

מפרט: לאספקת שירותי גישה לאינטרנט

1. כללי

- 1.1 משטרת ישראל מעוניינת לקבל סל שירותים בתחום הגישה לרשת האינטרנט, הסל כולל:
- 1.1.1 **קווי גישה ל- ADSL,+vdsl - קווים בשירות "אינטרנט מהיר", כיום במשטרה קיימים קווים של "בזק החברה הישראלית לתקשורת בע"מ".**
 - 1.1.2 **קווי גישה ל- IPVPN – קווים על רשת ה-MPLS של חברת "בזק החברה הישראלית לתקשורת בע"מ".**
 - 1.1.3 **קווי גישה לתמסורת מטר-אטרנט – קווים המבוססים על טכנולוגיה Ethernet Layer 2 של חברת "בזק החברה הישראלית לתקשורת בע"מ".**
 - 1.1.4 **קישורים-תשתית קווית או סלולרית או אלחוטית פעילות לשירותי אינטרנט.**
 - 1.1.5 **תשתית כבלים – גישה מבוססת על תשתית כבלים כדוגמת תשתית הכבלים של חברת "HOT".**
- 1.2 הזוכה לא יבצע שינויים במערכת ללא קבלת אישור בכתב ומראש מטעם נציג מדור תקשוב במשטרה.
- 1.3 הזוכה יתאים את הרשת אותה הוא מפעיל, ללא תמורה ועל חשבון, לתקנים, נהלים, פרוטוקולים ויישומים אשר יהיו מקובלים ברשת האינטרנט במהלך כל תקופת ההתקשרות.

2. רקע

- 2.1 במשטרת ישראל הוקמה רשת פנימית לטובת האינטרנט – "מירי". רשת זו הינה רשת נפרדת ואינה מקושרת לרשתות אחרות. כל אתרי המשטרה מקושרים למרכז רשת אחד אשר נמצא במתקן יהודאי בירושלים.
- 2.2 משטרת ישראל תספק קישור רחב סרט לזוכה ממתקן יהודאי עבור שירותי האינטרנט (גלישה, דוא"ל וכד'). רוחב הפס של קישור זה עשוי להשתנות מעת לעת בהתאם לצורכי משטרת ישראל.
- 2.3 בנוסף, ישנן מס' יחידות ברחבי הארץ אשר אינן מחוברות לרשת זו ואשר יצטרכו חיבור נפרד, (כגון ADSL כבלים וכו') ישירות לזוכה, לצורך שירותי גישה לאינטרנט.
- 2.4 הקישור בפועל של המזמין נעשה בהתאם לסדרי העדיפות הפנימיים במשרד והמגבלות הטכנולוגיות, התקציביות והאבטחתיות הרלוונטיות לביצוע החיבור.

3. גורמים משיקים למערכות.

- 3.1 אין חיבורים בין רשת "מירי" לרשתות אחרות.
- 3.2 על רשת האינטרנט של מ"י (רשת "מירי") יוגדרו אמצעי קצה עם כתובות IP תקפות עפ"י הצורך.

4. תיאור השירותים הנדרשים

4.1. השירות הבסיסי הנדרש כולל:

- 4.1.1. מנוי חודשי בלתי מוגבל לקו IPVPN/תמסורת מטרו ראשי סימטרי הכולל 3000 תיבות דואר אלקטרוני. התשתית תוזמן ע"י מ"י.
- 4.1.2. גיבוי קר לקו ה-IPVPN/תמסורת מטרו הראשי במהירות זהה (הגיבוי יופעל רק במידה והקו הראשי יושבת). תשתית הגיבוי תוזמן ע"י מ"י.
- 4.1.3. מנוי חודשי לקווי ADSL / כבלים הכולל תיבות דואר אלקטרוני.
- 4.1.4. העברה תיבות הדואר של Domain Police.gov.il מספק השירות הקיים וניהולן תוך כדי שמירה על התיבות הקיימות.
- 4.1.5. תחום של 100 כתובות IP תקפות.
- 4.1.6. לפחות 3000 תיבות דואר אלקטרוני.

