מערך הסייבר הלאומי

<u>פניה מוקדמת לקבלת מידע (RFI)</u>

<u>מס' 0205/2023</u>

<u>בנושא: שירות Protective DNS (PDNS)</u>

מאי 2023

פנייה מוקדמת לקבלת מידע (RFI) בנושא:
שירות Protective DNS (PDNS)

1. רקע ומטרת הפנייה

1.1 מערך הסייבר הלאומי מעוניין לקבל מידע בדבר שירות Protective DNS (PDNS) בתצורת ענן (SaaS) שיהווה מרכיב במטריית ההגנה למשק המכונה "כיפת הסייבר" ויאפשר יישום הגנה ברמת מדינה בשכבת פרוטוקול ה-DNS.

1.2 מטרת השירות הינה העלאת חוסן המשק באמצעות מניעת גישה לדומיינים זדוניים לטובת גלישה בטוחה באינטרנט.

1.3 במסגרת פניה זו מעוניין מערך הסייבר הלאומי לבחון, בין השאר, את האפשרות להפעלת השירות באופן פנימי וכן לאפשר לארגונים ולמשתמשים במשק להפעיל שירות זה, ברמת המגזרים השונים, תשתיות מדינה קריטיות ועוד כך שכל משתמש ו/או ארגון יוכל לתפעל את השירות באופן עצמאי וישיר (כולל רישום לשירות). מערך הסייבר הלאומי יוכל לתפעל את השירות עבור המערך עצמו וכן לנהל, ברמת ניהול-על, את השירות עבור קבוצות ארגונים מסויימות, בהיבטים שונים (למשל, מדיניות בסיס הנדרשת להגנה) במקביל לתפעול שוטף של הארגונים עבור עצמם.

2 כללי

2.1 פנייה זו הינה פנייה מוקדמת **לקבלת מידע** בהתאם לתקנה 14א לתקנות חובת המכרזים, תשנ"ג – 1993. אין בה כדי ליצור מחויבות כלשהי כלפי מי מהמשיבים ו/או לראות בה התקשרות משום סוג. הפנייה נועדה לקבלת מידע בלבד ובעקבותיה ישקול המערך את המשך פעולותיו בהתאם לשיקולים מקצועיים ועניינים.

2.2 אם וככל שיתקיים מכרז או הליך רכש אחר בעתיד, יהא רשאי המערך לשנות או להוסיף תנאים ודרישות, הכל לפי שיקול דעתו המקצועי ובהתאם לצרכיו.

2.3 המערך יהא רשאי לעשות שימוש במידע שיימסר לו במענה לפנייה זו, ולספק לא יהיו טענות בגין זכויות יוצרים.

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

2.5 ניתן לעיין ולהוריד את המסמכים המלאים של הבקשה לקבלת מידע באתר האינטרנט של מנהל הרכש הממשלתי בכתובת: https://www.mr.gov.il/Pages/HomePage.aspx או באתר האינטרנט של מערך הסייבר הלאומי בכתובת: http://cyber.gov.il.

2.6 להלן טבלת ריכוז התאריכים לפנייה זו:

הפעילות	תאריך	שעה

מועד פרסום הפנייה	2.5.2023	14:00
המועד האחרון להמצאת שאלות הבהרה מן הספקים	14.5.2023	12:00
מועד המענה של המשרד לשאלות ההבהרה	23.5.2023	12:00
המועד האחרון להגשת מענים	30.5.2023	12:00

3 מושגי יסוד:

3.1 **שירות אבטחה Protective DNS (PDNS) -** שירות המנתח שאילתות / בקשות תרגום DNS (Queries) ונוקט פעולות להתמודדות עם איומים תוך שימוש בפרוטוקול DNS והארכיטקטורה הקיימים. השירות מונע גישה לנוזקות, כופרות, התקפות דיוג, וירוסים, רוגלות, גישה ו/או שימוש בתקשורת ו/או אתרים זדוניים ועוד.

3.2 **מזהה** – פריט זיהוי, לדוגמה דומיין (Domain), כתובת IP וכו' שניתן לבדוק בחשד לפעילות זדונית ו/או לחסום גישה אליו.

