



קול קורא לקבלת מידע לארכיטקטורה וטכנולוגיות אפשריות ל"פעולה בטוחה" במרחב הסייבר

מטה הסייבר הלאומי מתכנן פיתוח והקמה של תשתית לאומית שתאפשר ביצוע "פעולה בטוחה" במרחב הסייבר - להלן "מרחב סייבר חסין". מטרתה של פעולה בטוחה לאפשר פניה, בקשה, פקודה או תגובה שאינה ניתנת להתחזות ו/או זיוף ונותנת מענה לאתגרים אלו בתקשורת בין צדדים רחוקים במרחב הסייבר (תיאור מפורט ראו בנספח).

מאפייני הפתרון

המטה מעוניין לעצב פתרון שיתמודד עם ניסיונות ההתחזות ו/או הזיוף בכך שיאפשר פעולה שתעמוד באלה:

1. כל שני צדדים בעסקה מקוונת יוכלו להחליף ביניהם מסרים בצורה אמינה ובטוחה תוך אימות הדדי מלא של זהות הצד שכנגד והבטחת השייך המלא של כל פעולה לכוונת הישות הפיזית/אנושית המחוברת לאותו צד.
 2. הפעולה הבטוחה תהיה מקצה לקצה: בין משתמש אנושי העושה שימוש במחשב (ציוד חישובי נייד או ניח לרבות מחשב, טלפון חכם, טאבלט וכו') לא מאובטח, לבין מערכת המציעה שירות מקוון בתוך האינטרנט.
 3. הנחת העבודה היא שהמשתמש עושה שימוש במחשב ובתווך לא בטוח (ניתן עם זאת להתבסס על ליבת שירות שהיא מאובטחת, ודרישה לרישום מוקדם ייעודי).
- פירוט למרחב הבעיה והפתרון ראו בנספח.

לצורך כך, מבקש המטה לקבל הצעות לארכיטקטורה או רכיבים לפתרונות כאמור.

הפרטים הנדרשים

ככל הניתן, מבוקשים פרטים שיאפשרו בחינת המידע המתקבל לאור תיאור הבעיה

1. מטרת הפנייה לקבל הצעות מגוונות ופורצות דרך, לכן יתקבלו גם מענים עקרוניים ולא מפורטים, ובלבד שהם מתייחסים באופן בהיר לדרישות שהוצגו לעיל, ויסבירו את הפתרון אותו מציע הפונה.
2. הפתרונות יכולים להיות מוצגים באופנים רבים, ויכילו בצורה מלאה או חלקית, אחד או יותר, מהרכיבים הבאים:
 - א. הארכיטקטורה והפרוטוקול המוצעים, את תכולותיהם ואת ההגיונות מאחוריהם, כולל אפיון מפרוט ככל הניתן;
 - ב. אפיון הטכנולוגיות השותפות בכל שלב, קיימות ועתידיות, מאפייניהן והתאמה אפשרית לשלבים שונים בתהליך;
 - ג. הצעה למו"פ (בשלבי התפתחות שונים) למימוש הפתרון המוצע.



3. ביחס להצעה רצוי (אך לא חובה) להתייחס לנושאים הבאים:
- א. **מידת הבשלות של ההצעה:** ניתן לספק מענה לא שלם ובלבד שיתבסס רק על מוצרים קיימים (או טכנולוגיות קיימות) ויהווה צעד בדרך לשלב בו יינתן פתרון מלא שעשוי להתבסס גם על מחקר ו/או פיתוח ייעודיים.
 - ב. **עלות-תועלת:** הערכת מחיר ראשונית לפתרון המוצע (בשלבים השונים), והוכחה לכך שבראיה לאומית החיסכון והתועלת למשק מביצוע פעולות מוגנות, שמירה על פרטיות המידע ובטחון הגלישה ברשת יעלו על עלות הפרויקט.
 - ג. **הסתמכות על מתווך ועזרים חיצוניים:** ניתן להעלות הצעות למימוש שמשמשות בעזרים (כגון Tokens, אozניה לפעולה ביומטרית קולית, שימוש בת"ז חכמה וכו') וגם במתווך מוגן (ראה נספח לפירוט). יחד עם זאת, ישנו יתרון משמעותי לפתרון בעל אי תלות באביזר פיסי, או לכל הפחות שימוש באביזר הקיים בשימוש נרחב בכל מקרה (כמו טלפון חכם עם SIM, לדוגמא).
 - ד. **אחידות ופשטות:** מענה אחוד לאזרחים לנגישות מוגנת לשירותים בתחומים שונים.
 - ה. **סיכונים והתמודדות עמם:** כגון ניהול הסיכון של יצירת נקודת כשל מרכזית וכיצד הפתרון המוצע מתמודד עם בעיה זו.

