



דוח מבקר המדינה

מערכות המידע והגנת הסייבר בבחירות לרשויות המקומיות

▪ אייר התשפ"ה ▪ מאי 2025 ▪

מערכות המידע והגנת הסייבר בבחירות לרשויות המקומיות

מבוא

הבחירות לרשויות המקומיות הן אבן יסוד מרכזית בקיומה של הדמוקרטיה המקומית, ותוצאות הבחירות משפיעות על היבטים נרחבים בחיי היום-יום של כלל תושבי מדינת ישראל. במדינת ישראל מתקיים תהליך הבחירות לרשויות המקומיות ולמועצות האזוריות אחת לחמש שנים, בכל הארץ בעת ובעונה אחת. בתהליך זה נבחר בכל רשות מקומית ראש הרשות ונקבע ההרכב של מועצת הרשות; ובמועצות האזוריות נבחר ראש המועצה האזורית ונקבע ההרכב של המועצה האזורית ושל הוועד המקומי (להלן - הבחירות לרשויות המקומיות)¹. מועד הבחירות בתקופת הביקורת נקבע במקור על פי חוק ל-31.10.23, אולם עקב פרוץ מלחמת חרבות ברזל הוא נדחה תחילה ל-30.1.24 ולאחר דחייה נוספת התקיים ב-27.2.24 (להלן - מועד הבחירות) בזמן המלחמה בכל הרשויות המקומיות, מלבד ב-12 רשויות שתושביהן פונו ובחלקן הבחירות התקיימו בנובמבר 2024².

תהליך הבחירות עשוי להיות מטרה לתקיפה בידי גורמים עוינים, שנועדה לפגוע בתחושות הביטחון והאמון במוסדות המדינה, סיכון שגובר בנסיבות שבהן הבחירות מתקיימות בשעת מלחמה. מאז תחילת מלחמת חרבות ברזל זיהה מערך הסייבר הלאומי (להלן - מערך הסייבר) גידול במספרם של התקיפות, של סוגי התקיפות ושל יעדי התקיפות במדינת ישראל. מספר האירועים המשמעותיים בתקופת המלחמה (משבעה באוקטובר 2023 ועד לסוף אותה שנה) היה 3,380 - גידול של פי 2.5 מבעת שגרה. כמו כן, מטרת מרבית התקיפות הייתה גרימת נזק, להבדיל מהתקיפות לפני המלחמה, שמטרותיהן העיקריות היו ריגול וגניבת מידע.

שר הפנים אחראי לתהליך הבחירות לרשויות המקומיות מכוח חוק³, ועליו לאפשר לכל בעל זכות בחירה לממש את זכותו הדמוקרטית לבחור ולהיבחר, וכן עליו להבטיח כי הבחירות ברשויות המקומיות יתקיימו כהלכה ובהתאם לחוק, ובכלל זה כי יישמרו העקרונות המנחים לקיומן: בחירות כלליות, ישירות, שוות, חשאיות ויחסיות⁴.

אגף בכיר בחירות ברשויות המקומיות במשרד הפנים (להלן - יחידת המפקח), בראשות המפקח הארצי על הבחירות (להלן - המפקח), אחראי לניהול תהליך הבחירות ולפיקוח עליו, מכוח סמכויות השר שהואצלו למפקח. בהקשר למערכות המידע המשמשות לביצוע תהליך הבחירות ולהיבטי הסייבר שלהן, המפקח על הבחירות הוא הגורם העסקי שמגדיר את הדרישות למערכות ואגף בכיר טכנולוגיות דיגיטליות ומידע במשרד הפנים (להלן - אגף טד"ם) מספק את שירותי הפיתוח והתחזוקה של מערכות אלו. בעיתות שגרה מונה יחידת המפקח שישה עובדים, וכשבעה חודשים לפני מועד הבחירות (להלן - תקופת ההיערכות לבחירות) גייסה יחידת המפקח 253 מנהלי בחירות שכל אחד מהם היה אחראי לניהול תהליך הבחירות ברשות המקומית שלו, ובסמוך ליום הבחירות הועסקו במערכת הבחירות כ-30,000 עובדים נוספים.

