דוח מבקר המדינה - סייבר ומערכות מידע
אייר התשפ"ג | מאי 2023

משרד המשפטים -
רשות האכיפה והגבייה

הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה

הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה

רקע

המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה (המג"ק) הוא הגוף שתפקידו לגבות חובות לטובתם של אוצר המדינה וגופים ציבוריים וכן לגבות פיצויים שנפסקו לנפגעי עבירה בהליכים פליליים. נכון לפברואר 2023 יתרת החוב בתיקים הפתוחים במג"ק מסתכמת בכ-6.8 מיליארד ש"ח. לצורך גביית החובות הוענקו למג"ק סמכויות גבייה וביניהן דרישת מידע על החייב מגוף ציבורי. על מנת לפעול לגביית החובות ביעילות מנוהלת עבודת המג"ק באמצעות מערכת ממוחשבת המכילה מאגר מידע רחב היקף בנוגע לכ-3 מיליון חייבים, וכוללת בין היתר שמות, מספרי זהות, כתובות מגורים, מספרי טלפון, פרטים על נכסים שברשות החייבים, מידע מהמוסד לביטוח לאומי, מאגף הרישוי שבמשרד התחבורה ומרשויות אחרות.

בכל הנוגע להגנת הפרטיות ולאבטחת מידע נדרש המג"ק לפעול בהתאם להוראות הדין, ובהן חוק הגנת הפרטיות, התשמ"א-1981 והתקנות על פיו, להחלטות ממשלה ולנהלים והנחיות הגופים המאסדרים את הנושא ובהם היחידה להגנת הסייבר בממשלה (להלן - יה"ב), המהווה גורם מנחה מקצועית בתחום הגנת הסייבר.

נתוני מפתח

3 מיליון
מספר החייבים שפרטיהם נכללים במאגרי המידע של המג"ק

כ-6.8 מיליארד ש"ח
סך יתרת החוב בתיקים הפתוחים במג"ק

7% בלבד
שיעור האירועים החריגים[1] (99 מתוך 1,391) שהתרחשו בספטמבר 2022 ונבדקו על ידי גורמי הבקרה במג"ק

52%
שיעור ההרשאות (23 מתוך 44) שנפתחו במערכת התפעולית של המג"ק בלי שמינהלן ההרשאות ברשות האכיפה והגבייה התבקש לאשרן

14 הרשאות
של עובדי מוקד המידע הטלפוני למאגר המידע של המג"ק לא הוסרו חרף סיום עבודתם בטווח של חודש עד 13 חודשים לפני מועד הביקורת

21%
שיעור עובדי מוקד המידע הטלפוני (20 מתוך 94) שהשתמשו במערכת ללא כרטיס חכם המשויך להם

פעולות הביקורת

בחודשים ספטמבר 2021 - אוקטובר 2022 בדק משרד מבקר המדינה היבטים בתחום ההגנה על הפרטיות ואבטחת המידע במערכות המג"ק. בביקורת נבדקו אופן תיעוד הגישה, השימוש במערכות המידע במג"ק והשינויים בהן, מערך ההרשאות למערכות המידע במג"ק וההתמודדות עם סכנת חדירה למערכות המידע. בדיקות השלמה בוצעו בחודשים ינואר ופברואר 2023.

הביקורת נעשתה במרכז לגביית קנסות שברשות האכיפה והגבייה ובמטה הרשות. בדיקות השלמה נערכו ברשות להגנת הפרטיות במשרד המשפטים וביחידה להגנת הסייבר בממשלה (יה"ב) במערך הדיגיטל הלאומי.

משרד מבקר המדינה בחן במקביל היבטים נוספים בפעילות המרכז לגביית קנסות - ניהול תהליך גביית החוב משלב קליטת התיק, משלוח דרישות תשלום ונקיטת הליכי גבייה שונים; מנגנוני פריסת החוב, הפחתות תוספות הפיגורים ומחיקת חובות במג"ק; ניהול

1 אירועים עסקיים שהוגדרו כאירועים חריגים במערכת התפעולית של המג"ק ומצדיקים בחינה פרטנית אם היו מוצדקים כגון סגירת תיק חוב מעל סכום מסוים ללא תשלום.

תהליך גביית חובות מסוג פיצויים לנפגעי עבירה והקשר עם נפגעי העבירה. ממצאי ביקורת אלו פורסמו בדוח מבקר המדינה ממאי 2023[2].

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, זאת לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

תמונת המצב העולה מן הביקורת

- **תיעוד של הגישה למידע במערכות המידע במג"ק ובקרה על כך** - המג"ק אינו מתעד את הגישה של משתמשי המערכת במג"ק למידע הרב והרגיש שקיים בה ואינו מבצע בקרה עליה. במצב דברים זה, גם אם קיימות חריגות של משתמשים, אין אפשרות לאתרן ולהפסיקן.

- **בדיקת אירועים חריגים במערכת** - אף שהמג"ק הגדיר בשנת 2016 רשימה של 13 אירועים עסקיים חריגים הדורשים בחינה פרטנית אם היו מוצדקים, בספטמבר 2022 תועדו 1,391 אירועים חריגים, מהם נבדקו 99 (7%) אירועים בלבד. נוסף על כך, המג"ק לא עדכן את רשימת האירועים החריגים במערכת משנת 2016.

- **ניהול הרשאות הגישה למערכות המג"ק** - מתוך 44 הרשאות למשתמשים שנפתחו במערכת הממוחשבת הייעודית לכך (מערכת ב') בשנת 2021, 23 הרשאות (52%) נפתחו בלי שהתבקש עבורן אישור ממינהלן ההרשאות, כנדרש בנוהל המג"ק.

- **בקרה על ההרשאות הפעילות במערכת התפעולית של המג"ק ועל היקפן** - החל ביולי 2020, מועד תחילת עבודת המג"ק באמצעות מערכת ב', ועד מועד סיום הביקורת באוקטובר 2022, לא בוצעה בקרה על ההרשאות שנפתחו במערכת, וכן לא נבדק אם יש צורך בהסרת הרשאות (נוכח אי-התאמה למהות התפקיד או עקב מעבר תפקיד).

- **היקף הרשאות הגישה למערכת התפעולית של המג"ק** - כל עובדי המג"ק וכן עובדי מוקד המידע הטלפוני שהם עובדים המועסקים במיקור חוץ, הם בעלי גישה למלוא המידע במערכת התפעולית של המג"ק על אודות מיליוני החייבים שנתוניהם שמורים במערכת, בלי שנבחן אם היקף הגישה למידע נחוץ על פי הגדרת תפקידם.

- **ניהול ההרשאות של עובדי מוקד המידע הטלפוני** - ההרשאות של 14 עובדי מוקד לשעבר למערכת התפעולית של המג"ק לא הוסרו חרף סיום עבודתם בטווח של חודש עד 13 חודשים לפני מועד הביקורת. כמו כן, המג"ק לא פעל לחסימת כרטיסים חכמים של עובדים שסיימו את עבודתם במוקד, ובפועל צוות המוקד משתמש בכרטיסים ובסיסמאות של עובדים אלה במקרים שונים.

2 מבקר המדינה, **דוח שנתי של מבקר המדינה - מאי 2023**, "המרכז לגביית קנסות ברשות האכיפה והגבייה", עמ' 1723.

- **ניהול הרשאות הגישה למערכת ג'** - הרשאות למערכת ג', המאפשרת להפיק דוחות רוחביים על פעילות המג"ק ומידע פרטני על תיקים, ניתנו לעובדים שאופי תפקידם אינו מצריך גישה למידע שבמערכת. ואכן, קרוב ל-40% מבעלי ההרשאות למערכת ג' (20 מתוך 52) לא השתמשו במערכת ג' לכל הפחות החל משנת 2021.

- **התמודדות רשות האכיפה והגבייה עם סכנת חדירה למערכת התפעולית של המג"ק** - במבדק חדירות שביצעה יה"ב נמצאו ליקויים ברמת התשתית שיכולים להוות סיכון משמעותי אם תתרחש חדירה לרשת הארגון. בביקורת נמצא כי על אף ממצאי מבדק החדירות, רשות האכיפה והגבייה לא הטמיעה במערכותיה, ובכלל זה במערכת התפעולית של המג"ק, פתרון אבטחתי טכנולוגי ייעודי מסוים.

עיקרי המלצות הביקורת

- על המג"ק להקים מערכת לתיעוד הגישה של משתמשי המערכת התפעולית למידע במערכת ולבצע בקרה עיתית על הגישה למידע, על פי הוראות תקנות אבטחת המידע ותקן ISO 27001 (שהוא תקן בין-לאומי העוסק במיסוד מערכת לניהול אבטחת מידע ארגונית ובתהליך השוטף של ניהול המערכת ושיפורה).

- על המג"ק לבצע בקרה איכותית ושוטפת על האירועים החריגים. כן מומלץ לבחון את הצורך לטייב את רשימת האירועים החריגים במערכת.

- על מרכז ההרשאות במג"ק להקפיד שלא לפתוח הרשאות אם מינהלן ההרשאות לא אישר את פתיחתן.

- על רשות האכיפה והגבייה לבצע בחינה של היקף הרשאות הגישה למערכת התפעולית של המג"ק של עובדים בתפקידים השונים, ולבצע בקרות עיתיות על מערך ההרשאות, בהתאם להנחיית יה"ב ולנוהלי רשות האכיפה והגבייה.

- מוצע כי המג"ק יבחן אם יש מקום להגביל את אפשרויות הגישה של עובדי מוקד המידע הטלפוני למערכת התפעולית של המג"ק על בסיס הפניות המתקבלות במוקד. כמו כן עליו לבצע בקרה עיתית על הרשאות עובדי המוקד הטלפוני ולהימנע מלהשתמש בהרשאות הגישה למערכת של עובדים שאינם מועסקים במוקד או מהעברת כרטיסים חכמים מעובד אחד למשנהו.

- מומלץ כי רשות האכיפה והגבייה תבחן באופן פרטני את ההרשאות שניתנו למערכת ג' בהתאם לצורך ולזיקה לתפקיד של בעל ההרשאה, כדי לצמצם את היקף בעלי ההרשאות למערכת למינימום ההכרחי.

- על רשות האכיפה והגבייה לקדם את ההליך המכרזי ולהטמיע פתרון אבטחתי טכנולוגי ייעודי מסוים, שיבטיח הגנה מרבית על נכסי המידע של רשות האכיפה והגבייה, בהתאם להנחיית יה"ב.

תהליך מתן ההרשאות בפועל למערכת התפעולית של המג"ק

על פי נתוני המג"ק, בעיבוד משרד מבקר המדינה.

