



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 המסדרים את הנושא ובהם היחידה להגנת הסייבר בממשלה (להלן - יה"ב), המהווה גורם מנחה מקצועית בתחום הגנת הסייבר.



נתוני מפתח

7% בלבד

שיעור האירועים החריגים¹ (99 מתוך 1,391) שהתרחשו בספטמבר 2022 ונבדקו על ידי גורמי הבקרה במג"ק

כ-6.8 מיליארד ש"ח

סך יתרת החוב בתיקים הפתוחים במג"ק

3 מיליון

מספר החייבים שפרטיהם נכללים במאגרי המידע של המג"ק

21%

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

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

52%

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

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 מצדקים 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 הרשאות 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 הרשאות 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 במערכתיה, ובכלל זה במערכת התפעולית של המג"ק, פתרון אבטחתי טכנולוגי ייעודי מסוים.

עיקרי הממצאות 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 הרשאות 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 הרשאה, כדי לצמצם את היקף בעלי הרשאות למערכת למינימום ההכרחי.

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



תהליך מתן הרשאות 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 הרשאות 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 המסדירים 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 הרשאות 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 המכריזי ולהטמיע במערכת 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.

