

דוח מבקר המדינה | סייבר ומערכות מידע | התשפ"ג-2022



רשות המיסים בישראל

**הגנת סייבר
והמשכיות עסקית
ביחידת שירות
עיבודים ממוכנים
ברשות המיסים**



הגנת סייבר והמשכיות עסקית ביחידת שירות עיבודים ממוכנים ברשות המיסים

רקע

שירות עיבודים ממוכנים (שע"ם) הוא גוף המשמש מערך המחשוב של רשות המיסים בישראל ונותן לה שירותי מחשוב לצורך גבייה ואכיפה, ליצירת הרתעה ראויה ולמיצוי זכויותיהם של הנישומים. שע"ם משרת כ-1.3 מיליון "לקוחות": חברות, תאגידים מסוגים אחרים, עצמאים, בעלי שליטה, שכירים, מקבלי מענקי עבודה, שכירים המבצעים תיאומי מס והחזרי מס, 6,000 העובדים של רשות המיסים, 13,000 משרדי מייצגים ו-7,000 עורכי דין. שע"ם מנהל מאות פרויקטים בכל שנה, החל בפרויקטים לביצוע מידי וכלה בפרויקטים שביצועם נמשך שנים מספר. שע"ם מחזיק במערכתיו מידע על אזרחים, נישומים, עוסקים וגופים נוספים.

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 קובע את תחומי הסמכויות והאחריות לאבטחה פיזית, לאבטחת מידע ולאבטחת מערכות מחשוב חיוניות של גופים ציבוריים שונים, לרבות גופי ממשלה וגופים בבעלות פרטית. החוק מגדיר מערכות ממוחשבות חיוניות כ"מערכות ממוחשבות שנקבעו כחיוניות על ידי הגוף שהסמיכה לכך הממשלה".

בשנת 2010 החליטה ועדת היגוי עליונה כי שע"ם ייכלל בתוספת השנייה והחמישית לחוק הסדרת הביטחון. בהתאם לכך, מערך הסייבר הלאומי הוסמך לתת הנחיות מקצועיות בתחום אבטחת מערכות מחשוב חיוניות לשע"ם.



נתוני מפתח

חלק

מעובדי שע"ם הנדרשים לסיווג אינם בעלי סיווג נדרש

1.3 מיליון

מקבלי שירות משע"ם: חברות, תאגידים, עצמאיים, שכירים ועוד


2014

השנה בה החלה הכנת תוכנית המשכיות עסקית בשע"ם, תהליך שטרם הסתיים

11

מספר ממצאי מבדק החוסן שביצע יועץ חיצוני מטעמו של משרד מבקר המדינה

פעולות הביקורת

בחודשים נובמבר 2021 - פברואר 2022 בדק משרד מבקר המדינה את אבטחת המידע והגנת הסייבר בשע"ם. הביקורת נעשתה בשע"ם, ובדיקות השלמה נעשו במערך הסייבר הלאומי. 

במסגרת הביקורת נבדקו היבטים מסוימים בהגנת סייבר, נעשתה בדיקת חוסן למערכת התומכת בתהליך עסקי ברשות המיסים (מערכת א'), ונבדקה היערכות שע"ם להמשכיות הפעילות העסקית ולהתאוששות מאסון.

הדוח שבנדון הומצא לראש הממשלה ביום 31.7.2022 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא הונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.



תמונת המצב העולה מן הביקורת



תפקידי ועדת היגוי לנושא התמ"ק - עלה כי תפקידי הוועדה הוגדרו בכתב המינוי באופן כללי, והם לא פורטו כנדרש בהנחיות הרגולטוריות. עלה כי דיוני הוועדה אינם עוסקים בפעולות שתנקוט הוועדה בהתאם לתפקידיה, כפי שנדרש בהנחיות.

מיפוי תהליכים ונכסי מידע - על פי ההנחיות הרגולטוריות, על הגוף למפות את נכסי המידע והגישות אליהם, כדי להתאים תוכנית אבטחה. עלו פערים במיפוי התהליכים ונכסי המידע שבוצע בשע"ם והוא אינו עונה במלואו על דרישות ההנחיות הרגולטוריות.

פערים בנוהלי שע"ם - בביקורת עלה כי במספר נהלים בשע"ם נמצאו אי התאמות להנחיות הרגולטוריות, בין היתר, בנושא ממשק העבודה מול מערך הסייבר הלאומי.

