעבדה בהתאם לעקרונות ומטרות המעבדה שהוצגו לעיל.
4. החל משלב ההקמה, משימות הספק או קבוצת ספקים באתר המעבדה הן:
   א. פיתוח מתודולוגיה ומפרטי בדיקות.
   ב. ביצוע בדיקות.
   ג. פיתוח ותחזוקה של התשתית הטכנולוגית של המעבדה (חומרה, תכנה וציוד תקשורת)
   ד. הרחבות והתאמות לצרכים לאורך זמן ובהתאם להתפתחות לאורך חיי המערכת.
5. ההתקשרות תהיה לתקופה של כ-4 שנים, באופן שתתאפשר הארכה או החלפה של הספק או קבוצת הספקים תוך שמירה על הידע ורציפות התפקוד של המעבדה. כלל הידע, הציוד והתשתיות הטכנולוגיות במעבדה יהיה בבעלות ממשלת ישראל.
6. היקף כח האדם הצפוי למעבדה יעמוד על 7-9 בעלי תפקידים.
7. כיוון שמדובר במערך ייחודי שהידע הדרוש להפעלתו אינו מרוכז ומפותח דיו, ומנגד טכנולוגיות ברשתות ארגוניות ומערכי הגנה המוטמעים בהן הינו עולם רחב מאוד, ייושמו העקרונות המנחים להלן:
   א. בשלב ההקמה – הצטיידות בתשתיות בסיסיות של חומרה ותוכנה, הבאת כח האדם המתאים והידע הקיים בארץ ובעולם.
   ב. עדיפות לשימוש במוצרי קוד פתוח היכן שניתן.

ג. החל משלב ההקמה, מרכיב חשוב ביכולת של המעבדה הינו הגמישות להתאמות ולהרחבת יכולות, תשתיות וכלים של בדיקות, לפי צורך ולמול מרחב האיום המשתנה.

8. המעבדה צפויה להתרחב לתחומי בדיקה נוספים ולטכנולוגיות נוספות. בפרט, קיימת אפשרות סבירה שהמעבדה תרחיב את פעילותה לתחום של רשתות ייצור ומערכות סקאדה (ICS) ותאפשר יכולות בדיקה גם עבור מערכות הגנה כגון IDS/IPS, זיהוי אנומליות, מערכות הפרדה וסינון תוכן ברשתות אלו.

מטרת פנייה זו

המטה מעוניין לקבל מידע מספקים בעלי ידע וניסיון מקומי ובינלאומי לטובת מערך שירותי הידע ותפעול המצוין בסעיף הקודם. המציעים מתבקשים להתייחס לנקודות הבאות:

1. הצעות או רעיונות בדבר הקמת התשתיות הנדרשות למימוש הפעילות ובפרט לפי הנושאים להלן:

א. הקמת תשתיות סביבת בדיקות ובה יכולת סימולציה של רשתות מבצעיות, יכולת חזרתיות של ניסויים וגמישות בטופולוגיה ובארכיטקטורה של הרשת לניסוי. רשת מבצעית הינה רשת ארגונית מוקטנת, בגודל של עד 50 מכונות וירטואליות/פיזיות מסוג Windows/Linux, מופרדת לסגמנטים שונים, ובה מוטמעות אפליקציות ארגוניות שונות וכן מערכות הגנה וניטור סטנדרטיות.

ב. הקמת תשתית להזרמת אירועים ותרחישי איום לסביבת הבדיקות. התשתית תאפשר הזרמת מתארי תעבורה לגיטימיים ולא לגיטימיים בצורה מבוקרת לסביבת הבדיקות. התשתית תאפשר גמישות להרחבה לתרחישים חדשים, לנפחי תעבורה שונים, לפרוטוקולי תקשורת ולאיומים שונים.