סיכום

דוח זה מעלה ליקויים בתחום הגנת הפרטיות ואבטחת המידע במערכות המידע במרכז לגביית קנסות שברשות האכיפה והגבייה, וביניהם: היעדר תיעוד של הגישה של משתמשי המערכת התפעולית של המג"ק למידע המצוי במערכת וכפועל יוצא מכך היעדר בקרה על אותה גישה; אי-ביצוע מעקב הולם אחר אירועים חריגים המתרחשים במערכת; ניהול לקוי של תהליך מתן ההרשאות למערכת התפעולית של המג"ק ושל הפיקוח והבקרה עליהן; היקף גישה בלתי-מוגבל של משתמשי המערכת למידע המצוי במערכת; ניהול לקוי של הרשאות עובדי מוקד המידע הטלפוני למערכת; וכן סיכון לחדירת תוקפים חיצוניים למערכות המג"ק.

ליקויים אלה אינם עולים בקנה אחד עם הוראות הדין, ובהן חוק הגנת הפרטיות והתקנות על פיו, החלטות הממשלה הרלוונטיות והנחיות הגופים המאסדרים את הנושא. הדברים מקבלים משנה תוקף נוכח העובדה שעל פי הוראות תקנות אבטחת מידע מסווגות המערכת התפעולית של המג"ק כמאגר שמחייב רמת אבטחה גבוהה.

על רשות האכיפה והגבייה והמג"ק לפעול בהקדם על פי הנחיות הגופים הרלוונטיים למניעת דליפת מידע מהארגון ולשמירה על שלמותו. בכלל זה עליהם להקים מערך לתיעוד ובקרה בעניין השימוש במערכות המידע של המג"ק. כן עליהם לבצע בקרות עיתיות על מערך ההרשאות של עובדי המג"ק ואף לבצע בחינה של היקף הרשאות הגישה למערכת התפעולית של המג"ק לעובדים בתפקידים השונים. נוסף על כך עליהם לבצע בקרה על הרשאות עובדי המוקד ומוצע כי המג"ק יבחן האם יש מקום להגביל את אפשרויות הגישה של עובדי מוקד המידע הטלפוני למערכת התפעולית שלו. נוסף על כך על רשות האכיפה והגבייה לקדם את ההליך המכרזי ולהטמיע במערכותיה פתרון אבטחתי טכנולוגי ייעודי מסוים, שיבטיח הגנה מרבית על נכסי המידע שלה.

מאגר המידע של המג"ק הוא רחב היקף וכולל מידע רגיש בנוגע לכ-3 מיליון חייבים. סכומי החוב שבטיפול המג"ק נכון למועד הביקורת מסתכמים בכ-6.8 מיליארד ש"ח. מכאן נובע הצורך לשמור על מערכות המידע למניעת פגיעה בשלמות המידע וברציפות התפקודית של המג"ק במתן שירותים, וכן כדי למנוע דליפה של נתונים ומידע ממאגר המידע או למנוע את חשיפתם לגורמים שאינם מורשים לכך.

הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה

מבוא

המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה (להלן - המג"ק) הוקם בשנת 1995 מכוח חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה-1995, כגוף שתפקידו לגבות חובות, בעיקר לטובת אוצר המדינה וכן לגבות פיצויים שנפסקו לנפגעי עבירה בהליכים פליליים (להלן - נפגעי עבירה). המג"ק הוקם לאחר שהתברר כי המנגנונים לגביית חובות שפעלו באותה עת לא היו יעילים והפכו את הגבייה ללא כדאית מהבחינה הכלכלית, וכי אי-תשלום החובות פגע קשות באכיפת החוק[3].

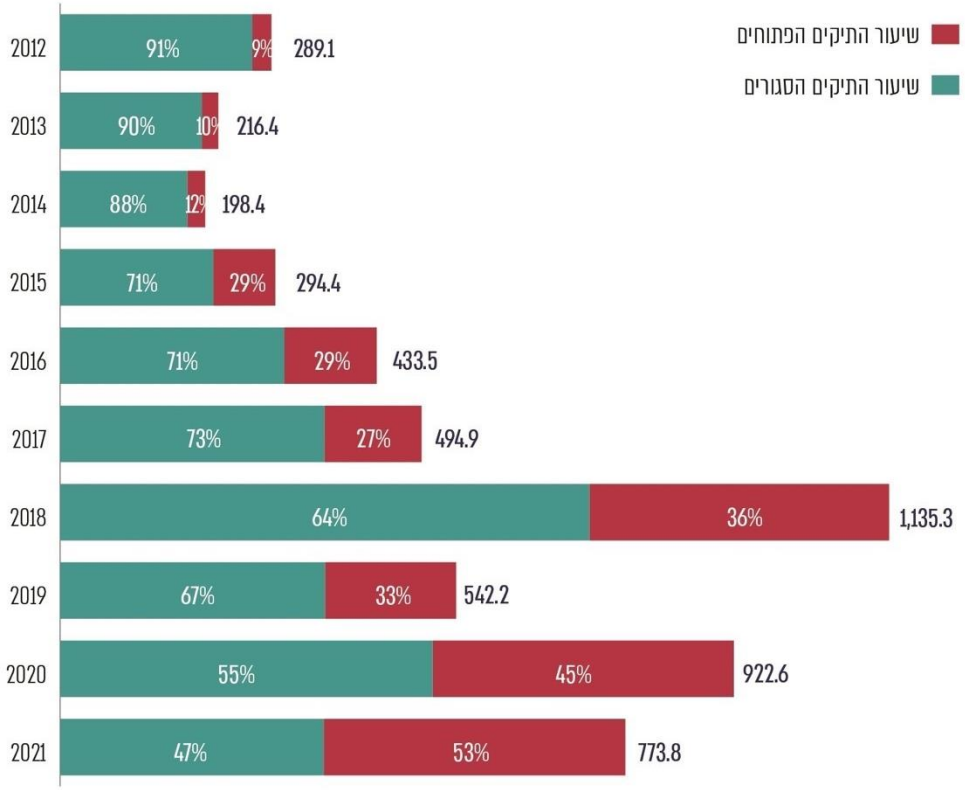
היקפי הפעילות של המג"ק: מאז הוקם בשנת 1995 ועד סוף שנת 2021 נפתחו במג"ק כ-9.9 מיליון תיקי חובות שהקרן בהם עמדה על כ-8.4 מיליארד ש"ח. מתוכם נסגרו כ-7.4 מיליון תיקים, תוך שהמג"ק גבה בכלל התיקים (הפתוחים והסגורים) סכום של כ-6.9 מיליארד ש"ח (הכולל בתוכו תוספות פיגורים, הפרשי הצמדה וריבית והוצאות)[4]. יתרת החוב בתיקים הפתוחים במג"ק מסתכמת בכ-6.8 מיליארד ש"ח[5].

3 דברי הסבר להצעת חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ב-1994, ה"ח הממשלה 2332, עמ' 159.

4 תחשיב משרד מבקר המדינה על פי נתונים שהועברו מהמג"ק, בניכוי תיקים שנסגרו בלי ששולמו החובות בשל נסיבות "טכניות" או משום שהחובות בוטלו מעיקרם.

5 תחשיב משרד מבקר המדינה, על פי נתונים שהועברו מהמג"ק, בניכוי תיקים מוקפאים.

תרשים 1: **שיעור התיקים הפתוחים והסגורים במועד הביקורת במג"ק* ומספרם הכולל של התיקים (באלפים) לפי שנת קליטת התיק, 2012 - 2021**



על פי נתוני המג"ק, בעיבוד משרד מבקר המדינה.

* ללא תיקים מוקפאים

במועד עריכת הביקורת היו מועסקים במג"ק כ-75 עובדים. כמו כן מקבל המג"ק שירותי מטה מרשות האכיפה והגבייה בתחום הייעוץ המשפטי, מערכות המידע ואבטחת המידע.

בחוק המג"ק ובתקנות על פיו[6] נקבעו סמכויות הגבייה של המג"ק, וביניהן דרישת מידע מגוף ציבורי לצורך גביית חוב. בהתאם, למג"ק גישה באמצעות ממשקים ממוחשבים, לנתונים מסוימים של כמה משרדים ממשלתיים ובהם אגף הרישוי במשרד התחבורה[7], רשם המקרקעין (טאבו)[8], רשות מקרקעי ישראל ורשות האוכלוסין וההגירה.

6 תקנות המרכז לגביית קנסות, אגרות והוצאות, התשנ"ו-1996; תקנות המרכז לגביית קנסות, אגרות והוצאות (קבלת מידע מאת רשות מס), התשס"ג-2003.

7 מידע על רכבים הרשומים על שם החייב.

8 מידע על נכסי מקרקעין הרשומים על שם החייב.

על מנת לפעול לגביית החובות ביעילות, מנהל המג"ק מאגר מידע רחב היקף בנוגע לכ-3 מיליון חייבים, המכיל בין היתר שמות, מספרי זהות, כתובות מגורים, מספרי טלפון, פרטים על נכסים שברשות החייבים, מידע מהמוסד לביטוח לאומי, מאגף הרישוי שבמשרד התחבורה ומרשויות אחרות. עבודת המג"ק והגישה למאגר המידע מנוהלות באמצעות מערכת תפעולית.

המערכת התפעולית של המג"ק, וכן תחום אבטחת המידע והסייבר במג"ק, מנוהלים ומתופעלים על ידי רשות האכיפה והגבייה עבור המג"ק. חטיבת טכנולוגיות דיגיטליות ומידע של רשות האכיפה והגבייה מפעילה את המערכות באמצעות עובדי רשות האכיפה והגבייה וכן באמצעות עובדים המועסקים במיקור חוץ כנותני שירותים אך ורק לצורך הפיתוח והתחזוקה שלהן.

תקציבו של המג"ק מנוהל כחלק מתקציבה הכולל של רשות האכיפה והגבייה. תקציב רשות האכיפה והגבייה הסתכם בכ-231 מיליון ש"ח[9] לשנת 2021.

העלויות הישירות של תקציב אבטחת מידע וסייבר של רשות האכיפה והגבייה מסתכמות בכ-7.2% מתקציב טכנולוגיות המידע של הרשות. נוסף על כך, בתקציב טכנולוגיות המידע עלויות נוספות שמקורן בצורכי אבטחת מידע וסייבר (רישוי של אנטי וירוס, לומדות אבטחת מידע, כוח אדם שנותן מענה גם על אבטחת מידע וסייבר ועוד) ולכן נחשבות לעלויות "עקיפות" של תחום סייבר ואבטחת מידע.