4 מפרט דרישות

במסגרת RFI זה מבקש מערך הסייבר הלאומי (להלן: "**המערך**") לקבל מידע על אודות שירות שמספק מענה כמפורט להלן.

יובהר כי הפתרון המבוקש נועד להשתלב בארגונים בעלי מאפיינים שונים במשק (תשתיות, גופי ממשל, גופי תעשייה ועוד) בהתאם לצרכים ומאפייני הארגון וקבוצת ארגונים.

4.1 **המשיב יפרט בדבר יכולות השירות בהתייחס להיבטים הבאים:**

4.1.1 האם השירות הינו SaaS?

4.1.1.1 האם למשיב קיימת יכולת להפעיל את השירות על-בסיס תשתיות הענן שנבחרו במכרז "נימבוס" (מכרז מרכזי 01-2020 לאספקת שירותי ענן על גבי פלטפורמה ציבורית עבור משרדי הממשלה ויחידות הסמך), AWS או GCP והאם המשיב יכול להקים מרכז נתונים ב-Region הישראלי של תשתיות הענן שנבחרו במכרז "נימבוס" על-מנת לספק את השירות ממנו?

4.1.1.2 במידה והתשובה הינה שלילית, כמה זמן יידרש על-מנת להקים את השירות כמתואר לעיל?

4.1.1.3 ניתן להתרשם מדרישות הממשלה בהיבטי הגנה בסייבר, פרטיות, תנאי שימוש, אחסון ועיבוד מידע וכן דרישות נוספות בהיבטי אבטחת מידע ביחס לעבודה בענן, אשר הפתרון

המוצע נדרש לעמוד בהן, בהתאם לפירוט הקיים במכרז המרכזי להוספת שירותים לשוק הדיגיטלי הממשלתי בענן, אשר נערך במסגרת פרויקט נימבוס ומסמכיו מפורסמים באתר מינהל הרכש בקישור הבא:

https://mr.gov.il/ilgstorefront/he/p/4000553566

4.1.2 מהו מנגנון החסימה המופעל במסגרת השירות ומהן אפשרויות המענה שיוכל המשתמש לקבל במקרה של חסימה (הודעת חסימה כללית, ייעודית, מותאמת ע"פ צרכי הלקוח, הפניה לשרת מסויים ועוד).

4.1.2.1 האם ניתן לבצע שינוי/עדכון במדיניות החסימה של משתמש מסוים מבלי שתהיה לכך השפעה על משתמשים אחרים?

4.1.2.2 האם ניתן לבצע שינוי/עדכון במדיניות החסימה של משתמש מסוים מבלי שהשינוי ייחשף בפני משתמשים אחרים ו/או ניתן יהיה לבחור בפני מי ייחשף השינוי?

4.1.2.3 האם השירות מאפשר חשיפת השינוי במדיניות החסימה של ארגון מסויים גם לארגון ממונה עליו (למשל, מערך הסייבר הלאומי)?

4.1.2.4 האם ניתן להגדיר כי משתמש-על (משתמש שממונה על ארגונים אחרים) לא יהיה חשוף לעדכון מדיניות חסימה של משתמש? האם קיימת גמישות בחסימת החשיפה לעדכונים מסויימים בלבד?

4.1.2.5 האם השירות עושה שימוש במידע ובפידים מודיעיניים (Intelligence Feeds) להעשרת מידע כבסיס לעדכון מדיניות החסימה?

4.1.2.6 מהו המידע ומהם הפידים המודיעיניים המשמשים להעשרה?

4.1.2.7 האם קיימת אפשרות להוספת פידים מודיעיניים הן ע"י המשיב והן ע"י המשתמש ובאיזה אופן?

4.1.2.8 מהו מספר המזהים (כמות) שאותם ניתן לטעון לשירות כחלק מפיד מודיעיני במטרה לעדכן את מדיניות החסימה?