אומנם תהליך הבחירות הוא ידני - הצבעה באמצעות פתקים במעטפות שכל בוחר משלשל לתיבת הקלפי - אולם בתהליכי ההיערכות לבחירות וניהולן משמשות מערכות מידע, בין השאר, לצרכים האלו: גיוס והכשרה של כוח האדם; ניהול המשימות לקראת הבחירות; העברת מידע על בעלי זכות בחירה; הנגשת המידע על הבחירות ואיתור מקום ההצבעה; הזנת תוצאות הבחירות במערכות הממוחשבות ופרסומן לציבור. מערכות המידע מפותחות ומתוחזקות באמצעות אגף

¹ חוק הרשויות המקומיות (בחירות), התשכ"ה-1965; חוק המועצות האזוריות (מועד בחירות כלליות), התשנ"ד-1994; חוק הרשויות המקומיות (בחירת ראש הרשות וסגניו וכהונתם), התשל"ה-1975; חוק המועצות האזוריות (בחירת ראש המועצה), התשמ"ח-1988.

² הרשויות שבהן נדחו הבחירות הן: אשכול, הגליל העליון, חוף אשקלון, מבואות חרמון, מטה אשר, מעלה יוסף, מרום גליל, קריית שמונה, שדות נגב, שדרות, שלומי ושער הנגב.

³ ראו הערת שוליים 1 לעיל.

⁴ חוק הרשויות המקומיות (בחירות), התשכ"ה-1965, סעיף 2; אצילת סמכויות - ילקוט הפרסומים 5350 - עמ' 801.

טד"ם, מערך הדיגיטל ורשות האוכלוסין וההגירה (להלן - רשות האוכלוסין) ובאמצעות ספקים חיצוניים שהאגף רוכש את שירותיהם. מערכות המידע של משרד הפנים מתארחות בתשתית ענן ציבורי ובתשתית של מערך הדיגיטל הלאומי. כמו כן, נעשה שימוש במערכת ג' של רשות האוכלוסין. להלן יפורטו מערכות המידע העיקריות בתחום זה בהתאם להגדרה של מערך הסייבר ומשרד הפנים:

לוח 1: מערכות מידע המשתתפות בתהליך הבחירות לרשויות המקומיות

אחראי	שם	תיאור
 רשות האוכלוסין	מערכת ג'	ניהול המידע על המועמדים והרשימות, על בעלי זכות בחירה ועל התוצאות הסופיות
 משרד הפנים	מערכת ב'	מערכת לניהול תהליך הבחירות
 משרד הפנים	מערכת ד'	קבלת קובצי פנקס הבוחרים
 משרד הפנים	מערכת ה'	צפייה בתוצאות זמניות
 משרד הפנים	מערכת ו'	אתר המידע הרשמי של הבחירות לרשויות המקומיות
 משרד הפנים	מערכת ז'	אתר אינטרנטי לקבלת מידע על מקום הקלפיות לפי בעל זכות בחירה
 משרד הפנים	מערכת ח'	מערכת לניהול בקשות של מועמדים ובאי כוח לקבלת רשימות בעלי זכות בחירה מפנקס הבוחרים
 משרד הפנים	מערכת ט'	מערכת למידה

על פי נתוני משרד הפנים, בעיבוד משרד מבקר המדינה.