לנוכח נחיצות השימוש במערכות מידע לתפקודו התקין והיעיל של המג"ק, היקף המידע ומספרם הרב של החייבים שעל אודותיהם קיים מידע במערכת התפעולית של המג"ק, קיימת חשיבות יתרה לשמור על התשתית הטכנולוגית, על שלמותו ומהימנותו של המידע ולהגן מפני דליפה שלו כדי להימנע מפגיעה ברציפות התפקודית של המג"ק ובפרטיות החייבים ונפגעי העבירה - מושאי המידע.

פעולות הביקורת

בחודשים ספטמבר 2021 - אוקטובר 2022 בדק משרד מבקר המדינה היבטים בתחום ההגנה על הפרטיות ואבטחת המידע במערכות המידע של המג"ק. בביקורת נבדקו תיעוד הגישה, השימוש והשינויים במערכות המידע במג"ק, מערך ההרשאות למערכות המידע במג"ק וההתמודדות עם סכנת חדירה למערכות המידע. בדיקות השלמה בוצעו בחודשים ינואר ופברואר 2023.

הביקורת נעשתה במרכז לגביית קנסות שברשות האכיפה והגבייה ובמטה הרשות. בדיקות השלמה נערכו ברשות להגנת הפרטיות במשרד המשפטים וביחידה להגנת הסייבר בממשלה (יה"ב) במערך הדיגיטל הלאומי.

משרד מבקר המדינה בחן במקביל היבטים נוספים בפעילות המרכז לגביית קנסות - ניהול תהליך גביית החוב משלב קליטת התיק, משלוח דרישות תשלום ונקיטת הליכי גבייה שונים; מנגנוני פריסת החוב, הפחתות תוספות הפיגורים ומחיקת חובות במג"ק; ניהול תהליך גביית

9 התקציב המאושר (התקציב המקורי, שכולל את השינויים שאישרה ועדת הכספים), מתוך פרסום אגף התקציבים במשרד האוצר במערכת "פיסקלי דיגיטלי".

חובות מסוג פיצויים לנפגעי עבירה והקשר עם נפגעי העבירה. ממצאי ביקורת אלו פורסמו בדוח מבקר המדינה ממאי 2023[10].

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]

תיעוד השימוש במערכות המידע במג"ק ובקרה עליו

הזכות לפרטיות הוכרה על ידי המחוקק כזכות יסוד בעלת מעמד חוקתי על-חוקי עם חקיקת חוק יסוד: כבוד האדם וחירותו בשנת 1992. עוד קודם לכן, בשנת 1981, נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), מתוך הכרה של המחוקק כבר אז בסכנה לפגיעה בפרטיות לנוכח ריבוי אמצעי התקשורת ההמוניים, ההתפתחות הטכנולוגית והתרחבות האיסוף והריכוז של מידע בידי גורמים ציבוריים ופרטיים[11]. במסגרת החוק נקבעו כללים בכל הנוגע להחזקת מאגר מידע על ידי גוף ציבורי ולאופן השימוש בו.

בחוק הגנת הפרטיות נקבעה החובה לאבטח את המידע שבמאגר המידע. בשנת 2017 הותקנו באישור ועדת חוקה, חוק ומשפט של הכנסת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע), והן נכנסו לתוקף במאי 2018. התקנות נועדו לצקת תוכן לעקרונות שנקבעו בחוק הגנת הפרטיות בדבר האחריות לאבטחת מידע במאגר המידע, והן כוללות, בין היתר, את חובותיו של ממונה אבטחת מידע, ובכלל זה החובות לקבוע נוהל אבטחת מידע, לערוך מסמך הגדרות מאגר הכולל מידע על סיכונים עיקריים של פגיעה באבטחת מידע, למפות את מערכות מאגר המידע, וכן החובות לניהול כוח האדם החשוף למאגר, לניהול הרשאות הגישה למאגר המידע, לתיעוד אירועי אבטחה והחובות בעניין השימוש בשירותי מיקור חוץ.

הגוף המסדיר את חוק הגנת הפרטיות בישראל, המפקח על יישומו והאוכף אותו הוא הרשות להגנת הפרטיות במשרד המשפטים, שהוקמה מכוח החלטת ממשלה בשנת 2006[12]. כמו כן, מכוח החלטת ממשלה בשנת 2015 (להלן - החלטת ממשלה 2443) הוקמה היחידה להגנת הסייבר בממשלה (להלן - יה"ב), הפועלת במסגרת רשות התקשוב הממשלתי במשרד הדיגיטל הלאומי, על מנת לשמש גוף מכווין ומנחה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך[13].

על פי תקנות אבטחת מידע, המערכת התפעולית של המג"ק מוגדרת כמאגר מידע שחלה עליו חובת אבטחה ברמה "גבוהה". בשל הגדרה זו חלות על המג"ק חובות נוספות ומוגברות בכל הנוגע לניהול המערכת, ובין היתר חובות הנוגעות לאופן זיהוי המשתמשים בעת הגישה למאגר,

10 מבקר המדינה, **דוח שנתי 73א** (2023), "המרכז לגביית קנסות ברשות האכיפה והגבייה".

11 דברי הסבר להצעת חוק הגנת הפרטיות, התש"ם-1980, הצעת חוק (להלן גם - ה"ח) 1453, עמ' 206.

12 החלטת הממשלה 4660 (19.1.06). תחילה היה שמה של הרשות "הרשות המשפטית לטכנולוגיות מידע והגנת הפרטיות", ובהמשך שונה שמה ל"הרשות להגנת הפרטיות".

13 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

ניהול מנגנון תיעוד (Log[14]) שיאפשר בקרות על הגישה למאגר המידע, וביצוע ביקורות תקופתיות לפחות אחת ל-24 חודשים בשל הצורך לוודא את קיומם ותקינותם של אמצעי האבטחה. זאת בין היתר כדי לאתר שימוש לרעה במידע שבמאגר[15].

תיעוד הגישה למידע במערכת התפעולית של המג"ק והבקרה עליה

בהחלטת ממשלה 2443 משנת 2015 נקבע כי כלל משרדי הממשלה ויחידות הסמך נדרשים להגדיר תוכנית מדורגת ל"הטמעה, התעדה והסמכה" בעניין תקן אבטחת מידע ארגוני 27001 ISO (להלן - תקן ISO 27001), שהוא תקן בין-לאומי העוסק במיסוד מערכת לניהול אבטחת מידע ארגונית ובתהליך השוטף של ניהול המערכת ושיפורה[16]. בשנת 2016 הוסמכה רשות האכיפה והגבייה לראשונה כעומדת בדרישות תקן ISO 27001. כמו כן הוסמכה הרשות כעומדת בדרישות תקן ISO 27032 לאבטחת סייבר.

על פי תקן ISO 27001, על הארגון לקבוע מדיניות לביצוע בקרה על גישת המשתמשים למערכות המידע, שתתבסס על דרישות אבטחת מידע ועל דרישות "עסקיות" (דרישות הנוגעות לצורך שהמערכת אמורה למלא, כפי שהוגדר על ידי הלקוח).

בשנת 2016 קבעה רשות האכיפה והגבייה נוהל שעניינו "מדיניות אבטחת מידע וסייבר" (להלן - נוהל מדיניות אבטחת מידע), ובו נקבע כי יש לתעד גישה למידע רגיש (המונח "מידע רגיש" הוגדר ככולל, בין היתר, "מידע שלא הותר לפרסום בהתאם להליך המקובל") על ידי המשתמשים במערכת, תוך שהתיעוד יבחין בין שינוי נתונים לבין צפייה בהם. כמו כן נקבע כי יבוצעו בקרות המאפשרות זיהוי חד-ערכי של משתמשים שניגשו למידע רגיש.

על הערך הרב שיש לתיעוד הגישה של משתמשים למאגר מידע של גוף ציבורי ניתן ללמוד מהדוגמה הזאת: בדיון בוועדת המדע והטכנולוגיה של הכנסת נדונו מקרים שהתגלו ברשות ציבורית, ובמסגרתם 50 עובדים ביצעו שאילתות במאגר המידע של הרשות שלא לצורך עבודתם. חיפושים אלו לא היו מתגלים אילולא היו מתבצעים תיעוד ובקרה של חיפושים במאגר המידע והמידע שנצפה[17].

14 קובץ שבו נרשמים אירועים חשובים בפעולת המערכת לשם בקרה על פעולת המערכת ולמטרות נוספות.

15 דברי ההסבר לטיוטת התקנות, כפי ששלחה שרת המשפטים דאז ליו"ר ועדת החוקה, חוק ומשפט דאז, ח"כ סלומינסקי, ב-11.5.16, עמ' 1.

16 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15). תקן ISO 27001 אומץ על ידי מכון התקנים הישראלי בפברואר 2007 ואומץ שוב בדצמבר 2020 (המהדורה השנייה מ-1.10.13, שאומצה בדצמבר 2000).

17 פרוטוקול דיון ועדת המדע והטכנולוגיה של הכנסת מ-18.7.17, עמ' 6.

בביקורת עלה כי המג"ק אינו מתעד את המסכים שבהם צפו המשתמשים במערכת התפעולית שלו ואת החיפושים שעשו בה, ולפיכך אין באפשרותו לבצע בקרה על הגישה של משתמשי המערכת למידע הקיים בה, כנדרש על פי תקנות אבטחת מידע ועל פי תקן ISO 27001. במצב דברים זה, גם אם קיימות חריגות של משתמשים, אין אפשרות לאתרן ולהפסיקן.

כדי להבטיח כי הגישה למערכת התפעולית של המג"ק, הכוללת מידע רגיש על חייבים, תינתן אך ורק לצורכי עבודה, על המג"ק להקים מערכת לתיעוד הגישה של משתמשי המערכת התפעולית שלו למידע במערכת ולבצע בקרה עיתית על הגישה למידע, על פי הוראות תקנות אבטחת המידע ותקן ISO 27001.

המג"ק מסר בתשובתו כי הוא מקבל את הערת משרד מבקר המדינה, וכי במסגרת תוכנית העבודה של שנת 2023 הוא יפעל לפיתוח מנגנון לתיעוד היסטוריית צפיות. כמו כן נמסר כי בדצמבר 2022 פורסם מכרז לביצוע בקרה נוספת על המשתמשים במערכת באמצעות מערכת לתיעוד מסכים, ובכלל זה על המשתמשים הצופים בנתונים שבמערכת, וכי הצפי לסיום המכרז הוא מרץ 2023.

