



דוח מבקר המדינה

אבטחת המידע במערכת הגיור שבמשרד ראש הממשלה

תוצאות מבדק חוסן

תמוז התשפ"ד | יולי 2024



אבטחת המידע במערך הגיור שבמשרד ראש הממשלה - תוצאות מבדק חוסן

מבוא

1. גיור הוא תהליך הצטרפות של אדם ליהדות. מערך הגיור (להלן גם - המערך) במשרד ראש הממשלה (להלן - משרד רה"ם) הוקם על פי החלטת הממשלה 3155 מפברואר 2008. המערך ממונה על מכלול התהליכים בתחום הגיור הממלכתי במדינת ישראל. המערך אחראי לבטיחות המיוחדים לגיור, להליכי הכשרת המתגיירים לקראת הגיור, לליווי המתגיירים ותמיכה בהם בעת התהליך ולביצוע הליכי הגיור בפועל עד להנפקת "תעודת המרה".

תעודת המרה היא אישור אזרחי-משפטי להמרת הדת, והיא מוכרת לכל דבר ועניין בישראל. אדם המחזיק בתעודת המרה יירשם במרשם האוכלוסין כיהודי ויהיה זכאי להינשא כדת משה וישראל ובבוא היום להיקבר כיהודי. להכרתו כיהודי בישראל יהיו השפעות גם על צאצאיו. אם מחזיק התעודה לא היה אזרח ישראלי, עם קבלתה הוא לרוב יוכר כעולה מכוח חוק השבות, התש"י-1950, ויהיה זכאי ל"סל קליטה". מחזיק בתעודת המרה יוכר כיהודי גם בקהילות יהודיות בחו"ל.

מערך הגיור, הפועל במסגרת משרד רה"ם, מטפל מדי שנה בשנה ביותר מ-5,000 הליכי גיור מסוגים שונים ובאוכלוסיות שונות (ישראלים, זרים, קטינים שאומצו וכיוצא באלה). מערך הגיור פועל בארבעה מחוזות (ירושלים, תל אביב, חיפה ודרום) וכן ב-12 מרכזי קליטה שבהם שוהים עולים חדשים ובבתי דין מיוחדים לגיור הפרוסים ברחבי הארץ. כמו כן, המערך מפקח על הגיור בצה"ל. במערך הגיור יש כ-70 עובדים, ובהם דיינים. מערך הגיור מנפיק את תעודות ההמרה, והן מאושרות בידי הרב הראשי לישראל.

2. להיותו של מערך הגיור חלק ממשרד רה"ם יש חשיבות בכל הנוגע להיבטי אבטחת מידע. ככלל, במערכות הממוחשבות במשרד רה"ם אצור מידע רב, לרבות מידע רגיש, מידע שמסווג כחסוי מהבחינה הביטחונית ומידע ברמת סודיות גבוהה ביותר, ומשום כך המשרד הוא יעד לתקיפות סייבר. בחודשים ינואר-מאי 2023 חווה משרד רה"ם אירועי סייבר, ובכלל זה חסם כ-6 מיליון הודעות דואר אלקטרוני (72% מכלל הודעות הדואר האלקטרוני שנשלחו למשרד באותה תקופה), בין היתר כיוון שכתובת השולח היתה חשודה או משום שהמייל הכיל נוזקה או קישור זדוני. כמו כן היו באותה תקופה כ-49 מיליון ניסיונות להתקפה על שירות החיבור מרחוק של משרד רה"ם, ובהם כ-44 מיליון ניסיונות לסריקת פרטוקולי תקשורת להעברת נתונים, כ-809,000 ניסיונות לסריקת פרטי משתמשים, כ-1.2 מיליון ניסיונות למניעת שירות וכ-9,170 ניסיונות לניצול חולשות ידועות.

3. אגף בכיר טכנולוגיות דיגיטליות ומידע (להלן - אגף טד"ם) אמון על הגנת המידע הבלתי מסווג במשרד, ובכלל זה על הגנת המידע במערך הגיור ועל פעולתה של מערכת "מאור" שנועדה לניהול תיקי גיור ותהליכי גיור, ברשת הבלתי מסווגת של המשרד. אגף טד"ם אחראי בין היתר לפיתוח מערכות מידע ולמתן שירותי תחזוקה, תמיכה, אחסון וטיפול בנוגע לחומרת המחשוב והתקשורת בכל רשתות המשרד. בראש אגף טד"ם עומד מנהל בדרג סמנכ"ל, הכפוף ישירות למנכ"ל משרד רה"ם.