תרשים 1: תהליכים מרכזיים בבחירות לרשויות המקומיות

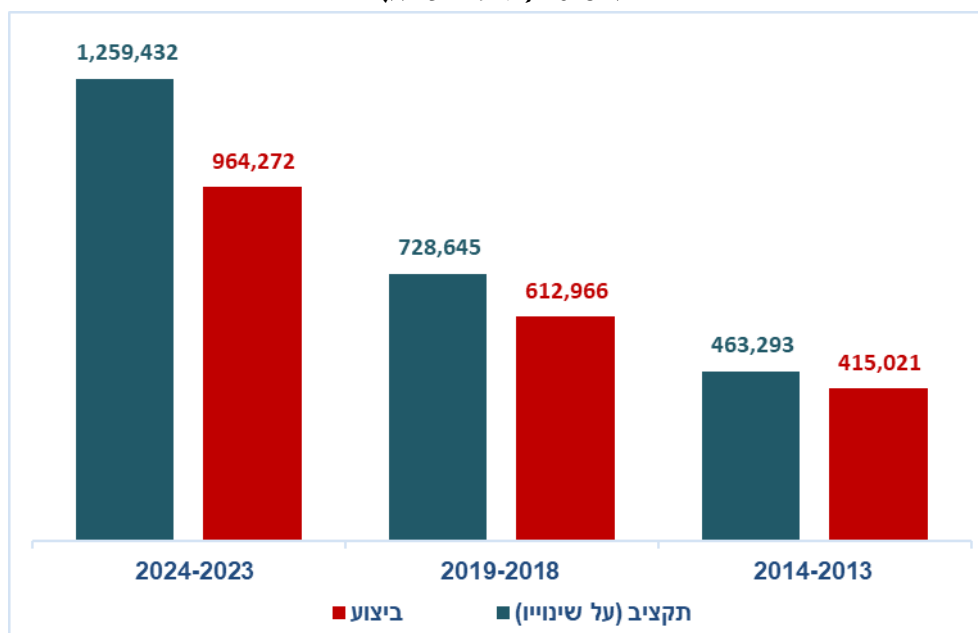


על פי נתוני משרד הפנים, בעיבוד משרד מבקר המדינה.

תקציב הבחירות לרשויות המקומיות מאושר במסגרת התקציב של משרד הפנים וכולל, בין היתר, את ההוצאות של יחידת המפקח, וכן את ההוצאות על מימון מפלגות ועל שכר כוח האדם. שכר כוח האדם משולם על ידי הרשויות המקומיות, וממומן על ידי משרד הפנים. בתרשים להלן מוצג תקציב הבחירות לרשויות המקומיות (על שינויי) וביצעו בשלוש מערכות הבחירות האחרונות⁵:

⁵ בשנים 2013 ו-2018 הבחירות נערכו בסוף השנה האזרחית, וכפועל יוצא מכך חלק מהתקציב מבוצע בשנה הבאה. בחירות 2023 נדחו והתקיימו בפברואר 2024, למעט ב-12 רשויות שתושביהן פונו, ובחלקן התקיימו בחירות בנובמבר 2024. לפיכך ביצעו התקציב נפרס על פני השנים 2023 - 2024.

תרשים 2: תקציב מערכות הבחירות לרשויות המקומיות (על שינוייו) וביצועו, 2018, 2013, 2023 (באלפי ש"ח)



על פי נתונים ממערכת מרכזית, בעיבוד משרד מבקר המדינה.
*הנתונים נכונים לינואר 2025.

כפי שעולה מהתרשים, תקציב הבחירות לרשויות המקומיות (על שינוייו) עבור מערכת הבחירות הנוכחית (נכון לינואר 2025) הסתכם בכ-1.26 מיליארד ש"ח (לא כולל יום שבתון), והוצאותיו של משרד הפנים על מערכת הבחירות האמורה עד תאריך זה הסתכמו בכ-964 מיליון ש"ח, מתוכם כ-761 מיליון ש"ח עבור הוצאות מימון מפלגות, כ-137.6 מיליון ש"ח עבור הוצאות שכר ובעלי תפקידים, כ-92 מיליון ש"ח עבור הוצאות חברי ועדת קלפי וכ-29.7 מיליון ש"ח עבור הוצאות מחשוב. חלק מהוצאות המחשוב מבוצעות גם בתקופה שבין הבחירות והן הסתכמו בתקופה שלפני הבחירות הנוכחיות, בין השנים 2020 - 2022, בכ-5.2 מיליון ש"ח.

פעולות הביקורת

בחודשים יולי 2023 עד יולי 2024 בדק משרד מבקר המדינה את מערכות המידע והגנת הסייבר הנוגעות לבחירות לרשויות המקומיות. הביקורת נעשתה במשרד הפנים - ביחידת המפקח ובאגף טד"ם. בדיקות השלמה בוצעו ברשות האוכלוסין, במשרד ראש הממשלה - במערך הסייבר הלאומי, במשרד המשפטים - ברשות להגנת הפרטיות, ובמשרד הכלכלה והתעשייה - במערך הדיגיטל הלאומי.

הביקורת בוצעה גם בזמן אמת והחלה עוד בשלב ההיערכות למערכת הבחירות. במהלך הביקורת העביר משרד מבקר המדינה חלק מהממצאים לגופים המבוקרים לצורך שיפור היערכותם לבחירות, וחלקם תוקנו לפני יום הבחירות. ביום הבחירות, בליל הבחירות ובימים שלאחר מכן ביצעו צוותים מטעם משרד מבקר המדינה ביקורת במרכז השליטה והבקרה שהפעילה יחידת המפקח, במרכז המיון של המעטפות החיצוניות ובמרכזי קליטה של 13 רשויות מקומיות⁶ ברחבי הארץ שהיו באחריותם של מנהלי בחירות שהועסקו מטעם יחידת המפקח (ברשויות נקלטו חומרי הבחירות מהקלפיות והוזנו תוצאות הבחירות למערכות הממוחשבות).