ג. תשתית כלים תומכי ניסוי ומערכות ניהול לסביבת הניסוי – אוסף כלי ניטור ואנליזה שיוטמעו בסביבת הבדיקות, כלי השליטה והאוטומציה של הסביבה, החל משלב תכנון הניסוי, ביצוע הניסוי, ניתוח מסקנות ועד לשמירתו בארכיון והכנת הסביבה לניסוי הבא (ניתן להניח שבכל זמן מתבצע ניסוי אחד בסביבת הניסוי).

2. הצעות או רעיונות בדבר תהליכי עבודה, המיומנויות וההתארגנות הנדרשים למימוש הפעילות, ובפרט לפי הנושאים להלן:

א. מתן שירותים לפיתוח מתודולוגיה ומפרטי בדיקות – פיתוח תכניות לבדיקות חוסן, בדיקות אפקטיביות וערך של מוצרי הגנת סייבר (במשפחות שונות של מוצרים), תוך התאמה לדרישות המבצעיות ולמפת הסיכונים, למול ידע מצטבר מאירועים ומבדיקות עבר. הגדרה ותכנון של מתווה הבדיקות, תרחישי תעבורה, יעדי ביצועים לדוגמא יעדי זיהוי או פעילות אופרטיבית אחרת. כל זאת באופן יעיל ככל שניתן ותוך שימוש במקורות מידע נגישים וסטנדרטים באם אפליקטיבי.

ב. מתן שירותי ביצוע בדיקות – ביצוע בדיקות למוצרי הגנה מתחומים ומשפחות מוצרים רחבים, על כל שלביהן לרבות הכנת התשתיות ותרחישי הבדיקה הנדרשים, ביצוע הבדיקות תוך מעקב אחר מדדים ויעדים וסיכומן, כל זאת באופן סדור ובהתאם למתודולוגיה שפותח במעבדה.

ג. מתן תמיכה טכנולוגית שוטפת למעבדה לרבות פיתוח ייעודי של כלים תומכים והתאמות לכלי הבדיקה, ולתשתיות. כמו כן, שדרוגים שוטפים, אינטגרציות ואוטומציה של המעבדה.

ד. פירוט בעלי התפקידים ומומחיות נדרשת.

3. <u>תכנית בדיקה לדוגמא</u>

א. תכנית בדיקה לדוגמא לפי ניסיונו והבנתו של המציע, עבור בדיקה של מוצר מדף ממשפחת מוצרי סריקה וסינון מייל ברשת ארגונית המחוברת לאינטרנט (אין להתייחס למוצר ספציפי).

ב. התכנית תתייחס הן לתהליך העבודה במעבדה על שלביו: תכנון, ביצוע וסיכום של הבדיקה, והן לתכנית הבדיקה עצמה ולהשתלבותה במערך הטכנולוגי התשתיתי המוצע על ידי הספק.

ג. היקף התכנית לא יעלה על 20 עמודים.

4. תיאור יכולתם וניסיונם של הספקים ליתן את השירותים בתחום שצוינו לעיל ובפרט בתחומים הבאים: הקמה והפעלת תשתיות מעבדה ושירותים כמפורט להלן, אפיון וביצוע בדיקות חוסן וחדירות למוצרי הגנה, אפיון וביצוע בדיקות אפקטיביות וערך למוצרי הגנה, יכולת הבאת ידע משלים מהעולם בתחום וכן יכולת להקים ולממש חלק מהפעילות בסיווג סודי ומעלה.

5. הערכות ראשוניות ומדדי עלויות למרכיבים הנדרשים למימוש הפעילות.

6. הצעות או רעיונות בדבר יכולות בדיקה לתחום רשתות ייצור וסקאדה ובפרט בתחומים שצוינו לעיל.

7. הצעות נוספות ושירותים מתקדמים נוספים לפי הצורך בהתאם למטרות ומשימות המעבדה.