פעולות הביקורת

באוגוסט 2023 בוצעה בדיקת חוסן יישומית (אפליקטיבית) למערכת מאור של מערך הגיור. הביקורת נערכה במשרד רה"ם, ובפרט באגף הגיור הפועל בו. בדיקת החוסן נערכה ב"סביבת בדיקות וירטואלית" של מערכת מאור (הזהה ל"סביבת הייצור", שכוללת את מכלול המידע



שבמערכת), כדי שלא לפגוע במידע הקיים במערכת¹. כן נבחן חוסנו של הטופס (טופס המופעל על ידי "ממשל זמין"²) במרשתת (אינטרנט) שבאמצעותו ניתן להגיש "בקשה לפתיחת תיק גיור". הבדיקה נעשתה בין השאר באמצעות בחינת תרחישים שגיבש צוות הביקורת, ובכלל זה ניסיון להפיק באמצעות המערכת תעודות המרה פיקטיביות. להלן יובאו הליקויים שעלו בבדיקת החוסן.

תהליך הגיור במערכת מאור

מערכת הגיור מנהל את תהליכי הגיור באמצעות מערכת מאור - יישום ממוחשב שפיתח משרד רה"ם, ובו חמישה מודולים: גיור אזרחי ישראלי, גיור נתין זר, גיור קטין, ניהול ראינות וניהול כיתות לימוד. במערכת יש משתמשים רשומים בעלי הרשאות פעולה מסוגים שונים, והיא כוללת את תיקי הגיור המנוהלים במערכת משנת 2020. המידע לגבי תיקים ישנים יותר (לא פעילים) שמור במערכת נפרדת בשם "מאור ארכיון". בתרשים הבא מתוארים שלבי תהליך הגיור.

תרשים 1: שלבי תהליך הגיור



על פי אתר המרשתת של מערכת הגיור, בעיבוד משרד מבקר המדינה.

הליך הגיור במערכת מאור נפתח על פי "בקשה לפתיחת הליך גיור". את הבקשה ניתן להגיש באופן דיגיטלי באתר המרשתת של מערכת הגיור, באמצעות מערכת השירותים של "ממשל זמין". עם פתיחת ההליך מוקם במערכת "תיק גיור", המכיל את פרטיו האישיים של המתגייר (פרופיל המתגייר) תחת ההגדרה "איש קשר". לכל תיק גיור מצורף גם "תיק מאגד", שבו יאוגדו תיקי הגיור של בני משפחה אחרים המצויים בתהליך גיור, אם יש בני משפחה כאלה. בתרשים שלהלן מתואר "פס תהליך" לגבי גיור של אזרחי ישראל³, המקביל ככלל לשלבי תהליך הגיור המתוארים בתרשים שלעיל.

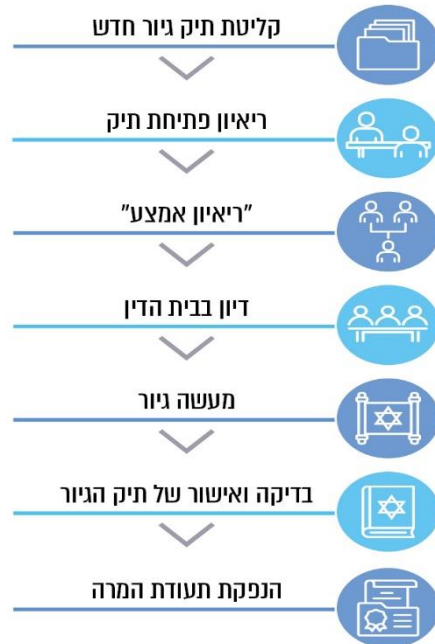
¹ סביבת בדיקות וירטואלית היא מערכת המאפשרת לבצע בדיקות תוכנה על גבי מכונות וירטואליות הדומות לסביבת הייצור (הסביבה שבה פועלת המערכת), ובכך להבטיח שהמידע והתהליכים בסביבת הייצור לא ייפגעו מביצוע הבדיקות.