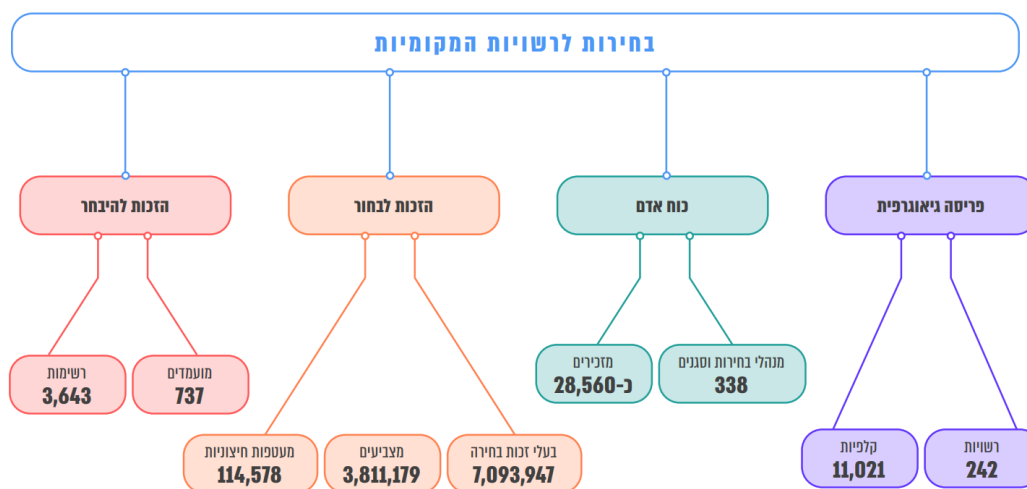
⁶ אלעד, אריאל, באר שבע, בני ברק, חיפה, ירושלים, ירכא, כרמיאל, המועצה האזורית מרחבים, עכו, פתח תקווה, קריית מוצקין וראש העין.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם חלקים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17(א) לחוק מבקר המדינה, התשי"ח - 1958 (נוסח משולב).

דיגיטציה של מערכות הבחירות

השימוש בתהליכים דיגיטליים ובמערכות מידע וניהול ממוחשבות חיוני לניהול המיטבי של פרויקט לאומי כדוגמת הבחירות לרשויות המקומיות, שבמסגרתו נעשה שימוש במאגרי מידע המכילים מיליוני נתונים (Big Data) ונדרש לנהל בו תהליכים רבים, לרבות באמצעות עשרות אלפי עובדים המועסקים ביום הבחירות ובסמוך לו.

תרשים 3: נתונים בתהליך הבחירות לרשויות המקומיות



על פי נתוני יחידת המפקח במשרד הפנים, בעיבוד משרד מבקר המדינה.

שימוש בדיגיטציה יכול לסייע לתהליכי הבחירות לרשויות המקומיות בעיקר בהיבטים אלו:

- 1. הגברת היעילות:** שימוש במערכות לצורך ביצוע פעולות אוטומטיות מיותר פעילות אנושית, מפחית את הסיכון לטעויות ומאפשר לזרז את ביצוען של פעולות.
- 2. שיפור אבטחת המידע של חומר רגיש:** תהליך ממחושב מיותר את הצורך בשינוע ובאבטחה של חומרים פיזיים המכילים מידע רגיש או פרטי (למשל: פרוטוקולים של ועדות קלפי) ובכך מפחית את הסיכון לדלף מידע או לאיבוד מידע עקב טעות אנוש או פגיעה בזדון.
- 3. שימוש ביכולת זיהוי חריגות ואנומליות בבסיסי מידע גדולים:** מידע ממוחשב ניתן לניתוח באמצעים סטטיסטיים ובאלגוריתמים מתקדמים של בינה מלאכותית (AI), הכוללים לימוד מכונה (ML) או ראיית מכונה (Computer Vision), המאפשרים להגיע לתובנות ולתחזיות מתקדמות ומורכבות וכן לזהות חריגות שעשויות להעיד על פגיעה בטוהר הבחירות.
- 4. שקיפות תהליכים והרתעה:** שימוש בכלים דיגיטליים, כגון מצלמה המתעדת את תהליך ספירת הקולות וסיכום התוצאות, מאפשר שקיפות של התהליך והרתעה מפני ביצוע פעולות הפוגעות במהימנותו. בבחירות הכלליות לכנסת נעשה שימוש במצלמות.