תיעוד ביצוע פעולות במערכת התפעולית של המג"ק ובקרה עליהן

על פי תקנות אבטחת מידע, על בעל מאגר המידע לקבוע נוהל אבטחת מידע שבמסגרתו יפורט, בין היתר, אופן הבקרה על השימוש במאגר המידע. בהנחיית יה"ב 5.2 שעניינה "הנחיית מסגרת להגנת הסייבר בממשלה"[18] (להלן - הנחיית יה"ב 5.2) נקבע כי איתור ניסיונות לבצע פעולות לא-מורשות במערכת יתבצע, בין היתר, באמצעות ניתוח בדיעבד ובזמן סמוך ככל שניתן לזמן אמת של הלוגים במערכות.

במג"ק הגדירו בשנת 2016 אפשרות להפיק דוח המכונה "דוח אירועים חריגים", הכולל דיווחים על 13 אירועים עסקיים שהוגדרו כאירועים חריגים במערכת התפעולית של המג"ק הדורשים בחינה פרטנית אם היו מוצדקים[19]. בין האירועים שהוגדרו: סגירת תיק ללא תשלום בסכום העולה על סכום שנקבע, שינוי סכום קרן החוב ושינוי סוג חישוב. גישה לדוח ניתנה למנהל המג"ק, למנהל תחום שיטות, תהליכים ופניות, למנהל תחום בקרות ולרואה חשבון חיצוני המבצע בקרות במג"ק.

יובהר כי ייתכן שאירוע שככלל יוגדר כחריג, במקרים מסוימים לא ייחשב כחריג בשים לב לתפקידו של העובד הספציפי.

18 עודכנה ביום 3.9.20.

19 יש לציין כי אירועים אלה הם שינויים שהתבצעו תוך כדי העבודה במערכת ולא אירועים "תשתיתיים" של המערכת, שמדווח עליהם ישירות ל"מרכז השליטה והבקרה למול איומי סייבר ממשלתי" (ה-SOC הממשלתי).

תחקור אירועים חריגים במערכת

נמצא כי אף שמדובר באירועים שהוגדרו על ידי הנהלת המג"ק כחריגים, הדורשים בדיקה פרטנית, ואף שחשוב לנתח אירועים חריגים בסמוך ככל הניתן לזמן התרחשותם, כפי שעולה גם מהנחיית יה"ב, בפועל דוחות אירועים חריגים נבדקים בתדירות נמוכה, באופן שאחת לחודש מיוצא מהמערכת דוח אירועים חריגים ובו מרוכזים האירועים שהתרחשו בחודש שקדם לו. מתוך הדוח האמור נבדקים כשני סוגי אירועים לכל עובד ששמו מופיע בדוח האירועים החריגים של אותו חודש. על פי נתוני המג"ק, בספטמבר 2022 תועדו 1,391 אירועים חריגים, מהם נבדקו 99 (7%) אירועים בלבד.

רשות האכיפה והגבייה מסרה למשרד מבקר המדינה במהלך הביקורת כי היא ערה לכך שכיום היכולת לתחקר דוח אירועים חריגים ולהבין אילו התרעות בדוח אכן אינן תקינות נמוכה מאוד. הרשות עדכנה בתשובתה כי בנובמבר 2022 גויס "חוקר אירועים" שתפקידו יהיה לתחקר באופן שוטף את האירועים החריגים הן במערכת התפעולית של המג"ק והן במערכת "כלים שלובים", שהיא המערכת התפעולית של ההוצאה לפועל שברשות האכיפה והגבייה, וכי תינתן לנושא עדיפות במהלך שנת 2023.

העובדה שבמשך שנים לא התקיימה בקרה הולמת על הצפייה והשימוש של משתמשי המערכת התפעולית של המג"ק בנתונים הרגישים שהיא כוללת ועל השינויים שהזינו למערכת אינה עולה בקנה אחד עם הוראות תקנות אבטחת מידע המסווגות את המערכת התפעולית של המג"ק כמאגר שמחייב רמת אבטחה גבוהה.

מבקר המדינה רואה בחיוב את גיוסו של חוקר אירועים שיהיה אחראי לבדיקת האירועים החריגים. על המג"ק לוודא כי חוקר האירועים יונחה ויוכשר כדי לבצע בקרה איכותית ושוטפת על האירועים החריגים, וכי יועמדו לרשותו האמצעים הנדרשים לכך. בהתאם לממצאיו ואם יתגלו מקרים הדורשים טיפול, תידרש הנהלת המג"ק לפעול כדי להבטיח כי השימוש במערכת התפעולית של המג"ק ייעשה בהתאם להוראות הדין.

עדכון רשימת האירועים החריגים

בביקורת פנים שבוצעה באפריל 2021 בתחום סגירת התיקים במג"ק צוין כי חסרות התרעות בתחום סגירת התיקים, ובין היתר התרעות על תיק סגור שנפתח מחדש, העברה כספית בין תיקים סגורים או סגירת תיק באיחור של מעל 180 ימים מיום קליטת התשלום המלא בתיק. לנוכח האמור הומלץ לשקול הוספת התרעות לדוח האירועים החריגים.

חרף הממצאים שהעלה מבקר הפנים של רשות האכיפה והגבייה באפריל 2021 בדבר חסר בהתרעות במערכת התפעולית של המג"ק על אירועים חריגים (כדוגמת ביטול תשלום והעברת כספים מתיקים סגורים), המג"ק לא עדכן את רשימת האירועים החריגים במערכת שהתקיימותם מצדיקה בדיקה פרטנית. נמצא כי רשימה זו לא עודכנה מאז תחילת העבודה באופן זה בשנת 2016. בנסיבות אלו, אירועים חריגים שמתרחשים אך אינם נכללים ברשימה זו אינם מנוטרים ולא נבדק אם הם מוצדקים.

מומלץ כי המג"ק יבחן את הצורך לטייב את רשימת האירועים החריגים ובכלל זה להגדיר אירועים נוספים כאירועים חריגים המצדיקים בדיקה פרטנית כדי לוודא שהם בוצעו בהתאם לנהלים.

המג"ק מסר בתשובתו כי חוקר האירועים שגויס יקדם את הטיפול בנושא בסיוע הגורמים המקצועיים, וכן יוגדרו בנוהל האחריות לבקרת האירועים, תדירות הבקרה, אחריות הגורם המקצועי ועוד.

ניהול תהליך מתן הרשאות הגישה למערכות המג"ק

נוהל מתן ההרשאות

בהנחיית יה"ב 5.2 נקבע העיקרון של "הפרדת סמכויות", ועל פיו בתהליכים רגישים במשרד ממשלתי או ביחידת סמך אדם אחד לא יוכל לבצע לבדו תהליך מלא. כמו כן נקבע כי לצורך מימוש עקרון הפרדת הסמכויות, על מערכות המחשוב השונות לתמוך בהפרדת הסמכויות המוגדרות במשרד. עיקרון זה נקבע גם בתקן ISO 27001[20].

בדומה לכך, בנוהל מדיניות אבטחת מידע של רשות האכיפה והגבייה נקבע כי נדרשת הפרדת תפקידים בין בעל תפקיד לאחראי ביצוע, באופן שלא יתאפשר מצב שבו גורם אחד מחליט על ביצוע פעולה רגישה ומבצע אותה בעצמו. הוראה זו נקבעה גם בכל הנוגע למתן הרשאות גישה.

כמו כן קבעה רשות האכיפה והגבייה בשנת 2013 נוהל ספציפי שעניינו "ניהול הרשאות למערכת" (להלן - נוהל ההרשאות של רשות האכיפה והגבייה). המג"ק קבע אף הוא "נוהל בקשת הרשאות למערכות מידע", הכפוף לנוהל ההרשאות של רשות האכיפה והגבייה (להלן - נוהל ההרשאות של המג"ק).

על פי נוהל ההרשאות של רשות האכיפה והגבייה, כאשר נדרשת הגדרת הרשאות למשתמש חדש או שינוי הרשאות למשתמש קיים, ממלא סגן מנהל המג"ק טופס מתן הרשאות למערכת התפעולית של המג"ק. הטופס מועבר למינהלן ההרשאות ברשות, שהוא עובד אגף אבטחת מידע ברשות (שאינו עובד מחשוב), האחראי לאישור סופי למתן הרשאות לכלל מאגרי המידע שבשימוש עובדי רשות האכיפה והגבייה (להלן - מינהלן ההרשאות), ואינו כפוף לסגן מנהל המג"ק. על פי הנוהל, "**מנהלן ההרשאות (ורק הוא) יעביר בקשה אל עובדי המחשוב לצורך פתיחת ההרשאה הנדרשת**[21]" (ההדגשה במקור). תהליך זה תומך בעקרון "הפרדת הסמכויות", הנדרש לצורך קיומה של בקרה תקינה על תהליך מתן ההרשאות, כפי שנקבע בהנחיית יה"ב.

20 הוראה דומה נקבעה בתקן NIST SP.800-192 (תקן המכון הלאומי לתקנים וטכנולוגיה של ארה"ב).

21 עובדי מערכות המידע ברשות האכיפה והגבייה המתפעלים, בין היתר, את המערכת התפעולית של המג"ק.

יש לציין כי נוהל ההרשאות של המג"ק הוכן לאחר שהוטמעו ברשות האכיפה והגבייה שתי מערכות: מערכת א' - שהיא מערכת לניהול בקשות ואישורים, שכל הבקשות מועברות למינהלן ההרשאות באמצעותה, ומערכת ב' - שהיא מערכת ליישום ההרשאות בפועל.

תרשים 2: **תהליך מתן ההרשאות בפועל למערכת התפעולית של המג"ק**

על פי נתוני המג"ק, בעיבוד משרד מבקר המדינה.

על אף האמור בנוהל ההרשאות של רשות האכיפה והגבייה, על פי נוהל ההרשאות של המג"ק והמצב בפועל, לאחר שמינהלן ההרשאות אישר בקשה למתן ההרשאה, הוא מחזיר אותה למרכז ההרשאות במג"ק[22], והוא שפותח את ההרשאות בפועל במערכת, ולא עובדי המחשוב של רשות האכיפה והגבייה.

מומלץ כי המג"ק יתקן את נוהל ההרשאות ויפעל על פי נוהל ההרשאות של רשות האכיפה והגבייה באופן שבו רק מינהלן ההרשאות יפתח את ההרשאות בפועל במערכת, על מנת לשמור על עקרון הפרדת הסמכויות ולמנוע מצב אפשרי של פתיחת הרשאות ללא קבלת אישור מינהלן ההרשאות.