² יחידה ממשלתית שהיא חלק ממערכת הדיגיטל הלאומי. היחידה פועלת ליעול השירות הציבורי ולשיפור השירות לאזרח, באמצעות פיתוח יישומים רוחביים להנגשת המידע הממשלתי, התשלומים והטפסים הממשלתיים.

³ פסי תהליך אחרים המוצעים במערכת הם "פס תהליך לנתין זר" ו"פס תהליך לקטין", המותאמים לשלבים הנדרשים בהליכי גיור אלה.



תרשים 2: שלבים בפס תהליך לגבי גיור של אזרח ישראלי



המקור: מערך הגיור, בעיבוד משרד מבקר המדינה.

עם השלמת כל אחד מהשלבים מועבר תיק הגיור לשלב הבא בפס התהליך. השלמת השלב של "בדיקה ואישור של תיק הגיור" מצריכה אישור של מנהל המחוז שבו מתנהל התיק, ולפיו התיק שלם ומוכן להעברתו לאישורו של נציג הרב הראשי. לאחר מכן נדרש אישורו של נציג הרב הראשי המאשר את הגיור ואת הנפקת תעודת ההמרה. הגדרות מערכת מאור אינן מאפשרות חזרה לשלב קודם שהושלם, ועם העברת התיק לאישור מנהל המחוז אמור התיק להינעל לעריכה. זאת בין היתר כדי להבטיח שלא יבוצעו בדיעבד שינויים שאינם מורשים בפרטי תיק הגיור.

בכל אחד משלבי פס התהליך נאספים המידע והמסמכים הרלוונטיים להשלמת אותו שלב ונשמרים בתיק הגיור של המתגייר במערכת, לרבות פרטיו האישיים של המתגייר; פרטים על תהליך המילה והטבילה שעבר; פרטים על תהליכי הלימוד שהשלים; סיכום הדיון שהתקיים לגביו בבית הדין; וכן מסמכים רלוונטיים (תעודות זהות, תעודות נישואין, מידע רפואי רלוונטי וכיו"ב). המידע והמסמכים האלה רגישים, ולכן איסופם ושמירתם כפופים להוראות חוק הגנת הפרטיות, התשמ"א-1981 ולתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. פגיעה בסודיות, בשלמות או בזמינות של המידע שבמערכת מאור עלולה לגרום נזק כלכלי ותדמיתי הן למדינת ישראל והן למתגיירים שעניינם מטופל באמצעות המערכת.

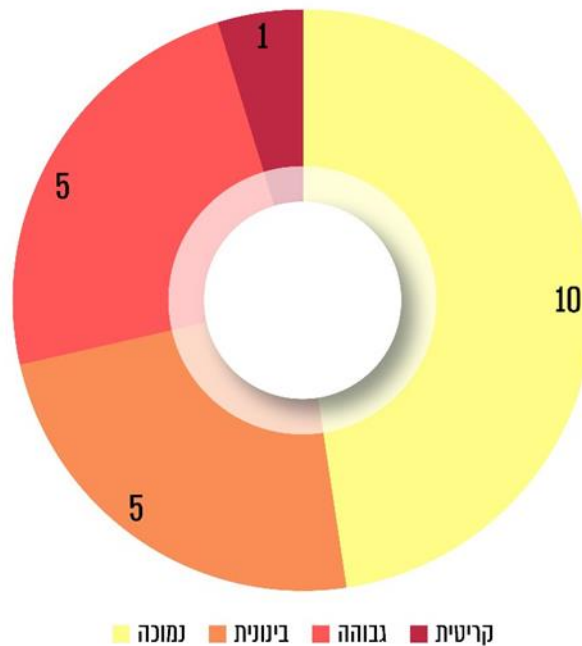
בסיום תהליך הגיור, כפי שעולה מהתרשים שלעיל, מערכת מאור מאפשרת הנפקת "תעודת המרה" למתגייר. אף שתעודת ההמרה כשלעצמה אינה תנאי הלכתי מהותי להשלמת התהליך, מבחינת מוסדות המדינה (כגון משרד הפנים וחברה קדישא), תעודה זו היא אסמכתה לכך שהמחזיק בה השלים את תהליך הגיור והצטרף כדת וכדין ליהדות. להחזקה בתעודת המרה נודעת אפוא משמעות כבדת משקל.



