

15 יולי 2020

כג' תמוז תש"פ

מנכ"ל הוא"א - מר זאב שניר

הנדון : סיום השאלה

1. בתאריך 1/9/2020 אתייצב בוא"א אחרי השאלה בת 4 שנים למשרד רוח"מ- מערך הסייבר הלאומי.
2. במסגרת תפקידי במערך הסייבר הלאומי כרמ"ח הנחייה באגף הכוונה ואסדרה הייתי אמון על הפעילויות הבאות בהיבטי ההגנה בסייבר:
 - ריכוז, תיאום, ניהול והובלת משימה לאומית מטעם מערך הסייבר הלאומי לבחירות המרכזיות של מדינת ישראל לכנסת ה- 21, 22, ו- 23 בכל האמור להיבטי ההגנה בסייבר על תשתיות טכנולוגיות וממשקיהן (קבלת תעודות הערכה והוקרה מטעם מערך הסייבר הלאומי). במסגרת משימה זו עבודה מול ועדת הבחירות המרכזית, חברות IT, גופי ממשל וגופי ביטחון למתן פתרונות הגנה לאתגרי התערבות שחקן בתוצאות הבחירות או שיבושן.
 - רמ"ח הנחיה למגזר ממשלתי- כלל משרדי הממשלה ויחידות הסמך, משרד החוץ על 103 נציגויותיו, מגזר הגנת הסביבה- כלל המפעלים בעלי היתר רעלים, מגזר הכלכלה והתעשייה – כלל תעשיות וספקי המזון, רשות הטבע והגנים והמוסד לביטוח לאומי.
 - רכישת ידע הכרות והנחייה במתודולוגיה מודל ביצוע המנהל את הסיכונים הכרוכים בשרשרת האספקה בהיבטי הגנת הסייבר.
 - רכישת ידע והכרות במתודולוגיה, באפיון דרישות לבניית מרכז ניטור ופיקוח ביטחוני(SOC) כולל הקמה והפעלה במערכות מורכבות ומסוגות .
 - ידע והיכרות מתודולוגיה ב Incident Responses והכרות עם מתודולוגיה לביצוע בדיקות ביטחון קוד מאובטח.
 - ידע והיכרות מתודולוגיה וביצוע בדיקות קבלה למערכות בהיבט הביטחוני (APT Security).
 - ידע והיכרות עם מתודולוגיות לביצוע Digital Forensics במערכות מחשב, וציווד תקשורת וביצוע סלולר.
 - היכרות טובה עם תקנים בינלאומיים בכלל ועם תקינת NIST בפרט לרבות מפגש מקצועי עמם.
 - הנחיה, הכוונה ושיתוף פעולה בתחום הסייבר באוריינטציה במגזר הממשלתי, המוסד לביטוח לאומי, מגזר הגנת הסביבה, משרד הבריאות- בתי חולים ממשלתיים, מגזר הכלכלה והתעשייה, מגזר התיירות.
 - עבודה ותיאום עם חברות IT גדולות בתחום הענן – Microsoft ,google ,amazon ,salesforce, אפיון מדיניות הקשחה והגנה בסייבר לתשתיות אלו.

- עבודה עם חברות IT גדולות ,NetApp Microsoft, VMWare מתן ופרסום הנחיות הגנה בסייבר ל win 10, תשתיות וירטואליזציה ומערכי אחסון.
 - עבודה עם חברת IBM בכל האמור להגנה על תשתיות מאגרי על – Main Frame.
 - כתיבת הנחיות וביצוע בדיקות קבלה ביטחוניות (SATP) לפרויקט VOIP ממשלתי בשיתוף גורמים מקצועיים.
 - מתן הנחיות לגופים בתחום שרשת האספקה ע"ב מתודולוגיה של מערך הסייבר הלאומי.
 - נציג מערך הסייבר הלאומי בוועדת ענן התקשוב הממשלתי.
 - עבודה וכתיבת דרישות הגנה בסייבר אל מול גורמי חשכ"ל למכרזים הגנה בסייבר שונים.
 - מגזר הגנ"ס עיצוב תהליכי עבודה, מיפוי סקרי סיכונים, היתר רעלים ומתודולוגית הגנה בסייבר לחומ"ס.
 - עבודה מול גורמי מודיעין לניתוח והבנה בסגירת והכלת אירועים.
 - מתן מענה אבטחתי להגנה על תשתיות מאגרי העל בביטוח לאומי.
 - עבודה אל מול גורמי משרד מבקר המדינה בביקורות נושאות.
3. לפני מספר חודשים שוחחנו טלפונית לגבי אופן שילובי המקצועי בוא"א בסיום השאלתי.
 4. בקשת ממני להשתבץ באגף מערכות מידע בתחום הסייבר מתוך כוונה כי בניסיון והידע שצברתי עד עתה אוכל לתרום ולקדם בהיבטי הגנה בסייבר את מערכות המידע של וא"א. כמו כן ציינת כי אם אבחר אני יוכל לחזור לתפקידי טרם השאלתי באגף הביטחון.
 5. צינתי כי אינני רואה מניעה תחת זאת שתפקידי באגף מערכות מידע בתחום הסייבר יוגדר במסמך שיפרט את תחומי האחריות והסמכות בתפקיד זה.
 6. בתאריך 07/05/2020 נפגשתי עם ר' אגף הביטחון מר רונן כהן. השיחה עמו הייתה נעימה ועניינית בה כל אחד הציג את עמדתו.
 7. בתאריך 19/5/2020 נפגשתי עם ר' אגף מערכות מידע מר עופר סנקר. עופר הציג את התפתחות האגף, השינויים המבניים שהתרחשו והאתגרים עימם מתמודדים. עופר הציג את ראייתו לגבי תכולת התפקיד. הצגתי את הידע והניסיון שנצבר אצלי עד עתה במס"ל. סיכמנו כי אכין מסמך המתאר את תכולת התפקיד לרבות סמכות ואחריות.
 8. בתאריך 25/5/2020 נפגשתי עם מר בוקי כרמלי דנו וניסחנו מקצועית את תכולת התפקיד ע"ב הצעתי לתכולת תפקיד. מסמך זה הועבר לעופר סנקר ביום זה.
 9. בתאריך 1/6/2020 בדקתי עם עופר את סטאטוס המסמך שקבל ונעניתי כי נמצא בבדיקה ותוך ימים יחזור אלי.
 10. נכון למועד כתבת מסמך זה טרם קבלתי כל התייחסות בנושא. במצב שנוצר ולאור כך שעוד מספר שבועות אחזור לוא"א, ללא ידיעה מה מצפה לי בהיבט השיבוץ,

ובתוך כך בחוסר ודאות יש בי תחושת אי נוחות ואי בהירות מטרידים מאוד לגבי עתיד.

11. לאור חוסר הודאות הקיים ולאור הנסיון שצברתי בתחום ההנחיה והבקרה בהגנה בסייבר ולאור סיכום קיים עם נציבות שירות המדינה, אני מבקש ממך לאפשר לי לחזור לתפקידי באגף הביטחון.

12. כולי ציפייה לחזור לשרת לוא"א, בטחוני כי אדע ליזום, לקדם, לדחוף ולתת מענה אשר יבסס את חוסנה ויציבותה של וא"א בכל האמור להיבטי הסייבר אשר תחת אחריותי.

בכבוד רב,

אפריאט אילן