בדיקת מינהלן ההרשאות לפני אישור הבקשה

בביקורת נמצא כי במערכת א' אשר משמשת לניהול תהליך העברת הבקשות למינהלן ההרשאות אין מידע על תפקידו של המשתמש ועל ההרשאות שקיימות עבורו במערכת[23], וכי למינהלן ההרשאות אין גישה למערכת "מרכב"ה"[24] על מנת שיוכל לבדוק מהו תפקידו של המשתמש. לפיכך מינהלן ההרשאות מאשר את הבקשה למתן הרשאות באופן אוטומטי, בהסתמך על האישור שנתנה סגנית מנהל המג"ק, ובלא שנבחן שוב אם היקף ההרשאות המבוקש תואם את הגדרות התפקיד של המשתמש ונדרש לצורך ביצוען.

יש לציין כי כבר בשנת 2015 המליץ מבקר הפנים של רשות האכיפה והגבייה שאישור מינהלן ההרשאות יינתן לאחר בחינת סוגי ההרשאות המבוקשות, "תוך עמידה בעקרון הפרדת תפקידים ולא על סמך קיומן של חתימות הגורמים הממונים בלבד". כמו כן הציע כי ליחידת אבטחת המידע ברשות האכיפה והגבייה תינתן גישה לצפייה בפרופיל המשתמשים במג"ק, באופן שתתאפשר בקרה יזומה ושוטפת על ההרשאות של המשתמשים.

מוצע כי רשות האכיפה והגבייה תפעל לכך שתינתן למינהלן ההרשאות גישה למידע הרלוונטי במערכת מרכב"ה, כדי שיוכל לצפות במידע על תפקידי העובדים שעבורם מתבקשות ההרשאות, וכי היא תנחה את מינהלן ההרשאות לבדוק אם היקף ההרשאות המבוקש תואם את הגדרות התפקיד של המשתמש ונדרש לצורך ביצוע תפקידו.

רשות האכיפה והגבייה מסרה בתשובתה כי הנושא יחודד מול מינהלן ההרשאות, כדי שיוכל, בין היתר, לבחון את הבקשות לפני אישורן.

22 עובד המג"ק האחראי לטיפול בבקשות למתן הרשאות למערכת התפעולית של המג"ק.

23 אם מבוקשות הרשאות עבור משתמש קיים שנדרש לשינוי הרשאות.

24 מרכב"ה (מערכת רוחבית כוללת במשרדי הממשלה) היא יחידה בחשכ"ל האחראית לפיתוח, לתחזוקה ולהטמעה של מערכת רוחבית ארגונית לניהול נכסי המדינה ומשאביה, הנמצאת בשימושם של רוב משרדי הממשלה ויחידות הסמך (למעט המגזר הביטחוני).

פתיחת ההרשאות במערכת התפעולית של המג"ק

הועלה כי אין ממשק בין מערכת א' (שבאמצעותה ניתן אישור מינהלן ההרשאות) לבין מערכת ב' (שבאמצעותה מיושמות ההרשאות בפועל על ידי מרכז ההרשאות). היעדר ממשק כאמור מאפשר למעשה לפתוח הרשאות לעובדים, בלי שניתן לכך אישורו של מינהלן ההרשאות.

בביקורת נמצא כי מתוך 44 הרשאות שנפתחו במערכת ב' בשנת 2021[25], 23 הרשאות (52%) נפתחו בלי שהתבקש עבורן אישור ממינהלן ההרשאות. אחת מן ההרשאות שנפתחה באופן זה היא הרשאה נוספת של עובדת במג"ק לעצמה.

מומלץ כי רשות האכיפה והגבייה תדאג להקים ממשק ישיר בין מערכת א' למערכת ב', על מנת שלא ניתן יהיה לפתוח הרשאה במערכת ב' בלא שמינהלן ההרשאות יעשה בקרה על כך ויאשר את פתיחתה באמצעות מערכת א'. גם בהיעדרו של ממשק כזה, על מרכז ההרשאות במג"ק להקפיד שלא לפתוח הרשאות אם מינהלן ההרשאות לא אישר את פתיחתן.

רשות האכיפה והגבייה מסרה בתשובתה כי מינהלן ההרשאות יחדד את הנוהל הנוגע לאופן פתיחת ההרשאות מול המג"ק. כמו כן מסרה כי תבחן את האפשרות להקמת ממשק ישיר בין מערכת א' למערכת ב'.

בקרה על ההרשאות הפעילות במערכת התפעולית של המג"ק

על פי הנחיית יה"ב 5.12, שעניינה "ניהול ותפעול הרשאות"[26] (להלן - הנחיית יה"ב 5.12), יש לבצע בקרה והסרת הרשאות לא נחוצות אחת לשנה. גם בהתאם לנוהל ההרשאות של רשות האכיפה והגבייה, על מינהלן ההרשאות לבצע הסרת הרשאות אחת לשנה, וזאת מעבר להסרת הרשאות לגבי עובד העוזב את תפקידו או לבדיקת הרשאות עודפות לעובד העובר תפקיד.

25 בביקורת נבדקו הרשאות שנפתחו בשנת 2021, משום שהמג"ק החל לעבוד באמצעות מערכת ב' ביולי 2020.

26 הנחיה מ-10.9.17, שעודכנה ב-20.4.20.

בביקורת נמצא כי החל ביולי 2020, מועד תחילת עבודת המג"ק באמצעות מערכת ב', ועד מועד סיום הביקורת באוקטובר 2022, לא בוצעה בקרה על ההרשאות שנפתחו במערכת ב', ובפרט לא נבחן אם ההרשאות ניתנו בהליך תקין בהתאם לנהלים וכן אם יש צורך בהסרת הרשאות (נוכח אי-התאמה למהות התפקיד או עקב מעבר תפקיד)[27]. זאת, הגם שנדרשת בקרה כאמור בייחוד על מערכות מידע שמנהלות מאגר נתונים עצומים בהיקפם, הכוללים מידע רגיש ואישי, כדוגמת נתוני המג"ק. יתרה מזו, נמצא כי למינהלן ההרשאות, האמון על ביצוע הבקרות על ההרשאות במערכת, לא הוקנתה הרשאת צפייה במערכת ב' לצורך ביצוע הבקרה.

על רשות האכיפה והגבייה לבצע בקרות עיתיות על מערך ההרשאות של עובדי המג"ק, בהתאם להנחיית יה"ב ולנוהלי רשות האכיפה והגבייה.

רשות האכיפה והגבייה מסרה בתשובתה כי הנושא יחודד מול מינהלן ההרשאות והמג"ק, ובין היתר תטפל בנושא הגדלת תדירות הבקרה על הסרת הרשאות.

היקף הרשאות הגישה למערכת התפעולית של המג"ק

על פי תקנות אבטחת מידע, על בעל מאגר המידע לקבוע הרשאות גישה למאגר המידע "בהתאם להגדרות תפקיד" ו"במידה הנדרשת לביצוע התפקיד בלבד". זאת בהתאם לגישת "הצורך לדעת" (Need To Know) ועל מנת שהיקף הגישה למערכות המאגר הניתן לעובד יהיה ההיקף הנדרש לו לצורך מילוי תפקידו ולא מעבר לכך[28]. בהתאם לכך נקבע בהנחיית יה"ב 5.12[29] כי ההרשאות למאגר המידע יינתנו על בסיס תפקיד העובד. בכל הנוגע להרשאות גישה למידע במאגר שלעובד יש גישה אליו, ייקבעו ההרשאות על פי עקרון "הצורך לדעת" (ובכל הנוגע להרשאות לביצוע פעולות, להבדיל מצפייה בלבד, על פי מינימום ההרשאות הנדרש לשם ביצוע העבודה).

ואכן, בנוהל מדיניות אבטחת מידע של רשות האכיפה והגבייה נקבע כי יש לבצע מיפוי הרשאות על פי חלוקת המידע והמשתמשים לקבוצות שייכות, וכי הרשאות הגישה למידע יינתנו בהיקף הנדרש לביצוע העבודה בלבד ועל פי עקרון "הצורך לדעת".

27 יש לציין כי במהלך הביקורת בוצעה בקרה ובה נבחן אם קיימות הרשאות פעילות לעובדים שסיימו את עבודתם במג"ק.

28 דברי ההסבר לטיוטת התקנות, כפי ששלחה שרת המשפטים דאז ליו"ר ועדת החוקה, חוק ומשפט דאז, ב-11.5.16, עמ' 6.

29 ראו גם הנחיית יה"ב 5.2.

בביקורת נמצא כי כל עובדי המג"ק הם בעלי גישה למלוא המידע במערכת התפעולית של המג"ק על כל החייבים שנתוניהם שמורים במערכת, בלי שנבחן אם היקף הגישה למידע נחוץ על פי הגדרת תפקידם, וזאת שלא בהתאם לתקנות אבטחת מידע ואף שמדובר במאגר מידע רחב היקף ורגיש הכולל פרטים אישיים בנוגע לכ-3 מיליון חייבים. למשל, לכל עובדי המג"ק יש גישה גם למידע בנוגע לחייבי עבר, שאין להם תיקים פתוחים במג"ק.

יש לציין כי בסקר סיכונים שבוצע עבור המג"ק על ידי משרד רואי חשבון חיצוני באפריל 2019 נמצא סיכון גבוה בניהול הרשאות הגישה למערכת התפעולית של המג"ק. בסקר צוין כי נשקף סיכון לזליגת מידע על ידי משתמשים בלתי מורשים עקב מתן הרשאות עודפות.

אף שבסקר הסיכונים של המג"ק משנת 2019 נמצא סיכון גבוה באופן ניהול ההרשאות במערכת התפעולית של המג"ק, במועד סיום הביקורת (אוקטובר 2022) עדיין לא בחן המג"ק את היקף הרשאות הגישה למידע בקרב משתמשי המערכת התפעולית של המג"ק ואת התאמתו לתפקיד שהם מבצעים. לליקוי זה משנה חשיבות, מאחר שכפי שפורט לעיל, לא מתבצעים תיעוד או בקרה בעניין הגישה בפועל של המשתמשים לנתונים במערכת התפעולית של המג"ק.

המערכת התפעולית של המג"ק הוגדרה על פי תקנות אבטחת מידע כמאגר שמחויב ברמת האבטחה הגבוהה ביותר. על המג"ק ורשות האכיפה והגבייה לבצע בחינה של היקף הרשאות הגישה למערכת התפעולית של המג"ק לעובדים בתפקידים השונים, ובכלל זה עליהם לבחון את האיזון בין אופי התפקיד וצורכי התפקיד לבין הצורך בשמירה על פרטיותם של מושאי המידע במערכת והצורך לעמוד בדרישות הדין. זאת על מנת לצמצם את הסיכון לזליגת מידע או לשימוש לא הולם בו.