הגשת מענה לפנייה זו

1. יודגש כי פנייה זו הינה פנייה מוקדמת לקבלת מידע בלבד. פנייה זו אינה בבחינת הזמנה להציע הצעות ואינה חלק מהליכי מכרז, לפיכך אין בה כדי ליצור מחויבות כלשהי כלפי מי מהמשיבים ו/או לראות בה התקשרות משום סוג. הפנייה נועדה לקבלת מידע בלבד ובעקבותיה ישקול המטה את המשך פעולותיו בהתאם לשיקולים מקצועיים ועניינים.

2. המטה שומר לעצמו את הזכות להשתמש במידע אשר יתקבל בעקבות פנייה זו לצורך הרכבת רשימת ספקים פוטנציאליים, הכל לפי שיקול דעתו הבלעדי.

3. אם וככל שיתקיים מכרז בעתיד, יהיה רשאי המטה לשנות או להוסיף תנאים ודרישות, הכל לפי שיקול דעתו המקצועי ובהתאם לצרכיו.

4. המטה שומר לעצמו את הזכות לפנות, ככל שיידרש, למי שענה על פנייה זו בבקשה להשלמת מידע והבהרות, להצגת מצגות והדגמות, לביצוע פיילוט, לביקור באתרי הלקוחות ובאתרים של מי שענה לפנייה זו.

5. המטה יהיה רשאי לעשות שימוש במדע שיימסר לו במענה לפנייה זו, ולספק לא יהיו טענות בגין זכויות יוצרים.

6. מענה לפנייה זו לא יהווה תנאי להשתתפות במכרז, אם וככל שייערך בעקבותיה, לא יקנה יתרון במכרז למי שנענה לפנייה רק בשל כך שנענה לה, ולא יחייב שיתופו במכרז או התקשרות עמו בכל דרך אחרת.

7. המענה לפנייה יהיה בהיקף כולל של <u>עד 25 עמודים המציגים את המענה, ו-20 עמודים המציגים תכנית בדיקה לדוגמא</u>. בנוסף על כך ניתן לצרף נספחים ומפרטים טכניים ללא הגבלת היקף.

8. המענה יוגש עד ליום 30.06.2016 בשעה 14:00 לידי איש הקשר לפנייה כמפורט להלן. על הספק לוודא כי המסמך התקבל ובשלמותו אצל איש הקשר לבקשה.
9. בראש המענה יירשם: "מענה לבקשה לקבלת מידע (RFI) לתשתיות ושירותים למעבדת בדיקות סייבר לאומית (ספקטרום)".
10. איש הקשר בכל הנוגע לבקשה: גב' מירי זילברשטיין - miris@pmo.gov.il בטלפון: 03-7450810.
11. ספקים רשאים להפנות את שאלותיהם לאיש הקשר עד ליום 31.05.2016 בשעה 14:00. על הספק לוודא ששאלותיו הגיעו בשלמות לאיש הקשר.
12. מענה לשאלות והבהרות יינתן עד לתאריך 07.06.2016 שעה 14:00 על ידי המטה באמצעות העברה לאיש הקשר בחברה.
13. ספק המעוניין להשתתף בתהליך יציג:
    א. תשובה למענה המתייחסת לסעיפים המופיעים לעיל.
    ב. פרטי הספק בטבלה הבאה:

מס"ד	המידע המבוקש	המענה
1	שם הספק	
2	כתובת הספק	
3	מס' טלפון	
4	מס' פקס	
5	שם איש הקשר לבקשה	
6	מס' טלפון של איש הקשר	
7	כתובת דואר אלקטרוני של איש הקשר	

הצגה פרונטלית של המענה

1. לאחר בחינת המענים, המטה שומר לעצמו את הזכות להזמין לפי בחירתו את מי שנענה לפנייה להציג את השירותים בפני צוות מקצועי מטעם המטה, במיקום ובמועד שיקבע המטה.
2. הצגת כל מענה תערך בהיקף של עד שלוש שעות בהן יתבקש המציג להתייחס למתואר במסגרת פנייה זו ולשאלות שיוצגו על ידי הצוות המקצועי מטעם המטה.