4.1.2.9 האם ניתן להגדיר מזהה במצב ניטור בלבד או שברגע שטוענים אותו לשירות מתבצעת אכיפה / חסימה בהתאם?

4.1.2.10 כיצד נקבעת רמת הסיכון של מזהה / פיד מודיעיני שהוזן לשירות (מהי הנוסחה)? על-בסיס מה מבוצעת החלטה אודות חסימה / התרעה (למשל, מהו סף רמת הסיכון) והאם ניתן לשינוי ע"י המשתמש?

4.1.3 האם השירות מאפשר בדיקת דומיינים חשודים באופן ידני ו/או אוטומטי וכיצד?

4.1.4 כיצד מזהה השירות כי שאילתת ה-DNS (DNS Query) מגיעה מארגון מורשה (ארגון העושה שימוש בשירות ה-PDNS)?

4.1.5 כיצד מבצע השירות Threat Intelligence ו-Threat Hunting? האם קיימת מתודולוגיה לכך?

4.1.6 האם השירות מאפשר שימוש בכתובות IPV4 וגם IPV6 ובדומיינים בהתאם?

4.1.7 מהן הנוזקות וההתקפות האפשריות שאותן מזהה השירות וכיצד מתמודד איתן (למשל, כופרות, וירוסים, רוגלות, דיוג, תשתית פיקוד, הזלגה ועוד)?

4.1.8 האם במסגרת השירות עלולים להיחסם גם קבצים שהמשתמש מעלה לאינטרנט או מוריד מהאינטרנט?

4.1.9 האם השירות שומר ו/או מאפשר שמירת כלל המידע הנוצר ומעובד בו?

4.1.9.1 אילו סוגי מידע נשמרים? למשל, כל נתוני הגלישה ל- IP או דומיין או חלקם? אילו לוגים נשמרים? האם נשמרים קבצים שעולים לאינטרנט על ידי המשתמש? האם נשמרים שמות הקבצים שעולים לאינטרנט?

4.1.9.2 היכן נשמר המידע?

4.1.9.3 לכמה זמן נשמר המידע?

4.1.9.4 האם ניתן לייצא מידע זה ובאיזה אופן? האם ניתן לסנן את המידע המיוצא בהתאם לבקשת המשתמש? האם קיימות אפשרויות שונות בהקשר זה?

4.1.9.5 האם ניתן להגדיר מראש כי משתמש-על לא יהיה חשוף למידע מסוג מסוים? (מהיבטי שמירה על פרטיות) אם כן, יש לפרט את האפשרויות השונות.

4.1.9.6 לאילו מערכות ניתן לייצא את המידע ללא צורך בהתאמה?

4.1.9.7 האם קיים מדרג הרשאות גישה למערכת המייצאת את המידע למשתמשים?

4.1.9.8 יש לצרף למענה דוגמאות לקבצי לוגים והתרעות שהשירות מפיק.

4.1.10 האם השירות כולל מנגנונים או ארכיטקטורה שמטרתה לעמוד בדרישות הגנת פרטיות (privacy by design)?

4.1.11 האם קיימת לשירות יכולת Fail Safe "שקופה" למשתמש, כך שאם חל כשל מהותי באספקת השירות, ניתן יהיה לעבור לתצורת עבודה רגילה ללא השבתה תפעולית. במידה וקיימת יכולת זו, האם המעבר לתצורת העבודה ללא השירות תחייב את הארגון לבצע שינויים מצדו?

4.1.12 האם השירות מבסס את מדיניות החסימה על המידע המצטבר בו ו/או מידע מפידים מודיעיניים חיצוניים ו/או אחר ובאיזה אופן?

4.1.13 כיצד מתגונן השירות בפני מתקפות DDOS על השירות עצמו כולל התייחסות לסוגי המתקפות עצמן ולמספר בקשות לפרק זמן ו/או קצב נפח לפרק זמן המשמשים כבסיס לתקיפה?

4.1.14 האם השירות מאפשר איתור כתובת ה-IP ברמת רשת הארגון (IP פנימי) שממנה הגיעה בקשת הגלישה (DNS Query)? האם השירות מאפשר איתור שם משתמש בתוך הארגון שממנו הגיעה בקשת הגלישה?