הליקויים שעלו במבדק החוסן ורמת הסיכון הכרוכה בהם

בתרשים שלהלן מוצגים נתונים על מספר הליקויים שעלו בבדיקת חוסן שנעשתה למערכת מאור באוגוסט 2023, בחלוקה לרמות הסיכון המשתקפות מהם (רמת סיכון קריטית לפעילות הארגון, רמת סיכון גבוהה, רמת סיכון בינונית או רמת סיכון נמוכה). רמת הסיכון נקבעה על פי שקלול של שני אלה: חומרת הנזק הפוטנציאלי של הליקוי והסבירות שהוא אכן יתרחש.

תרשים 3: מספר הליקויים שנמצאו בבדיקת חוסן שנעשתה למערכת מאור באוגוסט 2023, בחלוקה לרמות סיכון



מהתרשים עולה כי בבדיקת החוסן שנעשתה למערכת מאור העלתה 21 ליקויים: ליקוי אחד ברמת סיכון קריטית; חמישה ליקויים ברמת סיכון גבוהה; חמישה ליקויים ברמת סיכון בינונית; ועשרה ליקויים ברמת סיכון נמוכה.⁴

יצוין כי רוב הליקויים שהועלו בבדיקה נוגעים ל"איום פנימי", כלומר איום פוטנציאלי מצד משתמשים בעלי הרשאת גישה למערכת מאור. זאת, בשונה מ"איום חיצוני" מצד גורמים שאינם בעלי הרשאת גישה למערכת זו.

הלוגיקה העסקית במערכת מאור

הנפקת תעודת המרה ליהדות באמצעות מערכת מאור טעונה מעבר בכל שלבי פס התהליך המתואר לעיל, לרבות המצאת מסמכים שבהם מצוינים פרטיו האישיים של המתגייר וכן אישור של נציג הרב הראשי לישראל שתהליך הגיור הסתיים בהצלחה, שלאחריו מונפקת תעודת המרה למתגייר.

הבדיקה כללה תרחישים הנוגעים לליבת מערכת מאור - "הדרישות העסקיות" של המערכת, המגדירות את אופן הפעולה שלה ואת מגוון הפעולות שרשאים לבצע המשתמשים בה, והמגבלות החלות על פעולות אלו. הדרישות האלה חלות על המשתמש - "צד הלקוח" - ועל לב המערכת - "צד

⁴ לעיתים ליקוי אחד ניתן לניצול בכמה תרחישים. במקרה כזה רמת החומרה של הליקוי נקבעה על פי רמת החומרה של התרחיש החמור ביותר שמאפשר הליקוי.



השרת". להלן יובאו מרבית הליקויים שעלו בבדיקה הנוגעים לעקיפת הלוגיקה העסקית במערכת מאור, הנובעים מביצוע הדרישות בצד הלקוח בלבד ולא בצד השרת.

1. הנפקת תעודת המרה כוזבת - תרחיש ברמת סיכון קריטית: במסגרת הבדיקה דימה צוות הביקורת תרחיש של תוקף זדוני בעל הרשאה בדרגה הבסיסית ביותר במדרג ההרשאות ("ראש ענף"), והצליח להנפיק תעודת המרה כוזבת. הנפקת תעודת המרה כוזבת מאפשרת למחזיק בה להתחזות ליהודי ולהתל באופן הזה בכל אדם ובמוסדות המדינה, הרואים בתעודה זו אסמכתה לגיור כהלכה, למשל לצורך נישואין על פי ההלכה היהודית.

יודגש כי הפעולה נעשתה ברמת מיומנות של משתמש רגיל במערכת, ללא מיומנות של תוקף סייבר מקצועי וללא שימוש בכלי פריצה ייחודיים.