קידום דיגיטציה ומיכון בתהליכי הבחירות

הליך הבחירה בישראל הוא כאמור ברובו ידני. יש שימוש במערכות מידע, אולם מרביתן משמשות בעיקר בתקופת ההיערכות לבחירות לצרכים האלה: הפקת קובץ של שמות בעלי זכות בחירה; גיוס והכשרה של עובדים; ניהול משימות לקראת הבחירות; העברת מידע על בעלי זכות הבחירה למועמדים; הנגשת מידע על הבחירות למועמדים ולבעלי זכות הבחירה; איתור מקום ההצבעה; והזנת תוצאות הבחירות ופרסומן לציבור.

בנובמבר 2007 קיים המפקח הארצי על הבחירות דאז פיילוט של בחירות ממוחשבות לרשויות המקומיות בד בבד עם בחירות האמת⁷. מטרת הפיילוט הייתה לבחון את ההיתכנות של קיום בחירות אלקטרוניות על ידי מחשוב ועדת הקלפי, ניהול פנקס בוחרים ממוחשב, זיהוי אלקטרוני של הבוחר וביצוע הצבעה ממוחשבת על גבי מסך מגע. לפי תפיסת משרד הפנים, מטרת הפיילוט הושגו בהצלחה, ובסקר שביצע המשרד בעקבות הפיילוט עלה שרוב הציבור תומך בהצבעה אלקטרונית (מטעמים של אמינות, דיוק, מהירות ופשטות). לנוכח האמור, תוכנן לקיים בחירות אמת ממוחשבות בחמש רשויות⁸. ביצוע בחירות לרשויות המקומיות באמצעות מערכות ממוחשבות דורש שינויי חקיקה, ולכן בשנת 2009 הוגשה הצעת חוק לתיקון חוק הרשויות המקומיות (בחירות), התשכ"ה-1965, לצורך קיום הצבעה וסיכום קולות הבוחרים באופן ממוחשב, וההצעה הוגשה שנית בשנת 2013⁹.

בשנת 2019 החל משרד הפנים לפתח מערכת מחשוב חדשה לניהול בחירות ברשויות - מערכת א' - שיועדה לנהל את כל תהליכי הבחירות (הפצת פנקס הבוחרים, אישור מועמדים, סיכום תוצאות וכו'). פיתוח המערכת הוקפא במאי 2023, ולפיכך היא לא היתה בשימוש במערכת הבחירות בשנת 2024, וטרם הוחלט אם להמשיך בפיתוח המערכת לצורך מערכות בחירות עתידיות.

כאמור, מחשוב תהליך הבחירות ותתי-התהליכים בו יוכלו לסייע בהיבטים רבים. להלן דוגמאות לצורך במיכון תהליכים שכיום מתבצעים באופן ידני בבחירות לרשויות המקומיות, חלקם מבוצעים באופן ממוכן בבחירות הכלליות לכנסת, וחלקם גם אופייני במכרז להקמת מערכת מחשוב חדשה לניהול בחירות ברשויות - מערכת א' - שיועדה לנהל את כל תהליכי הבחירות (הפצת פנקס הבוחרים, אישור מועמדים, סיכום תוצאות וכו'):

טפסים מקוונים (Forms)

בתהליך המתבסס על מאגר מידע ממוחשב שימוש בטפסים ידניים מצריך שלב נוסף שבו נדרשת הזנת הנתונים מטופס ידני למערכת המידע, ולרוב הגורם המזין מידע זה אינו הגורם שיצר את התוכן. מיכון הטפסים ושימוש בטופס מקוון מאפשר הזנה ישירה של המידע באמצעות יוצר המידע למערכת. באופן זה נחסך זמן הקלדה, נמנעות טעויות הקלדה שבוצעו בשוגג, ניתן לבצע במערכת בדיקה ממוכנת לאימות הנתונים (Validation) וכן ניתן לנטר את מועדי קבלת הנתונים ולתעדם. להלן דוגמאות לשימוש בטפסים ידניים בתהליך הבחירות לרשויות המקומיות:

טופסי הגשת מועמדות: בתקופה שלפני יום הבחירות לרשויות המקומיות מועמדים ורשימות נדרשים להגיש טופסי מועמדות ידניים למנהל הבחירות האזורי וליחידת המפקח לצורך קליטת הטפסים, בקרה עליהם והזנה ידנית של המידע שבהם למערכת ג'. בבחירות שהתקיימו בשנת 2024 הגישו 737 מועמדים ו-3,643 רשימות טופסי מועמדות, וכל חוברת כללה עשרות עמודים המכילים נתונים שיש להזין. הליך הזנת הנתונים למערכת ג' התבצע במשמרות, לאורך כל שעות היממה (24 שעות) ובמשך כמה ימים והצריך בירור, ולעיתים אף התערבות משפטית, עקב כתב יד לא ברור, נתונים חסרים או נתונים שמולאו שלא בהתאם להוראות. בתהליך היו מעורבים

⁷ הפיילוט נעשה בשישה יישובים בתחום שיפוטן של ארבע מועצות אזוריות (מנשה, זבולון, לב השרון וחוף אשקלון), והשתתפו בו כ-5,300 בוחרים ב-12 קלפיות.

⁸ הצבעה אלקטרונית בבחירות - סקירה משווה, מרכז המחקר והמידע של הכנסת, מ-5.8.08.

⁹ הצעת חוק הרשויות המקומיות (בחירות) (תיקון -בחירות ממוחשבות), התשס"ט-2009; הצעת חוק הרשויות המקומיות (בחירות) (תיקון - בחירות ממוחשבות), התשע"ג-2013.

גורמים רבים מגופים שונים (מנהלי בחירות, קלדנים, יועצים משפטיים, מטמיעים של מערכת ג'י' וטכנאים). בהקשר זה, המפקח ציין שמסתמנת מגמת גידול במספר המועמדים במערכות הבחירות, וכי ללא הטמעת טכנולוגיה ושימוש בדיגיטציה תתקשה היחידה להתמודד עם מספר המועמדים בבחירות הבאות.

פרוטוקול מזכירי קלפי: בליל הבחירות ועדת הקלפי ומזכירי ועדת הקלפי ממלאים פרוטוקול (טופס ידני) לסיכום תוצאות הבחירות בקלפי, והוא מועבר למרכז הקליטה ברשות הרלוונטית. בליל הבחירות מנהל הבחירות וגורמים מטעמו נדרשים לקלוט את הפרוטוקולים ולוודא כי נתונים תקינים, וזאת לצורך היערכות להזנת תוצאות ההצבעה המצוינות בפרוטוקול למערכת ב' וסיכום תוצאות הבחירות ברשות.

טופס קליטת קלפיות: צוותי הביקורת בליל הבחירות מצאו כי ב-10 (83%) מתוך 12 הרשויות שנבדקו¹⁰ (אלעד, אריאל, בני ברק, חיפה, ירכא, כרמיאל, מרחבים, פתח תקווה, קריית מוצקין וראש העין) המעקב אחר קבלת כלל הקלפיות נעשה באופן ידני (סימון כל פרוטוקול שהגיע לוועדת הקליטה) וכי בשתי רשויות (ירושלים ובאר שבע - 17% מכלל הרשויות) נוהל המידע בדבר הגעת הקלפיות במערכת מידע באופן שהיה נגיש וקריא יותר.

תמונה 1: מעקב אחר קבלת קלפיות באופן ידני ובאמצעות מערכת מידע, ליל הבחירות



צולם על ידי צוותי משרד מבקר המדינה ב-27.2.24.

יחידת המפקח אינה מבצעת מיכון של טפסים ידניים שבהם היא משתמשת לצורכי הבחירות, כגון אלפי טופסי הגשת מועמדות (שהתקבלו מ-737 מועמדים ו-3,643 רשימות) וכ-11,000 פרוטוקולי ההצבעה המכילים עמודים רבים כל אחד. שימוש בטפסים ידניים מחייב הזנת נתונים במערכות באמצעות כוח אדם שאינו בעל המידע, באופן שמחייב תשומות עבודה ותשומות זמן גבוהות יותר מהנדרש בתהליך ממוכן (למשל, בהליך הגשת מועמדות בוצעו כ-500,000 תנועות לצורך הזנת הנתונים למערכת) וחושף את הזנת הנתונים לטעויות אנוש (למשל, טעויות הקלדה) ולסיכון של דלף מידע בעת שינועם של חומרים רגישים.