4.2. שירותים נוספים

- 4.2.1. שירותי האינטרנט אותם יספק הזוכה רק באישור נציג מדור תקשוב למזמין בנוסף לשירות הבסיסי, כמפורט להלן:
- 4.2.2. הגדלת נפח מנויי האינטרנט (ISP בלבד) עד 1 ג'יגה (כרגע 200 מגה)
- 4.2.3. הגדלת נפח תיבות הדואר עד 2 ג'יגה (כרגע 1 ג'יגה)
- 4.2.4. הגדלת כמות כתובות ה-IP התקפות, עד 150 (כרגע 100)

4.3. ניתוב לכל כתובת IP תקפה

- 4.3.1. הציוד והתוכנה שיפעיל הזוכה לצורך אספקת שירותי האינטרנט, יאפשרו ניתוב על פי דרישת המשתמש ע"י הפעלת שני שרתי שמות מלאים בלתי תלויים.
- 4.3.2. הזוכה מפעיל לפחות שני שרתים, היכולים לתרגם שמות (Domain Names) לכתובות IP, כאשר כל אחד מהם מחזיק את מלוא מרחב השמות ברשת והם מגבים האחד את השני.

4.4. תמיכה בכל הפרוטוקולים המקובלים

- 4.4.1. רשת הזוכה תתמוך בכל הפרוטוקולים המקובלים ברשת האינטרנט, ובפרט בפרוטוקולים ממשפחת TCP/IP ופרוטוקולים המוגדרים כ- RFC תקפים.

4.5. תמיכה בכל שירותי האינטרנט

- 4.5.1. רשת הזוכה תתמוך בכל טווח שירותי האינטרנט ובכלל זה גלישה, העברת קבצים (FTP), קבוצות דיון, CHAT, שירותי דואר, קול ווידאו.

4.6. אספקת שירותי דואר

- 4.6.1. רשת הזוכה תתמוך בכל פרוטוקולי הדואר האלקטרוני המקובלים ברשת האינטרנט ותיתן שירות אמין של ניתוב והעברת הודעות מכל הסוגים.

4.6.2 חבילת השירות תכלול תיבת דואר אלקטרוני : שתסופק על ידי הזוכה במפרט הבא :

4.6.2.1 במסגרת השירות, יועברו לאחריות הזוכה ניהול ה-Domain וניהול התיבות של Police.gov.il. הזוכה נדרש לשמר Domain זה כולל החשבונות הקיימים כיום. באם יתאפשר, הזוכה ישמר גם את הסיסמאות הקיימות.

4.6.2.2 הזוכה יקצה לכל משתמש כתובת דואר אלקטרוני ברשת הזוכה. לכל כתובת תוקצה מחיצת נפח דיסק של לפחות 1000 MB לקבלת דברי דואר במסגרת השירות הבסיסי. כמו כן יתאפשר למשתמש קידום אוטומטי יזום (forward) של דברי הדואר לכל כתובת תקפה שיספק המשתמש. במקרה של ביטול חשבון/משתמש, מתחייב הזוכה לנתב את הדואר האלקטרוני המגיע לכתובת זאת לכתובת חדשה שיספק המשתמש במשך 90 יום ממועד הביטול. למשתמש תתאפשר שליחת דבר דואר כולל צרופה בגודל של עד M10.

4.6.3 למשתמש המחזיק כתובת דואר אלקטרוני משלו, ייתן הזוכה שירותי ניתוב מלאים לדברי הדואר האלקטרוני, ובלבד שהמשתמש מסר את הפרמטרים הטכניים הנדרשים למוקד הסיוע של הזוכה.

4.6.4 הזוכה יספק שירותי סינון דואר anti virus+SPAM

4.7 הפעלת מערך אבטחת מידע

4.7.1 הזוכה יתפעל מערך מקיף לזיהוי, מניעה והתראה של בעיות אבטחת מידע ברשת הזוכה ויש לו יכולת טיפול מיידיית בבעיות אבטחת המידע המתגלות, ובפרט בבעיות המפורטות להלן (על הזוכה להראות יכולת המבטיחה נטרול מיידי של ההתקפה, זיהוי המתקיף וניתוקו):

4.7.1.1 ניסיון פריצה של מנוי מרשת האינטרנט למנוי משטרת.