4.1.14.1 אם כן, כיצד והאם יכולת זו מופעלת באופן אוטומטי או ידני (לבחירת המשתמש)?

4.1.14.2 האם נדרש להתקין רכיב תוכנה כלשהו בתוך רשת הארגון למטרה זו?

4.1.15 האם השירות מספק פתרון למצב שבו קיים נתק תקשורתי בין מדינת ישראל לבין העולם ומהו?

4.1.16 באילו פרוטוקולים תומך השירות?

4.1.16.1 האם השירות תומך במתן שירותי DNS over HTTPS (DoH)?

4.1.16.1.1 יש לפרט כיצד מממש השירות את התמיכה ומתמודד עם DoH.

4.1.16.1.2 במקרה שהשירות לא מתמודד כיום עם DoH, האם מתוכננת תמיכה עתידית כזו במסגרת שירות ה- PDNS ומתי?

4.1.17 באילו רשומות של שאילתת ה-DNS תומך השירות?

4.1.18 האם השירות תומך בעבודה מרחוק (Roaming Clients) ובאיזה אופן? מהם ה- Best Practices בעת עבודה עם משתמשים הנמצאים בבית (BYOD)?

4.1.19 מהם ה-Best Practices בעת עבודה עם ארגונים שיש להם סביבת ענן ציבורית?

4.1.20 מהו מבנה ממשקי ניהול ברמות ארגוניות שונות (משתמש, ארגון, קבוצת ארגונים)?

4.1.21 האם השירות תומך בשימוש ב White Labeling Domain / URL כך שבעת גישה של משתמש לשירות ה-PDNS מתוך פורטל פנימי של הארגון, העושה שימוש בשירות (למשל מערך הסייבר הלאומי), יראה המשתמש בשורת הדפדפן שהוא עובד עם דומיין של הארגון ולא של המשיב?

4.1.22 מהן ההרשאות הניתנות בכל רמה ארגונית?

4.1.23 אפשרויות הדו"חות הניתנים להפקה במסגרת השירות.

4.1.24 אפשרויות ההתרעות הנשלחות ע"י השירות.

4.1.25 אפשרויות השימוש ב- API וכלל הנתונים הניתנים להעברה באמצעותו.

4.1.26 אפשרויות האינטגרציה של השירות עם מערכות וכלים של צד ג'.

4.1.27 אפשרויות הפיתוח וההתאמה של השירות ואופן יישומן.

4.1.28 התקנים הבינלאומיים בהם עומד השירות.

4.1.29 אפשרויות הפעלת שירותי מומחים (אנליסטים וכו') בנוסף לשימוש בשירות.

4.1.30 אפשרויות הטמעה ותמיכה בהגדרות למיצוי השירות (למשל, תמיכה בהתאמת התשתיות הקיימות בארגון לשימוש בשירות, כגון הגדרות FireWall וכד').

4.1.31 מודל התמיכה, השירות, ההדרכה וזמני התגובה (SLA).

4.1.32 מאפייני אבטחת המידע של השירות.

4.1.33 האם קיים מודל לשיתוף המשק כשירות הגנה בסיסי ללא תשלום?

4.1.34 בנוסף למענה המבוקש כמפורט לעיל, המשיבים רשאים להציג יכולות ושירותים נוספים ו/או משתלבים (לדוגמה שירות הגנה בפני התקפת DDoS על המשתמש / הארגון) וכן תפיסה ורעיונות קיימים ועתידיים.

4.2 **<u>המשיב יפרט בדבר פרטי החברה המשיבה:</u>**

4.2.1 האם החברה המשיבה היא החברה המפתחת את השירות והבעלים שלו?

4.2.2 האם ההטמעה והתמיכה בשירות ניתנות ישירות ע"י החברה המשיבה? אם לא, מי מספק את ההטמעה והתמיכה?

4.2.2.1 מהו מודל ההטמעה, כיצד ועל ידי מי הוא מתבצע?