רשות האכיפה והגבייה מסרה בתשובתה כי היא תבחן את היקף הרשאות הגישה למערכת, ובמידת הצורך תבצע פיתוח מחשובי מתאים להגבלת הצפייה של המשתמשים במערכת, בהתאם לתפקידם.

ניהול ההרשאות של עובדי מוקד המידע הטלפוני והיקפן

מוקד המידע הטלפוני של המג"ק (להלן - המוקד) מנוהל כחלק ממוקד המידע הטלפוני של רשות האכיפה והגבייה. המוקד מתופעל בשיטת מיקור חוץ על ידי חברה א', והוא מנוהל מהבחינה המקצועית על ידי עובדת של רשות האכיפה והגבייה.

הליך מתן הרשאות גישה למערכת התפעולית של המג"ק לעובדי המוקד הטלפוני

בביקורת פנים שביצעה רשות האכיפה והגבייה בדצמבר 2015 נמצאו אי-התאמות בין רשימות העובדים הפעילים של מוקד המידע שנוהלו על ידי מנהל המוקד לרשימות עובדי המוקד שנמצאו בידי הנהלת המג"ק ולרשימות העובדים בעלי ההרשאות למערכת על פי מערכות המידע. על כן הומלץ כי תהליך מתן הרשאות הגישה למערכת לעובדי מוקד המידע יבוצע באמצעות מינהלן ההרשאות ברשות האכיפה והגבייה.

גם בהתאם לנוהל ההרשאות של המג"ק, כמפורט לעיל, בקשה למתן הרשאה עבור עובדי המוקד צריכה להתבצע באמצעות מערכת א' - מערכת הבקשות והאישורים ובהתאם לשלבים שהוגדרו בנוהל. כמו כן נקבע כי ההרשאות שיינתנו למוקדנים יוגבלו לתקופה של חצי שנה.

בביקורת נמצא כי ניתנו הרשאות למערכת התפעולית של המג"ק לכל 94 עובדי המוקד בלי שניתן אישור של מינהלן ההרשאות ברשות האכיפה והגבייה, וזאת שלא בהתאם לנוהל ההרשאות של המג"ק. כמו כן, אף שתוקף ההרשאה לעובדי המוקד אמור להיות מוגבל לחצי שנה בלבד, נמצא כי הגבלת תוקף ההרשאה לחצי שנה אינה חוסמת בפועל את ההרשאה, וזאת שלא בהתאם לנוהלי המג"ק. למשל נמצאו 45 הרשאות אשר מסווגות ברשימת ההרשאות של אגף מערכות מידע[30] ככאלה שאינן בתוקף אף שבפועל הן אינן חסומות ומתאפשרת באמצעותן גישה למערכת התפעולית של המג"ק.

רשות האכיפה והגבייה מסרה בתשובתה כי היא תבחן את הנושא, וכי היא מקדמת אפיון של התהליך.

הסרת הרשאות גישה למערכת התפעולית של המג"ק לעובדי המוקד הטלפוני

כאמור, בהנחיית יה"ב 5.12 נקבע כי יש לבטל הרשאות של עובדים שעוזבים את הארגון. הוראה דומה נקבעה בתקן ISO 27001.

בביקורת נמצאו 14 עובדי מוקד לשעבר שהרשאות הגישה שלהם למערכת התפעולית של המג"ק לא הוסרו חרף סיום עבודתם בטווח של חודש עד 13 חודשים לפני מועד הביקורת. במצב דברים זה, ניתן להשתמש בהרשאות המערכת שלהם לצורך כניסה למערכת התפעולית של המג"ק ואף לבצע פעולות בשמם.

30 האחראי לפתיחה ולסגירה של ההרשאות.

שיוך "כרטיס חכם" לעובדי המוקד הטלפוני

על מנת להיכנס למחשבי המוקד, מקבלים עובדי המוקד "כרטיס חכם", המשויך לכל אחד מהם. שיוך הכרטיס לכל עובד באופן אישי מאפשר זיהוי חד-ערכי של המשתמש ובקרה על ההרשאות כפי שמחויב במאגר מידע ברמת אבטחה גבוהה. עם הכניסה למחשב באמצעות הכרטיס החכם, מתאפשרת גישה אוטומטית למערכת התפעולית של המג"ק וכן למאגר "CRM מוקד" - מאגר מידע השואב מידע הן מהמערכת התפעולית של המג"ק והן ממאגר המידע של ההוצאה לפועל בדבר מספרי הזהות של הפונים, כתובותיהם, מספרי הטלפון שלהם, כתובות הדוא"ל שלהם (אם הן שמורות במערכת), וכן רשימת התיקים בהוצאה לפועל ובמג"ק, לרבות מספר התיק, סוג התיק וסכום החוב בגין התיק.

בביקורת נמצא כי המג"ק לא פעל לחסימת כרטיסים חכמים של עובדים שסיימו את עבודתם במוקד, ובפועל במוקד קיימים כרטיסים חכמים פעילים המשויכים לעובדים שסיימו את עבודתם במוקד, וצוות המוקד משתמש בהם ובסיסמאות של עובדים אלה בעת קבלת עובד חדש עד לשלב שבו משויך לאותו עובד כרטיס חכם אחר, או כאשר כרטיס חכם של עובד אחר נחסם מסיבה כלשהי.

נמצא כי מתוך 76 כרטיסים חכמים פעילים שהיו משויכים לעובדי המוקד במועד הביקורת, ארבעה (5%) שויכו לעובדים שסיימו את עבודתם במוקד[31], ובשניים מהכרטיסים אף נעשה שימוש לצורך חיבור למחשב לאחר שהעובדים סיימו את עבודתם במוקד. עוד נמצא כי מתוך 94 עובדי מוקד, ל-20 (21%) לא שויכו כרטיסים חכמים ולפיכך הם אינם משתמשים בכרטיס חכם אישי על שמם כדי לבצע את עבודתם, אף על פי שחלקם כבר עובדים במוקד שנים אחדות. לנוכח האמור, נפגעת האפשרות לבצע בקרה על כניסת העובדים למערכות המג"ק ואף היכולת לנטר פעולות שבוצעו על ידי אותם עובדים.

היקף הרשאות הגישה של עובדי המוקד הטלפוני

בנוהל מדיניות אבטחת מידע של רשות האכיפה והגבייה נקבע כי החשיפה של עובדי חברות חיצוניות למידע ולמערכות של הארגון תהיה מצומצמת ומבוקרת במידת האפשר, וכי היא תתבסס על יישום מחמיר של עקרון "הצורך לדעת", באופן שבו כל עובד יקבל גישה רק למידע הנחוץ לביצוע תפקידו, והעיקרון של "מינימום הרשאות" גישה לצורך ביצוע עבודתו יוחל במידת האפשר.

מוקד המידע משתמש במערכת "CRM מוקד"[32] לצורך זיהוי הפונים למוקד. עובדי המוקד, שהם כאמור עובדים במיקור חוץ, מקישים במערכת פרטים מזהים של הפונה על פי מידע שהפונה מוסר (מספר הזהות, תאריך הלידה, תאריך הנפקת תעודת הזהות ומספר התיק במג"ק)

31 בטווח של חודשיים עד יותר משנתיים ממועד הביקורת.

32 Customer relationship management (מערכת קשרי לקוחות). מדובר במערכת לניהול עבודת המוקד, השואבת נתונים מהמערכת התפעולית של המג"ק, ממאגר המידע של ההוצאה לפועל וממאגר מרשם האוכלוסין, וכוללת פרטים אישיים של החייבים וכן פירוט של התיקים שלהם במג"ק ובהוצאה לפועל.

ומקבלים מהמערכת מענה אם הפונה זוהה או לא. כמו כן, לעובדי המוקד הרשאת גישה למערכת התפעולית של המג"ק, המאפשרת חיפוש מידע על חייבים על פי מספר זהות.

בביקורת נמצא כי הרשאות עובדי המוקד לעיון במידע השמור במערכת התפעולית של המג"ק אינן מוגבלות למידע על מי שפנה למוקד וזוהה באמצעות מערכת "CRM מוקד", אף שהגבלה זו אפשרית מהבחינה הטכנולוגית.

על מנת לשמור על פרטיות החייבים ועל עקרון "הצורך לדעת" המחמיר, בייחוד בהתייחס לעובדי חברות חיצוניות, מוצע כי המג"ק יבחן אם יש מקום להגביל את אפשרויות הגישה של עובדי מוקד המידע הטלפוני למערכת התפעולית של המג"ק על בסיס הפניות המתקבלות במוקד, ובין היתר יבחן את האפשרות להקמת ממשק חוזר בין מערכת "CRM מוקד" לבין המערכת התפעולית של המג"ק, באופן שבו המידע על הפונה במערכת התפעולית של המג"ק ייפתח לצפייה רק עם זיהוי הפונה במערכת "CRM מוקד". בעניין זה יהיה מקום לבחון אם לעיתים אכן נחוצה לעובד המוקד גישה לתיקים של פונה אף שלא זוהה במערכת "CRM מוקד", למשל כשבא כוחו של הפונה מתקשר בשם החייב.

רשות האכיפה והגבייה מסרה בתשובתה כי תבוצע בחינה של היקף הרשאות הגישה של עובדי המוקד הטלפוני למערכת, ובמידת הצורך יבוצע פיתוח מחשובי מתאים. עוד מסרה כי לנוכח התחלופה הגבוהה יחסית של עובדי מוקד המידע הטלפוני, ייבחן נושא העבודה באמצעות כרטיס חכם במוקד המידע הטלפוני. כמו כן הציעה הרשות חלופה אפשרית - כניסה למערכת באמצעות סיסמה חד-פעמית (OTP).

על המג"ק לפעול בהתאם לנוהלי אבטחת מידע ולהקפיד על מתן הרשאות לעובדי המוקד על ידי הגורמים המוסמכים תוך גידור ההרשאות לצורכי התפקיד הספציפי; כמו כן על המג"ק לבצע בקרה עיתית על ההרשאות; לוודא כי כשעובדים מפסיקים את עבודתם במוקד יבוטלו באופן מיידי ההרשאות שניתנו להם וגם השיוך של הכרטיסים החכמים אליהם; ולהימנע מלהשתמש בהרשאות הגישה למערכת של עובדים שאינם מועסקים במוקד או מהעברת כרטיסים חכמים מעובד אחד למשנהו.