4.7.1.2 גילוי ועצירת התקפות הבאות :

4.7.1.2.1 Distributed Denial of Service (DDoS) בכל הרמות (Layer3-) המפריעות לעבודה השוטפת של משתמשי המשטרה מול רשת האינטרנט, לרבות תמיכה ב:

4.7.1.2.2 התקפות נפח (Volumetric Attacks)

4.7.1.2.3 התקפות (TCP State Exhaustion Attacks)

4.7.1.2.4 התקפות אפליקציה (Application Layer Attacks)

4.7.1.2.5 התקפות וירוסים והתקפות (Mass Email Attacks) על כתובות דואר אלקטרוני של המשטרה

4.7.1.2.6 התקפות DDoS על שרתי DNS (Domain Name Server)

4.7.1.2.7 התקפות מרשת המציע לכיוון רשת המשטרה/אתרי המשטרה

4.7.1.3 יכולת גילוי וזיהוי התקפות ותמיכה בטכנולוגיות/רמות הבאות :

4.7.1.3.1 יכולת זיהוי וגילוי מבוססת חתימות (Signature Based Detection)

- 4.7.1.3.2 יכולת זיהוי וגילוי תופעות חריגות (Anomaly Based Detection)
- 4.7.1.3.3 יכולת זיהוי וגילוי כיוון ההתקפה (Stateful Protocol Analysis)
- 4.7.1.3.4 יכולת זיהוי וגילוי התקפות ברמת הרשת (Network Behavior Analysis)
- 4.7.1.3.5 יכולת זיהוי וגילוי התקפות ברמת ה- Transport (Transport Layer Attacks)
- 4.7.1.3.6 יכולת זיהוי וגילוי התקפות ברמת ה- Network (Network Layer Attacks)
- 4.7.1.3.7 יכולת זיהוי וגילוי התקפות ברמת האפליקציה (Application Layer Attacks)
- 4.7.1.4 תמיכה ביכולות הבאות :
 - 4.7.1.4.1 אפשרות רישום ודיווח אירועים בזמן אמת
 - 4.7.1.4.2 אפשרות הפקת דו"חות אירועים
 - 4.7.1.4.3 אפשרות שינוי סביבת רשת/אבטחת מידע לחסימת התקפות (דוגמת שינוי טבלאות ניתוב והפניית התקפות)
 - 4.7.1.4.4 אפשרות לשינוי/הסרת תוכן זדוני והעברת מידע נקי בלבד
 - 4.7.1.4.5 אפשרות הגדרת ספים לגילוי תופעות חריגות
 - 4.7.1.4.6 אפשרות הגדרת Whitelist/Blacklist
 - 4.7.1.4.7 אפשרות הגדרת Policy Violations
 - 4.7.1.4.8 אפשרות חסימת התקפות Passive/Online

5. אופן ביצוע השירות

- 5.1 הזוכה יספק רק שירותי אינטרנט (ISP) ולא שירותי התשתית.
- 5.2 עם קביעתו כזוכה יעביר לידי המזמין את ההגדרות הרלוונטיות לנתבים הראשיים על מנת לאפשר את הקישור הראשי ממתקן יהודאי .
- 5.3 עם קביעתו כזוכה תעביר המשטרה לזוכה את כתובות ה-Domain, הזוכה נדרש להפעיל את כל התיבות לא יאוחר מחמישה ימי עבודה מרגע העברת התצורה, בהתאם לנדרש בסעיף 4.6.2.2.
- 5.4 כל פניה להוספת תיבה/חשבון גלישה או שינוי/הגדלה של תיבה/חשבון קיימים יהיו בהתאם להנחייה ואישור של נציג צוות תשתיות אקטיביות ויבוצעו תוך 4 שעות מפנייה, פרט להגדלת מהירות מנוי IPVPN / תמסורת מטרו שזמן הטיפול בבקשה לא יעלה על 24 שעות מפנייה.
- 5.5 המנויים לא יהיו מוגבלים בשימוש בשירותי האינטרנט של הזוכה למשך 24 שעות ביממה, 7 ימים בשבוע.
- 5.6 שם המנוי בקישורי האינטרנט לא יזוהה עם משטרת ישראל או כגוף ממשלתי.