תמונה 1: תעודת המרה כוזבת שהופקה במסגרת המבדק



2. שינויים מסוימים במערכת "מאור" - תרחיש ברמת סיכון גבוהה: במסגרת הבדיקה דימה צוות הביקורת תוקף זדוני בעל הרשאה בסיסית והצליח לעשות שינויים כגון שינוי בהחלטתו הכתובה של בית הדין לאשר את המשך הליך הגיור ולציין במקומה כי הוחלט לבטל את הגיור עקב נתונים לא אמינים שנמסרו.



3. **שינוי נתונים מסוימים במערכת "מאור" - תרחיש ברמת סיכון בינונית:** צוות הביקורת דימה תוקף זדוני והצליח באמצעותו לעשות שינוי בתהליך, העלול להביא לאישור גיור של מתגייר בעל פרטים שונים מפרטיו האמיתיים.
4. **הוספת פרטי מוסד לימוד ללא ציון כמות השעות - תרחיש ברמת סיכון נמוכה:** על פי מאפייני המערכת, בעת הוספת פרטי מוסד הלימוד שבו השלים המתגייר את חובת לימודיו, יצוין גם מספר שעות הלימוד שאמור המתגייר להשלים במוסד זה. צוות הביקורת דימה תוקף זדוני והצליח להוסיף למערכת מוסד לימוד ללא ציון כמות השעות שנלמדו.
5. **הוספת מכר עם דרכון זר ללא ציון ארץ הפקת הדרכון - תרחיש ברמת סיכון נמוכה:** צוות הביקורת הצליח להוסיף לתיק הגיור פרטי מכר כאמור, שלא על פי הנדרש במאפייני המערכת.
6. **הוספת איש קשר ללא ציון שמו - תרחיש ברמת סיכון נמוכה:** צוות הביקורת הצליח לעשות כן, שלא על פי הנדרש במאפייני המערכת.

הגדרת הרשאות

במערכת מאור יש כאמור משתמשים בעלי הרשאות פעולה מסוגים שונים. ככלל, הגדרת התפקידים, רמות ההרשאה והסוגים השונים שלה במערכת מאפשרים תפקוד הייררכי ומבוקר של הפעילות העסקית. הגדרה "אנכית" של רמות הרשאה מאפשרת למשל לקבוע כי פעולות מסוימות יוכלו להתבצע באישור דרג נמוך בהיררכייה הארגונית, ופעולות רגישות יותר יתבצעו באישור דרג גבוה יותר. הגדרה "אופקית" של הרשאות מאפשרת מידור של המידע במערכת ומקילה את השליטה בביצוע הפעולות. למשל, ניתן להגדיר לגבי תיקים שמטופלים במחוז מסוים כי רק עובדי המחוז יהיו רשאים לצפות במידע המצוי בתיקים ולבצע פעולות בהם. יובהר כי עיקר החשש משימוש לא מורשה בהרשאות נוגע בהקשר זה לשימוש לא תקין של עובד בהרשאות הגבוהות מאלו שניתנו לו או לביצוע פעולות שאינן בתחום אחריותו.

צוות הביקורת הצליח לעקוף את מנגנון ההרשאות - ולממש תרחישים ברמת סיכון גבוהה, וכך הצליח להפיק תעודת המרה כוזבת, כמוצג בתמונה הבאה.



תמונה 2 : תעודת המרה כוזבת שהופקה במסגרת המבדק



הצפת המערכת במידע

כאמור, פתיחת תיק גיור מתבצעת באמצעות מילוי ושליחה של טופס "בקשה לפתיחת תיק גיור" באתר המרשתת של מערך הגיור, באמצעות שירותי ממשל זמין. הליקויים שלהלן התקבלו מבדיקת המערכת בכלל, ומבדיקת הטופס האמור בפרט, שאפשר להגיש דרך אתר המרשתת של מערך הגיור.

1. **הצפת המערכת במידע באמצעות פתיחת תיקי גיור - תרחיש ברמת סיכון גבוהה :** נמצא כי המערכת מאפשרת למשתמשים הגולשים באתר המרשתת של מערך הגיור לשלוח טופסי "בקשה לפתיחת תיק גיור" ללא הגבלה, וכי כמות הנתונים שניתן לטעון למערכת באמצעות הטופס אינה מוגבלת. צוות הביקורת דימה תוקף זדוני והציף את המערכת בתיקים מאגדים רבים שנפתחו כולם על ידי אותו משתמש באותו היום. הצפת המערכת בטופסי בקשה או בנתונים רבים עלולה למנוע מהמערכת לספק שירות.