בתשובת משרד הפנים מנובמבר 2024 נמסר כי שימוש בממשקים דיגיטליים יפחית טעויות אנוש שמתרחשות במסגרת העברת נתונים באופן ידני למערכות. במערכת הבחירות הנוכחית המשרד הטמיע מנגנון בקרה כדי לתת מענה על נושא זה. כיום נעשה במשרד שימוש בטפסים מקוונים לצורכי הגשת בקשה לקבלת פנקס בוחרים, בקשת מימון ופניות ציבור, ועם זאת במקרים

¹⁰ מעקב ידני אחר קבלת פרוטוקולים בוצע ברשויות אלה: אלעד, אריאל, בני ברק, חיפה, ירכא, כרמיאל, מרחבים, פתח תקווה, קריית מוצקין וראש העין; מעקב באמצעות מערכת מבוססת ברקוד בוצע רק בבאר שבע. בירושלים בוצעו מעקב ידני ומעקב ממחשב במערכת של הרשות.

מסוימים הרחבת השימוש כאמור מחייבת שינוי חקיקתי. בשנת 2023 החל משרד הפנים בקידום הצעת חוק לשינוי חקיקתי הנוגע להטמעת מערכת ממוכנת שתשמש בהליך הגשת הרשימות ובדיקתן, אך במועד סיום הביקורת הצעת החוק טרם אושרה.

מומלץ כי יחידת המפקח תרחיב את השימוש בטפסים מקוונים לתהליכים נוספים כגון: טופסי הגשת רשימות, פרוטוקול מזכירי קלפי, וטופסי קליטת קלפיות, ובהתאמה את הצורך בייזום שינויי חקיקה, אם הדבר ידרש.

ניתוח נתונים

כלי ניתוח נתונים ובינה מלאכותית מאפשרים לעבד מידע (Data) ולהפיק ממנו תובנות נוספות באמצעים סטטיסטיים. ניתן להפיק מכלים אלה יכולות שונות, ובהן: זיהוי חריגות (Anomaly Detection), שיבוץ רנדומלי תואם חוקיות (Fair Random Assignment) וחיזוי מגמות (Time-Series Prediction). להלן דוגמאות לפעולות בתהליך הבחירות המתבצעות ללא שימוש בכלי ניתוח נתונים מתקדמים:

שיבוץ חברי ועדת קלפי: לפי חוק הרשויות המקומיות (בחירות), התשכ"ה-1965, הרכבה הסיעתי של ועדת הקלפי ייקבע על ידי ועדת הבחירות מבין כל הסיעות המיוצגות, ובלבד שבכל ועדת קלפי ייוצגו לפחות שלוש סיעות, אם אכן משתתפות בבחירות לפחות שלוש סיעות, וזאת באופן שיובטח ייצוג הולם של כל הסיעות. מנהל הבחירות נדרש לבצע בקרה על שיבוץ ועדות הקלפי, כדי לוודא ששיבוץ בוצע בהתאם לדין¹¹.

צוותי הביקורת מצאו כי מנהלי הבחירות בכל 13 הרשויות שבהן ביקרו בליל הבחירות¹² השתמשו בקובצי אקסל לצורך ניהול השיבוץ של עשרות אלפי ועדות הקלפי שלא כללו כלי בקרה על נכונות השיבוץ, וכך נעשה גם בשתי רשויות נוספות שצוות הביקורת בדק לפני יום הבחירות¹³. הנחיה דומה בדבר הרכב ועדות הקלפי ניתנה גם לגבי הבחירות הכלליות לכנסת. החל משנת 2013 ועדת הבחירות המרכזית לכנסת משתמשת בבחירות הכלליות במערכת מידע ייעודית, המנהלת באופן ממוחשב את הליך שיבוץ נציגי הסיעות בוועדות הקלפי בהתאם למבנה ולהרכב של הוועדות שמוגדר בחוק¹⁴.

יחידת המפקח משתמשת בכלים ממוכנים בסיסיים בביצוע פעולות ליבתיות בהליך הבחירות, שאינם מאפשרים ביצוע חישובים מורכבים. כמו כן היחידה מבצעת פעולות באופן ידני (על ידי גורם אנושי) שחשוף לטעויות (למשל, טעויות הקלדה). זאת בשעה שקיימים כלי ניתוח נתונים מתקדמים הזמינים בשוק, כגון כלים לשיבוץ רנדומלי תואם חוקיות (לצורך בקרה על שיבוץ נציגי סיעות בוועדות קלפי), אשר יכולים לסייע לה במניעת טעויות אנוש או בזיהוי פעולות המעלות חשש לפגיעה בטוהר הבחירות.

מומלץ כי יחידת המפקח תבחן שימוש בכלי ניתוח נתונים מתקדמים לצורכי תהליך הבחירות.