- **ניהול שינויים** - לא נמצאה בנוהל הרלוונטי התייחסות לצורך לעדכן את הגורם הרלוונטי ולשתפו בנייתוח הסיכונים וההשפעות הצפויות של השינויים כנדרש בהנחיות.

- **נוהל טיפול באירועי אבטחת מידע** - נמצא כי בשע"ם קיים נוהל אך הוא אינו עוסק בחובה לדווח לגורם הרלוונטי ולצורך לשלבו בתחקור האירוע. בנוסף חסרה התייחסות רלוונטית לתחום מסוים הנדרש בהנחיות.

ריכוז מידע בדבר שרשרת אספקה - עלו פערים בדבר המידע שנאסף על ידי אגף אבטחת מידע בשע"ם בנוגע לשרשרת האספקה. כמו כן, לא נעשה שימוש במודול שרשרת אספקה במערכת הייעודית שפיתח מערך הסייבר הלאומי.

חולשה בשרת מסוים - עלו פערים בבקרה על השרת המסוים.

סיווג נדרש - הביקורת העלתה כי קיימים פערים בין רמת הסיווג הנדרשת בהתאם לתפקידיהם של חלק מהעובדים בשע"ם לבין רמת הסיווג שלהם בפועל.

בדיקת חוסן מטעם משרד מבקר המדינה על מערכת א'

מערכת זו תומכת בתהליך עסקי ברשות המיסים. במהלך הבדיקה הועלו ממצאים אשר מסכנים מהבחינה העסקית את המידע ואת מוניטין הארגון.

היערכות להמשכיות עסקית והתאוששות מאסון

הסדרת פעילות האגף - בנובמבר 2016 החליט מנהל שע"ם כי לצורך הקמת אגף איכות והמשכיות עסקית יתוכנן מבנה ארגוני לאגף בסיוע יועצים. נציבות שירות המדינה התנתה את אישור האגף באישור נחיצותו מטעם רשות התקשוב הממשלתי. עלה כי האגף פועל מסוף שנת 2016, אף שהנציבות לא אישרה את שינוי המבנה הארגוני. הגדרות התפקיד של עובדי האגף הן הגדרות תפקידיהם הקודמים, והם מועסקים בהתאם לתקנים שהוקצו לאגפים אחרים. בעקבות זאת סמכות האגף ותפקידיו אינם מוסדרים.



תוכנית התאוששות מאסון - תוכנית התאוששות מאסון כוללת תוכנית להתאוששות המערך הטכנולוגי, תהליך הפעלת מצב החירום, תהליך החזרה ממצב החירום לשיגרה, תרגילי החירום ומדדים עיקריים להתאוששות:






Return Point Objective (RPO) - כמות המידע שאבד בהתרחש אסון.

Return Time Objective (RTO) - משך הזמן המרבי מרגע קבלת ההחלטה עד להפעלת אתר החירום.

נמצאו פערים בנוגע להשלמת תוכנית התאוששות מאסון.

תוכנית להמשכיות עסקית - נמצאו פערים בתהליך גיבוש תוכנית להמשכיות עסקית ובהשלמתה.

עיקרי המלצות הביקורת

- מומלץ כי שע"ם יתקן את הליקויים שנמצאו במיפוי התהליכים ונכסי המידע שנערך. 
- מומלץ כי שע"ם יעדכן את נהליו באופן שיכללו את כל הפעולות הנדרשות בהתאם להנחיות הרגולטוריות. 
- מומלץ כי שע"ם ישתמש במערכת הייעודית שפיתח מערך הסייבר הלאומי לבחינת שרשרת האספקה. 
- מומלץ כי שע"ם יפעל לכך שרמת הסיווג של כלל העובדים בשע"ם תותאם לתפקידיהם. 
- מומלץ כי שע"ם יבחן את הממצאים שהועלו במבדק החוסן שנערך מטעם משרד המבקר המדינה ויתקן את הליקויים שהועלו בדוח זה. 



סיכום

שע"ם הוא גוף ה-IT של רשות המיסים, וככזה הוא מפתח מערכות מידע עבודה, מתחזק מערכות קיימות ומחזיק במידע. יש חשיבות גדולה לרמה גבוהה של הגנת סייבר בשע"ם וכן לתפקוד מלא של שע"ם בעתות משבר והתאוששות מהירה מאסון.

ממצאי הביקורת מעלים כי על שע"ם לפעול לשיפור הגנת הסייבר על מערכתיו.

מומלץ כי שע"ם יפעל בהקדם לתיקון הליקויים שהועלו בדוח זה תוך בחינת יישום המלצות הדוח.