הוראות כלליות

1. את המענה לקול הקורא יש להגיש למטה הקיברנטי עד ל- 30.6.2015.
2. יתקבלו פניות בכתב בדואר אלקטרוני בלבד, יש לציין בפתח הנייר את פרטי הפונה, תפקידו ופרטי יצירת הקשר עמו.
3. יש לסמן סודות מסחריים שמוצעים במסגרת הפתרון.
4. קול קורא זה אינו בבחינת הזמנה להציע הצעות ואינו חלק מהליכי מכרז, אלא נעשה לשם קבלת מידע בלבד, ובעקבותיו ישקול המטה את המשך פעולותיו.
5. המטה שומר לעצמו את הזכות לפנות בשאלת הבהרה או בפנייה לקבלת מידע או כל נתון אחר למשיבים לקול קורא זה.
6. אין בקול קורא זה כדי ליצור מחויבות כלפי מי מהמשיבים לו, ואין במענה לו כדי ליצור מחויבות כלשהי ו/או יתרון למשיבים לו מכל מין וסוג, והמטה יהיה רשאי לשקול צעדיו ולפעול בהתאם לשיקול דעתו הבלעדי.
7. שאלות ביחס לפנייה זו ניתן להעביר עד ליום 01.06.15.
8. את הפניות יש לשלוח בדואר האלקטרוני לכתובת cyberkol@pmo.gov.il. פרטים נוספים ניתן לקבל בכתובת המייל או בטלפון 03-7450810.



נספח – תיאור מרחב הבעיה והפתרון

מרחב האיומים

שגרת העבודה בין משתמשי קצה (פרטיים או עסקיים) במרחב הסייבר מורכבת מאוסף של טרנזקציות, באמצעות גורמי ביניים מתווכים, שרבים מהם אינם ידועים או חשופים למשתמשי הקצה. לשם ביצוע הטרנזקציה, נדרש המשתמש להוכיח את זהותו ו/או שיש לו הרשאה לבצע את הפעולה המבוקשת, בהתאם להקשר שבו מדובר. דרישה זו ממומשת ע"י ביצוע **אוטנטיקציה** (אימות זהות) כשלב מקדים ל**טרנזקציה**.

ניתן להבחין בשתי משפחות איומים על פעולות האוטנטיקציה והטרנזקציה המתבצעות ברשת:

1. **התחזות** - פעולת סייבר שבוצעה לא על ידי הגורם האוטנטי שבשמו ובזהותו נעשית הפעולה וללא ידיעתו ורצונו באמצעות שימוש בפרטים מזהים חוקיים. סיבות נפוצות לכך הן פרטים מזהים שנגנבו, הועתקו, הוצאו במרמה או יוצרו באופן לא מורשה, תוך ניצול חולשה בהם, בתהליכי ההזדהות או בקרב משתמשים לא זהירים ו/או נטולי כלים, למשל באחת הדרכים הבאות:

- א. **ניחוש ו/או פיצוח סיסמאות;**
- ב. **פריצה, גניבה ו/או שחזור של מאגרי רשימות משתמש-סיסמא, מאפיינים מזהים, מספרי כרטיסי אשראי וכו';**
- ג. **גניבת cookies;**
- ד. **מתקפות פשינג (דיוג) למיניהן;**

2. **זיוף / ניצול לרעה** - ביצוע או שינוי פעולות סייבר שלא על ידי הגורם האוטנטי שביצע את הפעולה וללא ידיעתו ורצונו באמצעות התערבות בתווך (או במחשב המשתמש) במהלך "שיחה אוטנטית" ("רכיבה" על session מאומת) וניצול הזיהוי ההדדי שביצעו הצדדים הלגיטימיים זה לזה מבעוד מועד, למשל באחת הדרכים הבאות:

- א. **מתקפות העושות שימוש בכלי RAT;**
- ב. **מתקפות בסגנון Man in the Middle על תוך ה-SSL תוך שימוש בסרטיפיקטים מזויפים לא מחשידים.**

לגניבת זהות המשתמש ישנו כמובן פוטנציאל נזק רב:

באופן ישיר - כל פעולה בעלת משמעות כספית (קניה, ביצוע תשלום, העברת כספים וכו').