במהלך הביקורת, במאי 2022, הכינה רשות האכיפה והגבייה "נוהל אבטחת מידע למוקד המידע", ובמסגרתו נקבעו הוראות בכל הנוגע להליך מתן הרשאות לעובדי המוקד והסרתן, להליך שיוך הכרטיסים החכמים והשימוש בהם, לחובת ביצוע בקרה על יישום הנוהל ועל ביצוע אחת לשנה של סקר סיכונים ובדיקת חוסן.

משרד מבקר המדינה רואה בחיוב את הכנת הנוהל, הנותן מענה על חלק מהליקויים העולים בפרק זה. על רשות האכיפה והגבייה לוודא כי הוא מיושם בפועל, באופן שהליך מתן ההרשאות והסרתן והליך הנפקת הכרטיסים החכמים וגריסתם יבוצעו בהתאם לנוהל החדש שקבעה ויעמדו בהוראות תקנות אבטחת מידע, בהנחיות יה"ב ובתקן ISO 27001.

רשות האכיפה והגבייה מסרה בתשובתה כי תפעל לחידוד נוהל העבודה מול מינהלת מוקד המידע הטלפוני.

היקף הרשאות צוות הפיתוח

כאמור, המערכת התפעולית של המג"ק מפותחת ומנוהלת על ידי עובדי רשות האכיפה והגבייה ועובדים המועסקים במיקור חוץ כנותני שירותים.

הפיתוח והתחזוקה של המערכת התפעולית של המג"ק נחלקים לשלושה שלבים עיקריים: שלב פיתוח המערכת, שלב ביצוע הבדיקות במערכת ושלב הייצור, שבמסגרתו המערכת נמצאת בשימוש בפועל ויש לתחזק אותה. בהנחיית יה"ב בעניין פיתוח מאובטח נקבע כי יש לדאוג להפרדה מוחלטת בין סביבת הייצור לסביבת הפיתוח ולסביבת הבדיקות[33]. גם בתקן ISO 27001 נקבעה הוראה דומה, וזאת כדי להפחית את הסיכון לגישה לא-מורשית למידע או לביצוע שינויים לא-מאושרים במערכת התפעולית (שלב הייצור)[34].

גם בהנחיית יה"ב 5.13 שעניינה "פיתוח מאובטח"[35] נקבע כי הבסיס למתן הרשאות הגישה לעובדי מערכות מידע למאגר הנתונים צריך להיקבע על פי עקרון "הצורך לדעת" ועל פי מינימום ההרשאות הנדרש לצורך ביצוע התפקיד. כמו כן נקבע שאין לאפשר לתוכניתנים גישה לבסיסי הנתונים שבסביבת הייצור, וכי אין להעביר בסיסי נתונים מסביבת הייצור לסביבת הפיתוח ללא ביצוע פעולות להסתרת נתונים מזהים[36].

בנוהל מדיניות אבטחת מידע של רשות האכיפה והגבייה נקבעו הנחיות דומות, ובכלל זה נקבע בו כי מידע אמיתי יימצא רק בשרתי ייצור ובבסיסי נתונים המשרתים את הייצור, וכי בשרתי פיתוח, בדיקות והדרכה ייעשה שימוש במידע שאינו אמיתי.

בביקורת נמצא כי בסביבות הפיתוח והבדיקות של המערכת התפעולית של המג"ק קיים מידע אמת[37] שלא עבר פעולות להסתרת נתונים מזהים, שלא בהתאם לנוהל רשות האכיפה והגבייה בנושא ובאופן שחושף מידע רגיש ואישי לפני גורמים שאינם מורשים לכך, חלקם גורמים שאינם מוגדרים כעובדי מדינה (אלא כנותני שירותים בתחום פיתוח ותחזוקה של המערכת המועסקים באמצעות חברה חיצונית).

על רשות האכיפה והגבייה לפעול להסתרת הנתונים המזהים במידע הקיים במערכות הפיתוח והבדיקות ולהימנע מלתת למפתחים בשלבי הפיתוח והבדיקות גישה לנתוני אמת מסביבת הייצור.

רשות האכיפה והגבייה מסרה בתשובתה כי תבחן רכישת מוצר טכנולוגי מתאים להסתרת הנתונים המזהים בסביבת הפיתוח והבדיקות.

33 הנחיית יה"ב 5.13 מ-24.9.19.

34 ראו גם תקן NIST 800-128 בעניין פיתוח מאובטח (SSDF), P.O.5.1.

35 הנחיה 5.13 מ-24.9.19.

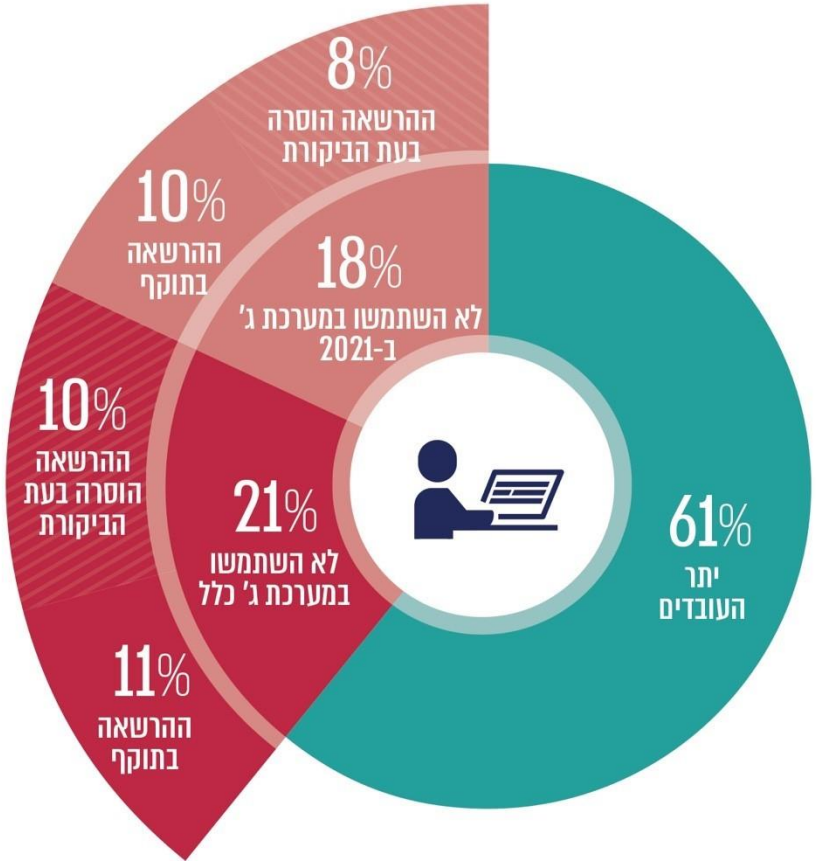
36 באמצעות התממה או ערפול של הנתונים. להרחבה ראו מילון מונחים בתחום התקשוב שמפרסמת רשות התקשוב באתר המרשתת שלה.

37 נכון ליום הקודם.

ניהול הרשאות הגישה למערכת ג'

מערכת ג' היא מערכת בינה עסקית המקושרת למערכת התפעולית של המג"ק ושואבת ממנה נתונים לצורך הפקת דוחות מובנים בתחומי פעילות המג"ק. באפשרות משתמשי מערכת ג' לצפות בנתונים על מספר רב של תיקים וחייבים ברמת-על וכן לבחון את נתוני כל תיק ותיק הכלול באותם נתונים (נתונים ברמת היחידה), לרבות המידע בעניין מספרי הזהות, סכום החוב וסיבת החוב. זאת ועוד, במערכת ג' שמור מידע על נפגעי עבירה שהמג"ק גובה עבורם את כספי הפיצויים שנפסקו להם, לרבות פרטיהם האישיים. ניהול ההרשאות למערכת ג' מבוצע על ידי מחלקת תכנון מחקר וקשרי חוץ של רשות האכיפה והגבייה.

תרשים 3: **שימוש בעלי ההרשאות למערכת ג' במערכת בשנים 2019 - 2022**



על פי נתוני המג"ק, בעיבוד משרד מבקר המדינה.

בשנים 2019 עד 2021 ניתנו הרשאות למערכת ג' עבור 52 עובדי המג"ק ורשות האכיפה והגבייה. בביקורת עלה כי מדובר בין היתר בעובדים שאופי תפקידם אינו מצריך גישה למידע שבמערכת; למשל במרכז מחסנים ברשות האכיפה והגבייה, במרכזת דיוור בחטיבת שירות לקוחות ובסטודנט שהעסקתו הסתיימה עוד בשנת 2018. הרשאות נרחבות אלו ניתנו על אף רגישות המידע שבמערכת המאפשרת להפיק דוחות רוחביים על פעילות המג"ק וכן להפיק מידע פרטני, לרבות מידע על החייבים ועל נפגעי העבירה. כמו כן, מהתרשים עולה כי על אף הצורך לנהל את ההרשאות באופן שיקטין את הסיכון לזליגת מידע ולפרצות אבטחה, קרוב ל-40% מבעלי ההרשאות למערכת ג' (20 מתוך 52) לא השתמשו במערכת ג' לכל הפחות החל משנת 2021. כמו כן, במועד הביקורת עדיין לא בוטלו הרשאותיהם של 54% מבעלי ההרשאות שלא השתמשו במערכת ג' לכל הפחות החל משנת 2021 (52% מהם לא השתמשו בה מעולם).

יצוין כי במהלך הביקורת הוסרה ההרשאה של 18% מכלל בעלי ההרשאות.

לנוכח היקף המידע הנרחב השמור במערכת ג', מומלץ כי רשות האכיפה והגבייה והמג"ק יבחנו באופן פרטני את ההרשאות הקיימות לנוכח הצורך והזיקה לתפקיד של בעל ההרשאה, כדי לצמצם את היקף בעלי ההרשאות למערכת למינימום ההכרחי. זאת בהתאם לעקרון "הצורך לדעת" שעומד בבסיס מדיניות ההרשאות שאליה מחויב כל בעל מאגר מידע על פי תקנות אבטחת מידע.

רשות האכיפה והגבייה מסרה בתשובתה כי תחדד את הנושא מול הגורם המאשר את הבקשות למתן הרשאות למערכת ג'.