4.2.2.2 מהו מודל התמיכה, כיצד ועל ידי מי הוא מתבצע?

4.2.3 האם לחברה המשיבה יש מרכז פיתוח ו/או תמיכה בישראל?

4.2.4 כמה לקוחות משלמים קיימים לשירות?

4.2.5 האם חלק מהלקוחות המשלמים הם לקוחות פיננסיים ו/או ממשלתיים? אם כן, כמה והאם בישראל? במשך כמה שנים?

4.2.6 כמה זמן נמצא השירות בשוק, בשימוש של הלקוחות המשלמים המפורטים לעיל, בארץ ובעולם?

4.2.7 מהו מודל התמחור, תוך התייחסות לתכולת רישיון לשימוש בשירות:

4.2.7.1 מה כולל רישיון למשתמש ובאילו כמויות (כמות נקודות קצה, ארגון ע"פ טווח נקודות קצה, שימוש בפועל של נקודות קצה ו/או כמות בקשות תרגום לפרק זמן ועוד)?

4.2.7.1.1 האם קיימת הגבלה של כמות שאילתות (DNS Queries) לכתובת IP ספציפית?

4.2.7.2 כמה ארגונים נכללים ברישיון למשתמש?

4.2.7.3 כמות הארגונים המקסימלית לניהול במסגרת רשיון בשירות (ברמת ניהול-על), אם קיימת.

4.2.7.4 האם קיימות מדרגות תמחור עבור כמויות שונות של רישיונות למשתמשים? מהי הערכת העלות במדרגות השונות?

4.2.7.5 במידה והתשובה לאחד משני הסעיפים, הנוגעים להפעלת השירות על-בסיס זוכות מכרז "נימבוס" ומרכז נתונים ב-Region הישראלי, לפחות, הינה שלילית, מהי העלות למימוש הפעלת השירות באופן זה? במידה ונושא זה יהווה תנאי לאספקת השירות למשרדי ממשלה בישראל, מהו הפתרון המוצע ע"י המשיב?

4.2.7.6 כיצד מתומחרות שעות פיתוח בהתייחס למשימות ייעודיות ולפרוייקטים שלמים?

4.2.7.7 כיצד מתומחרות שעות Professional Services (PS)?

4.2.7.8 האם ניתן לתמחר פרוייקט התממשקות למערכות ולפורטלים חיצוניים לשירות ע"פ דרישות הלקוח ומה מנגנון התמחור?

4.2.7.9 האם ניתן לתמחר פרוייקט פיתוח ע"פ דרישות הלקוח ומה מנגנון התמחור?

4.2.7.10 האם קיימים שירותים נוספים, שלא כלולים ברישיון, ומה מחירם?

4.2.8 האם קיימים מסמכים המפרטים תנאי שימוש בשירות ותנאי התקשרות? אם כן, נא לצרפם.

4.2.9 המשיב רשאי להוסיף כל מידע רלוונטי נוסף בהקשרים אלה.

5 <u>המענה המבוקש</u>

על ההצעות לתת מענה המתייחס לכל אחת מהדרישות המפורטות בסעיף 4 לעיל, ובכלל זה לכלול התייחסות לנושאים הבאים:

5.1 עבור כל ההצעות:

5.1.1 הצגת יכולות כמפורט בסעיף 4.

5.1.2 היצע פתרונות עם יכולת התאמה לארגונים שונים – גודל, סיווג (בלמ"ס, מסווגת, תפעולי) ומבנה רשתות פתוח / סגור.

5.1.3 קלות התקנה, תפעול ועדכון.

5.1.4 הצעות או רעיונות בדבר הקמת התשתיות, הכלים או המערכות הנדרשות למימוש הדרישות מהמערכת המוצעת.

5.1.5 בנוסף למענה המבוקש כמפורט לעיל, המשיבים רשאים להציג גם תפיסה ורעיונות קיימים ועתידיים וכן שירותים נוספים המרחיבים את המענה הכולל.