2. **הצפת חשבונות בהודעות דוא"ל של מערך הגיור - תרחיש ברמת סיכון בינונית**: נמצא כי המערכת מאפשרת למשתמשים לשלוח מספר בלתי מוגבל של הודעות דוא"ל מהדומיין (domain) של המערכת, כלומר ממערך הגיור, ובכך לגרום לזיהויו של הדומיין של המערך כמקור ל"דואר זבל" ולחסום קבלת דוא"ל ממנו.

3. **הצפת המערכת בנתונים - תרחיש ברמת סיכון בינונית**⁵: נמצא כי המערכת מתעדת פעולות שבוצעו בה (עדכון סטטוס, עדכון החלטה, עדכון פרטי איש קשר וכו'), אך אינה מגבילה את כמות הפעולות שמשתמש רשאי לבצע ושיתועדו בה. במצב זה יכול תוקף זדוני לבצע בכלים אוטומטיים פעולות רבות שיתועדו, ובכך לצמצם את המקום הפנוי בבסיס הנתונים בכונן הקשיח. באופן דומה, יכול תוקף להוסיף רשומות חדשות (כגון איש קשר, מכר, מוסד לימוד, כיתה, ביקורים בארץ ופרוטוקול דיון) וכן להוסיף באופן אוטומטי כמות גדולה של בקשות להוספת נתונים בתיקים קיימים, ובכך למנוע מהמערכת לספק שירות.



מערך הגיור מטפל מדי שנה בשנה ביותר מ-5,000 הליכי גיור ומפיק תעודות המרה המאושרות בידי הרב הראשי. להחזקה בתעודת המרה יש משמעות כבדת משקל בהיבט האישי, החברתי והכלכלי. למשל, אדם המחזיק בתעודת המרה יירשם במרשם האוכלוסין כיהודי, יהיה זכאי להינשא כדת משה וישראל ויהיה זכאי בבוא היום להיקבר כיהודי. אם מחזיק התעודה לא היה לפני קבלתה אזרח ישראלי, עם קבלתה הוא לרוב יוכר כעולה מכוח חוק השבות, התש"י-1950, ויהיה זכאי ל"סל קליטה". המידע והמסמכים הנאספים במערכת מאור של מערך הגיור הם רגישים, ופגיעה בסודיות, בשלמות או בזמינות של המידע במערכת עלולה לגרום נזק כלכלי ותדמיתי הן למדינת ישראל והן למתגיירים.

בדיקת החוסן של מערכת מאור העלתה 21 ליקויים. בין השאר, צוות הביקורת הצליח להפיק באמצעות המערכת תעודת המרה כוזבת, המאפשרת למחזיק בה להתחזות ליהודי ולהתל באופן הזה בכל אדם ובמוסדות המדינה, הרואים בתעודה זו אסמכתה לגיור כהלכה, תוך עקיפת תהליך העבודה ואמצעי הבקרה המובנים במערכת. להלן פירוט מרבית הליקויים:

1. ליקוי אחד ברמת סיכון קריטית - עקיפת הלוגיקה העסקית במערכת באופן שמאפשר הנפקת תעודת המרה כוזבת.
2. חמישה ליקויים ברמת סיכון גבוהה, לרבות ביצוע פעולות במערכת ללא הרשאה מתאימה ואפשרות להציף את המערכת בנתונים על ידי תוקף אנונימי, באמצעות שליחה אוטומטית של טופסי פתיחת תיק.
3. חמישה ליקויים ברמת סיכון בינונית ועשרה ליקויים ברמת סיכון נמוכה.

מומלץ שמשרד רה"ם ינקוט פעולות המתחייבות מהליקויים שעלו בבדיקה. כמו כן מומלץ שמשרד רה"ם והיחידה להגנת הסייבר (יה"ב) ויחידת ממשל זמין ינקטו את הפעולות הנדרשות לתיקון הטופס במרשתת בנושא "בקשה לפתיחת תיק גיור".