התמודדות רשות האכיפה והגבייה עם סכנת חדירה למערכת התפעולית של המג"ק

הטמעת פתרון אבטחתי טכנולוגי ייעודי מסוים למערכות ולרשתות המידע הארגוניות של רשות האכיפה והגבייה

פתרון אבטחתי טכנולוגי ייעודי למערכות ולרשתות מידע ארגוניות נועד לאיתור ולניטור של מידע ומאפשר לאתר מתקפות רוגלה ונוזקה מסוגים שונים ולהגן מפניהן. על פי הנחיית יה"ב 5.9 בנושא הגנה בסייבר על מערכות ורשתות ממוחשבות, על משרדי הממשלה לבדוק תרחישי כניסה של רוגלה ולהציב פתרונות ייעודיים להגנה בסייבר באופן שיבטיח הגנה מיטבית על נכסי המידע של המשרד ושלא תיווצר נקודת כשל בודדת. עוד נקבע כי פתרון מסוים זה ינטר את המערכות והרשתות באופן שוטף וכולל.

באוקטובר 2020 ביצעה רשות האכיפה והגבייה מבדק חדירות באמצעות חברה חיצונית, בו נמצאו ליקויים ברמת הגנת התשתית. באפריל 2021 בוצע מבדק חדירות חוזר לבדיקת איכות

תיקון הליקויים שאותרו באוקטובר 2020, והוא העלה כי ממצאי הבדיקה הקודמת תוקנו באופן חלקי. ממידע שנמסר מרשות האכיפה והגבייה עולה כי עיקר הממצאים שאותרו במבדק החדירות החוזר מאפריל 2021 תוקן.

בבקרת מבדק חדירות אוטומטי שביצעה יה"ב במערכות רשות האכיפה והגבייה בנובמבר 2021, נמצאו ליקויים ברמת הגנת התשתית. לנוכח האמור קבעה יה"ב במסגרת הבקרה כי על רשות האכיפה והגבייה להטמיע פתרון אבטחתי טכנולוגי ייעודי מסוים במערכות וברשתות רשות האכיפה והגבייה על מנת לצמצם את הסיכונים הנובעים מליקויים אלה.

נמצא כי במועד סיום הביקורת רשות האכיפה והגבייה עדיין לא הטמיעה במערכותיה, ובכלל זה במערכת התפעולית של המג"ק, פתרון אבטחתי טכנולוגי ייעודי מסוים. זאת חרף הנחיות יה"ב המחייבות זאת ולמרות ההנחיה המפורשת שניתנה לרשות האכיפה והגבייה מאת יה"ב כבר בנובמבר 2021 בעקבות מבדק החדירות שביצעה.

רשות האכיפה והגבייה מסרה במהלך הביקורת באוקטובר 2022 כי לפני כחמש שנים הוטמע פתרון אבטחתי טכנולוגי חלקי[38] במערכות רשות האכיפה והגבייה, וכי רשות האכיפה והגבייה נמצאת כיום בתהליך של יציאה למכרז לצורך הטמעת פתרון אבטחתי טכנולוגי מקיף. יש לציין כי הפתרון החלקי שקיים כיום ברשות האכיפה והגבייה היה קיים עוד טרם ביצוע בקרת מבדק החדירות על ידי יה"ב בשנת 2021, ואולם הוא לא הצליח למנוע את הליקויים שנמצאו במערכת. לפיכך הנחתה יה"ב את רשות האכיפה והגבייה להטמיע פתרון אבטחתי טכנולוגי ייעודי מסוים במערכות וברשתות שלה.

רשות האכיפה והגבייה מסרה בתשובתה כי במבדק החדירות שביצעה יה"ב נמצאו ליקויים ברמת הגנת התשתית רק לאחר שהרשות ויתרה על מנגנון הגנה שמונע חיבור של מחשב זר לרשת. כמו כן מסרה רשות האכיפה והגבייה כי במהלך מבדק החדירות הועברו התרעות של מערכות האבטחה בשל פעילות הבודקים.

יה"ב מסרה בהתייחסותה מפברואר 2023 כי מטרת מבדק החדירות המבוצע על ידה היא לדמות פעולות של תוקף לאחר שזה חודר לרשת הארגון, ולכן מלכתחילה נערך ויתור על מנגנון ההגנה המונע חדירה של תוקף חיצוני.

על רשות האכיפה והגבייה לקדם את ההליך המכרזי ולהטמיע במערכותיה פתרון אבטחתי טכנולוגית ייעודי הולם, שיבטיח הגנה מרבית על נכסי המידע של רשות האכיפה והגבייה, בהתאם להנחיית יה"ב.

רשות האכיפה והגבייה מסרה בתשובתה כי טיפלה באופן מיידי במרבית הנושאים שהעלתה יה"ב, לרבות באמצעות הטמעת מנגנוני הגנה נוספים, וכי היא תפעל להשלמת יתר הפערים שהועלו במהלך שנת 2023, לרבות השלמת פריסת פתרון אבטחתי טכנולוגי ייעודי מסוים בכל המערכות והרשתות שלה. כמו כן מסרה הרשות כי היא מבצעת באופן יזום ותדיר בדיקות חדירות "בהיקפים שונים ובאמצעים מגוונים".

38 מדובר בפתרון מיושן ברמה ירודה ביחס לפתרונות הקיימים היום בשוק.

ביצוע שינויים במערכת הגיבויים

פעילותו של המג"ק נעשית באמצעות מערכת המידע שלו ומבוססת על המידע הרב שאגור בה. אובדן של המידע על החובות שגובה המג"ק צפוי לגרום לנזק משמעותי לקופה הציבורית בהיעדר יכולת לגבות את החובות, ועל כן היכולת לשחזר מידע או להגן על המערכת מפני אובדן המידע חיונית להמשכיות תפקודו התקין של המג"ק כגוף הגובה חובות לאוצר המדינה. לצורך כך מגבה המג"ק את המידע השמור במערכת התפעולית שלו בהתאם למדיניות גיבויים שקבע. בנוהל הגיבויים של רשות האכיפה והגבייה נקבע כי לכל שינוי של תכולת הגיבוי יש לקבל אישור של שני גורמים: מנהל התשתיות ומנהל אבטחת מידע.

התוכנה לניהול מערכת גיבוי הנתונים ברשות האכיפה והגבייה כוללת תוסף המאפשר לקבוע שלא יבוצע שינוי במדיניות הגיבוי במערכת ללא אישור מתועד במערכת של שני גורמים[39], באופן התואם את נוהל הגיבויים של רשות האכיפה והגבייה. מדובר בתוסף שאינו כרוך בתשלום נוסף עבור המג"ק.

> בביקורת נמצא כי על אף ההוראה בנוהל הגיבויים, רשות האכיפה והגבייה אינה משתמשת בתוסף הנמצא בתוכנה לניהול מערכת הגיבויים, המחייב אישור מתועד במערכת של שני גורמים קודם שיבוצע שינוי במדיניות הגיבוי.
>
> מוצע כי רשות האכיפה והגבייה תשתמש באמצעים העומדים לרשותה לצורך מניעת שינויים לא מאושרים במערכת הגיבויים ותבחן את תרומתו של השימוש בתוסף לעניין זה.

רשות האכיפה והגבייה מסרה בתשובתה כי היא תבחן ותיישם כלים למניעת שינויים לא מאושרים במערכת הגיבויים.

יה"ב ציינה בתשובתה למשרד מבקר המדינה מדצמבר 2022 כי בכוונתה להשתמש בממצאים שהועלו בדוח זה ליצירת מודול הדרכה בנושא המיועד למשרדי הממשלה השונים, כדי לסייע בידה להנחיל את ההנחיות המחייבות לגבי ניהול מאגרי מידע.

39 מדובר בתוסף של התוכנה המכונה "Dual authorization workflows".

סיכום

דוח זה מעלה ליקויים בתחום הגנת הפרטיות ואבטחת המידע במערכות המידע במרכז לגביית קנסות שברשות האכיפה והגבייה, וביניהם: היעדר תיעוד של הגישה של משתמשי המערכת התפעולית של המג"ק למידע המצוי במערכת וכפועל יוצא מכך היעדר בקרה על אותה גישה; אי-ביצוע מעקב הולם אחר אירועים חריגים המתרחשים במערכת; ניהול לקוי של תהליך מתן ההרשאות למערכת התפעולית של המג"ק ושל הפיקוח והבקרה עליהן; היקף גישה בלתי-מוגבל של משתמשי המערכת למידע המצוי במערכת; ניהול לקוי של הרשאות עובדי מוקד המידע הטלפוני למערכת; וכן סיכון לחדירת תוקפים חיצוניים למערכות המג"ק.

ליקויים אלה אינם עולים בקנה אחד עם הוראות הדין, ובהן חוק הגנת הפרטיות והתקנות על פיו, החלטות הממשלה הרלוונטיות והנחיות הגופים המאסדרים את הנושא. הדברים מקבלים משנה תוקף נוכח העובדה שעל פי הוראות תקנות אבטחת מידע מסווגת המערכת התפעולית של המג"ק כמאגר שמחייב רמת אבטחה גבוהה.

על רשות האכיפה והגבייה והמג"ק לפעול בהקדם על פי הנחיות הגופים הרלוונטיים למניעת דליפת מידע מהארגון ולשמירה על שלמותו. בכלל זה עליהם להקים מערך לתיעוד ובקרה בעניין השימוש במערכות המידע של המג"ק. כן עליהם לבצע בקרות עיתיות על מערך ההרשאות של עובדי המג"ק ואף לבצע בחינה של היקף הרשאות הגישה למערכת התפעולית של המג"ק לעובדים בתפקידים השונים. נוסף על כך עליהם לבצע בקרה על הרשאות עובדי המוקד ומוצע כי המג"ק יבחן האם יש מקום להגביל את אפשרויות הגישה של עובדי מוקד המידע הטלפוני למערכת התפעולית שלו. נוסף על כך על רשות האכיפה והגבייה לקדם את ההליך המכרזי ולהטמיע במערכותיה פתרון אבטחתי טכנולוגי ייעודי מסוים, שיבטיח הגנה מרבית על נכסי המידע שלה, וכן מוצע כי רשות האכיפה והגבייה תשתמש באמצעים העומדים לרשותה לצורך מניעת שינויים לא מאושרים במערכת הגיבויים.

מאגר המידע של המג"ק הוא רחב היקף וכולל מידע רגיש בנוגע לכ-3 מיליון חייבים. סכומי החוב שבטיפול המג"ק נכון למועד הביקורת מסתכמים בכ-6.8 מיליארד ש"ח. מכאן נובע הצורך לשמור על מערכות המידע למניעת פגיעה בשלמות המידע וברציפות התפקודית של המג"ק במתן שירותים, וכן כדי למנוע דליפה של נתונים ומידע ממאגר המידע או למנוע את חשיפתם לגורמים שאינם מורשים לכך.