6 אופן הגשת שאלות הבהרה ומענה לפנייה זו

6.1 איש קשר

איש/אשת הקשר מטעם המערך בנוגע לפנייה זו הוא/היא שרון בוסידן,
דוא"ל cyber-michrazim@cyber.gov.il

6.2 שאלות הבהרה

6.2.1 שאלות הבהרה בנוגע לפנייה זו יש להגיש בכתב בלבד, לא יאוחר מהמועד האחרון להמצאת שאלות הבהרה כמפורט בטבלה שבסעיף 2.6 ,
לאיש/אשת הקשר בדוא"ל cyber-michrazim@cyber.gov.il.
על הספק לוודא ששאלותיו הגיעו בשלמות לאשת הקשר, בטל' **072-3388578**.

6.2.2 המערך שומר לעצמו את הזכות לנהל סבב אחד או יותר של שאלות הבהרה בהתאם לשיקול דעתו הבלעדי.

6.2.3 שאלות ההבהרה יוגשו בשפה העברית או האנגלית, במבנה הבא:

מספר הסעיף בפנייה	פירוט השאלה

6.2.4 מענה לשאלות ההבהרה יועבר על ידי המערך אל הפונים, וכן יפורסם באתר האינטרנט של מינהל הרכש הממשלתי ושל מערך הסייבר הלאומי בכתובות המפורטות בסעיף 2.5 לעיל. מובהר כי תשובות ההבהרה ינוסחו באופן שאינו חושף את זהות השואלים.

6.3 <u>הגשת מענה לפנייה</u>

6.3.1 המענה לפנייה יהיה **<u>בשפה העברית או האנגלית</u>**, בהיקף כולל של עד 50 עמודים המציגים את המענה. בנוסף על כך ניתן לצרף נספחים ומפרטים טכניים ללא הגבלת היקף.

6.3.2 את המענה לבקשה לקבלת מידע יש להגיש בעותק דיגיטלי עד למועד האחרון להגשת מענים המפורט בטבלה שבסעיף 2.6 לעיל באמצעות תיבת דוא"ל Cyber-Michrazim@cyber.gov.il. ולוודא אישור קבלה בטל' **072-3388578** בנושא הדוא"ל יירשם: "פניה מוקדמת לקבלת מידע (RFI) בנושא שירות Protective DNS (PDNS)".

6.3.3 המערך רשאי לדחות את המועד האחרון להגשת מענה לפי שיקול דעתו הבלעדי. הודעה על כך תישלח לכל מי שהשיב לפנייה, וכן תפורסם באתר האינטרנט של מינהל הרכש הממשלתי ושל המערך בכתובות המפורטות בסעיף 2.5 לעיל. בהודעה יצוין המועד החדש להגשת המענים.

6.3.4 במסגרת המענה יפורטו פרטי המשיב:

מס"ד	המידע המבוקש	מענה
1	שם המשיב	
2	כתובת המשיב	
3	מס' טלפון	
5	שם איש קשר מטעם המשיב	
6	מס' טלפון של איש הקשר	
7	כתובת דואר אלקטרוני של איש הקשר	

7 <u>בדיקת המענה</u>

7.1 המערך שומר לעצמו את הזכות לפנות, ככל שיידרש, למשיבים לפנייה זו בבקשה להשלמת מידע והבהרות, להצגת מצגות והדגמות, לביקור באתרי הלקוחות ובאתרים של מי שהשיב לפנייה זו, בהתאם לשיקול דעתו של המערך.

7.2 במסגרת בחינת המענים, המערך שומר לעצמו את הזכות להזמין את כל מי שנענה לפניה, להציג את הפתרון המוצע על-ידו בפני צוות מקצועי מטעמו במיקום ובמועד שיקבע המערך.

7.3 במסגרת בחינת המענים, המערך שומר לעצמו את הזכות להזמין את המשיבים לקיים פיילוט שמשכו עד חודשיים. יובהר כי המערך שומר לעצמו את הזכות להזמין רק חלק מהמשיבים לקיום פיילוט כאמור, בהתאם לשיקול דעתו הבלעדי, בהתאם לצרכיו ויכולותיו של המערך וזמינות המשיבים.