באופן כמעט ישיר - כל פעולה שגרמה לחשיפה ו/או אובדן/שינוי של מידע פרטי/אישי/עסקי ו/או כל פעולה שהשפיעה על העולם הפיזי לרעה.

באופן עקיף - כל פעולה שיצרה השפעה על עמיתים של המשתמש שנסמכו על מידע שהועבר אליהם לכאורה בשם בעל הזהות האמיתי.

מרחב הפתרון

במרחב הסייבר החסין יוכלו כל שני צדדים בעסקה מקוונת, המוכרים למערכת, להחליף ביניהם מסרים בצורה אמינה ובטוחה תוך אימות הדדי מלא של זהות הצד שכנגד **והבטחת השיוך המלא של כל פעולה לכוונת הישות הפיזית/אנושית המחוברת לאותו צד**. באופן זה כל פעולה תתבצע אם ורק אם הייתה בכוונת המשתמש, תבוצע בדיוק כיצד שרצה המשתמש וללא ספחים נוספים, קרי אך ורק מה שתכנן המשתמש.

הפעולה הבטוחה תהיה מקצה לקצה: בין משתמש אנושי העושה שימוש במחשב (צידוד חישובי נייד או ניח לרבות מחשב, טלפון חכם, טאבלט וכו') לא מאובטח, לבין מערכת המציעה שירות מקוון בתווך האינטרנט.

מגוון השימושים האפשריים לשירות: תשלומים, שירותים ממשלתיים, שירותי מסחר, גישה למידע אישי/מסחרי וכו'

המענה לקול הקורא יכול הצעה לארכיטקטורה, כיווני פעולה ו/או שיטות אשר יאפשרו לממש את חזון מרחב הסייבר החסין באופן אקטיבי, יעיל ובטוח. ניתן להציע פתרונות שיורכבו מטכנולוגיות קיימות וגם מטכנולוגיות עתידיות אפשריות (עם או בלי מו"פ ייעודי).

הגדרות:

1. **פעולה בטוחה:** פניה, בקשה, פקודה או תגובה שאינה ניתנת להתחזות, זיוף/ניצול לרעה.

הנחות היסוד בהצעת הפתרון (מצ"ב תרשים):

1. **משתמש ותווך לא בטוח:** כל המחשבים בשרשרת ההתקשרות משתמש-ספק מודבקים בפוגענים, כולל פוגענים בעלי יכולת שליטה ותקשורת Real Time, למעט שרתי הליבה של ספק השירות.
 2. **ליבת ספק מוגנת:** ליבת המחשוב בספק השירות, שהוא ה"צד השני" בפעולה, הינה אמינה ונקייה מפוגענים שעשויים להפריע לתהליך (זוהי הנחת היסוד להתמודדות עם צירי התקיפה הרלוונטיים לקול קורא זה, על אף שהיא אינה טריוויאלית בשל הקשיים הטכנולוגיים ביסודה).
- מרכיבים אפשריים בהצעת הפתרון (מצ"ב תרשים):

1. **מתווך:** בבניית הארכיטקטורה ניתן להציע פתרון בו קיים גם מתווך לפעולה, שגם ליבתו מוגנת. המתווך יכול להיות משולב בכל שלב בתהליך (החל מזיהוי ראשוני מולו וכלה בשימוש רציף לאורך הדרך), ויכול גם לא להיות משולב כלל בתהליך.
 2. **חומרה ייעודית:** ניתן להוסיף חומרה ייעודית (כגון Tokens, אוזניה לפעולה ביומטרית קולית, שימוש בת"ז חכמה וכו') אם ניתן להוכיח שהסבירות לתקיפתה הינה זניחה.
- אי לכך ובהתאם לזאת האתגר העיקרי הינו היכולת להמחיש שבפתרון מוצע שפועל תחת הנחות היסוד ניתן ליצור קשר אמין בין המשתמש האנושי וליבת ספק השירות ללא יכולת התחזות וזיוף/ניצול לרעה ע"י גורם אחר.