מערך הדיגיטל הלאומי ציין בתשובתו מינואר 2024 כי הטופס המקוון הקיים של מערכת הגיור נמצא במערכת הטפסים הישנה של מערך הדיגיטל הלאומי וכי משרד רה"ם נדרש להעביר אותו למערכת הטפסים החדשה, במטרה לשפר את החוסן של מערכת מאור. משרד רה"ם ציין בתשובתו

⁵ התרחיש בסעיף 1 לעיל בתת הפרק על הצפת המערכת במידע, הנוגע גם הוא להצפת נתונים, מתואר כתרחיש ברמת סיכון גבוהה, היות שביצעו מתאפשר גם באמצעות גורמים אנונימיים שאינם מאומתים בארגון. זאת בשונה מתרחיש זה, שניתן לביצוע רק על ידי עובד מאומת בארגון.



כי בכוונתו להעביר את הטופס המקוון למערכת החדשה של מערך הדיגיטל הלאומי עד לסוף מרץ 2024.

פעולות משרד רה"ם בעקבות הביקורת

משרד רה"ם פירט בתשובתו ממרץ 2024 את פעולותיו לתיקון הליקויים שעלו במבדק החדירה, בין היתר ציין כי: הליקוי שהוגדר קריטי טופל ותוקן בימים שלאחר ביצוע מבדק החדירה; האפשרות שתוקף אנונימי יציף את המערכת בנתונים באמצעות שליחה אוטומטית של טופסי פתיחת תיק תטופל עם המעבר של יחידת "ממשל זמין" במערך הדיגיטל הלאומי לטכנולוגייה חדשה עד לסוף מרץ 2024; ליקויים שהוגדרו בסיכון נמוך ובינוני נבחנו ויטופלו באמצעות חידוד נוהלי העבודה והבקרה במערכת, לצד בחינת הכדאיות של פיתוחים אפשריים כמענה לליקויים האלה, תוך שקילת עלותם לעומת תועלתם.

סיכום

גיור הוא תהליך הצטרפות של אדם ליהדות. מערך הגיור הפועל במשרד רה"ם ממונה על מכלול התהליכים הקשורים לתחום הגיור הממלכתי במדינת ישראל. המערך אחראי לבתי הדין המיוחדים לגיור, להליכי הכשרת המתגיירים לקראת הגיור, לליווי המתגיירים ותמיכה בהם בתהליך ולביצוע הליכי הגיור בפועל עד להנפקת תעודת המרה, שהיא אישור אזרחי-משפטי להמרת הדת ומוכרת לכל דבר ועניין בישראל.

משרד מבקר המדינה בדק את חוסנה של המערכת הממוחשבת המשמשת את מערך הגיור. המידע והמסמכים הנאספים במערכת זו הם רגישים, ופגיעה בסודיות, בשלמות או בזמינות של המידע שבמערכת עלולה לגרום נזק כלכלי ותדמיתי למדינת ישראל ולמתגיירים. הבדיקה העלתה בין היתר ליקוי קריטי הנוגע לליבת "התהליך העסקי" של מערך הגיור - היכולת להפיק תעודת המרה כוזבת, המאפשרת למחזיק בה להתחזות ליהודי ולהתל באופן הזה בכל אדם ובמוסדות המדינה, הרואים בתעודה זו אסמכתה לגיור כהלכה.

משרד רה"ם פירט בתשובתו ממרץ 2024 את פעולותיו לתיקון ליקויים שעלו במבדק החדירה, לרבות הטיפול בליקוי שהוגדר קריטי ותיקונו בימים שלאחר ביצוע מבדק החדירה. משרד מבקר המדינה מציין לחיוב את פעולות משרד רה"ם לתיקון ליקויים, לפני גיבוש דוח הביקורת הסופי.

על משרד רה"ם לפעול לתיקון הליקויים שעלו בביקורת, כמפורט בדוח ביקורת זה. יש מקום שמערך הדיגיטל הלאומי ויחידת ממשל זמין שבו יבדקו אם הליקויים שמפורטים בדוח זה רלוונטיים גם לשירותי ממשל ממוחשבים אחרים העוסקים בהנפקת תעודות רשמיות לציבור.



משרד מבקר המדינה
ונציב תלונות הציבור