5.7. מוקד שירות

- 5.7.1. הזוכה מתחייב לתפעל מוקד שירות לקוחות עשרים וארבע שעות ביממה בכל ימות השנה.
- 5.7.2. זמן ההמתנה של משתמש עד לקבלת מענה במוקד זה לא יעלה על 3 דקות.
- 5.7.3. המזמין יקבל קוד (מספר לקוח) אשר יקצר את זמן המענה הטלפוני במרכז הסיוע.
- 5.7.4. הזוכה יחל בטיפול בפניית משתמש לא יאוחר מ- 30 דקות מהזמן בו דיווח על הבעיה לראשונה. בנוסף, מתחייב הזוכה לדווח למשתמש בתוך 30 דקות נוספות לגבי מצב הטיפול בפנייתו. תקלה תתוקן עד 4 שעות מקבלתה.
- 5.7.5. משך זמן מקסימאלי לטיפול בתקלה משביתה באתר המרכזי או באתר POP של הזוכה לא יעלה על 180 דקות. אם נמשכה התקלה יותר מ- 180 דקות, במידה ולא ימצא פתרון תוך 3 שעות מרגע פתיחת הקריאה – יינתן למזמין פתרון חלופי להפעלת השירות ועד לפתרון הבעיה.
- 5.7.6. כתובת IP תהיה תקפה בכל תקופת המכרז, במידה ולא מתאפשר ניתוב כזה, מתחייב הזוכה לדאוג להסדרת יכולת הניתוב תוך 6 שעות מקבלת קריאה.
- 5.7.7. הודעה על סיום הטיפול בבקשה תישלח למזמין ע"י דוא"ל.

6. תיעוד

- 6.1. הזוכה יעבד, יכין ויעביר ללא תוספת תשלום את הדו"חות הבאים אחת לחודש, בכל 10 לחודש, לפי הפרוט דלהלן:
 - 6.1.1. דו"ח מרכז - פירוט כלל מנויי המשטרה לפי סוגי השירות שהם צורכים וכמויות הצריכה מכל סוג.
 - 6.1.2. חשבון מרכז לתשלום – בפורמט שורה לקישור שתכלול פירוט של סוגי השירותים בגינם נדרש תשלום, בסיס וערך מוסף. החשבון המרוכז יכלול סיכום לפי שורות (קישורים), עמודות (סוגי שירותים) וסה"כ.
 - 6.1.3. דו"ח קישורים לא פעילים, אשר יכלול את כל הקישורים שהשתמשו פחות מ- 60 דקות בשירותי האינטרנט במהלך החודש שקדם להוצאתו.
 - 6.1.4. דו"ח פירוט חודשי של קווי ADSL / כבלים / IPVPN / תמסורת מטרו אשר הותקנו על פי דרישת המזמין, כולל רוחב פס.
 - 6.1.5. דו"ח תקלות וחריגים כללי, אשר יכלול הן פירוט של התקלות הגדולות ברשת המציע אשר השפיעו על המשתמשים, מועדן ומשכן, והן פירוט של חריגים והתרעות כתוצאה מפעילות לא סטנדרטית של משתמשים ברשת המציע, כדוגמת ניסיונות LOGIN רבים שנדחו.
 - 6.1.6. דו"ח עומסים על כל קישור ברמה יומית, שבועית וחודשית.
 - 6.1.7. דו"ח תיבות דוא"ל לא פעילות אשר יכלול את רשימת תיבות הדואר האלקטרוני הלא פעילות במשך 3 חודשים ומעלה.

7. הבטחת איכות

- 7.1. במהלך ההתקשרות תיבדק עמידה בזמני הוספת תיבה/חשבון והתיקונים כנדרש במפרט.
- 7.2. קבלת דוחו"ת בהתאם לנדרש בסעיף 6 במפרט.