11 חוק הרשויות המקומיות (בחירות), התשכ"ה-1965 - סעיף 32; דיני הבחירות למועצות האזוריות - סעיף 1א4.

12 אלעד, אריאל, באר שבע, בני ברק, חיפה, ירושלים, ירכא, כרמיאל, מרחבים, עכו, פתח תקווה, קריית מוצקין וראש העין. עיריית באר שבע השתמשה, נוסף על קובצי אקסל, במערכת מידע לניהול הבחירות שרכשה לטובת הבחירות.

13 גוש עציון ומגדל העמק.

14 חוק הבחירות לכנסת [נוסח משולב], התשכ"ט - 1969 - [סעיף 21](#); דין וחשבון שנתי על פי חוק חופש המידע, התשנ"ח-1998 - עמוד 65.

זיהוי בוחרים ובדיקת זכאות הצבעה

ביום הבחירות בעלי זכות בחירה זכאים להצביע בקלפי מסוימת הנמצאת ברשות שלהם, למעט מי שאושר לו על פי חוק (למשל - חיילים) להצביע בקלפי מיוחדת שאינה נמצאת בהכרח ברשות שלו. ההצבעה מתבצעת באופן המפורט להלן:

1. הצבעה בקלפי של הבוחר: בשלב הראשון מזכיר הקלפי נדרש לזהות את הבוחר באופן ידני מול תעודה מזהה ולוודא שהוא בעל זכות בחירה (מול רשימת הבוחרים באלפון), כדי למנוע ניסיונות של הצבעות לא חוקיות (למשל, הצבעה בשם נפטר או שוהה בחו"ל). לאחר מכן, הבוחר ניגש להצביע באמצעות פתקי הצבעה ידניים עבור מועמד ורשימה.

2. הצבעה באמצעות מעטפה חיצונית: בשלב הראשון מזכיר הקלפי נדרש לזהות את הבוחר באופן ידני מול תעודה מזהה ולמלא את פרטי הבוחר על גבי מעטפה חיצונית. לאחר מכן הבוחר ניגש להצביע באמצעות פתקי הצבעה ידניים עבור מועמד ורשימה. הבוחר מכניס את המעטפה ובה פתקי ההצבעה למעטפה החיצונית הכוללת את פרטיו.

המעטפות החיצוניות שאינן שייכות לאותה רשות שבה נמצאת הקלפי משונעות למרכז מיון מרכזי, ממוינות לפי רשויות ומשונעות לרשות הרלוונטית. מנהל הבחירות בכל רשות מבצע בדיקת זכאות בחירה ידנית לגבי כל מעטפה חיצונית השייכת לרשות שלו מול האלפונים של כלל הקלפיות ברשות (ומול יתר המעטפות החיצוניות). בבחירות הנוכחיות (לשנת 2024) הצביעו בסבב א' בסך הכול 114,578 בוחרים באמצעות מעטפות חיצוניות, ובסבב ב' - 7,497 בוחרים. למשל, בירושלים מנהל הבחירות נדרש לאמת ידנית זכאות של 6,590 מצביעים שהצביעו במעטפות חיצוניות מול האלפונים של 826 קלפיות. בתמונה להלן מוצג תהליך הבדיקה של 1,051 מעטפות חיצוניות בבחירות סבב א' בראש העין שבוצעה מול 85 אלפונים.

תמונה 2: בדיקת מעטפות חיצוניות, ראש העין, סבב א'



צולם על ידי צוותי משרד מבקר המדינה ב-28.2.24.

לצורך בדיקת הזכאות להצבעה וזיהוי ומניעת הצבעות כפולות בבחירות המרכזיות לכנסת משתמשת ועדת הבחירות המרכזית בתוכנה ייעודית.

נמצא כי תהליך הבחירות לרשויות המקומיות בשנת 2024 עלה 1.26 מיליארד ש"ח (לא כולל יום שבתון) וכי הוא ברובו ידני, ובכלל זה שני הליכים ליבתיים - ההצבעה ותהליך זיהוי הבוחרים שהם בעלי פוטנציאל מחשובי. המעבר להליכי זיהוי דיגיטליים החל להיות מיושם במערכות בחירות שונות בעולם¹⁵ לנוכח היתרונות הגלומים בו: ניהול יעיל יותר, הפחתה של הסיכון

¹⁵ מבקר המדינה, דוח שנתי של מבקר המדינה - מרץ 2022 (2022), "מערכות מידע והגנת הסייבר בבחירות לכנסות ה-21, ה-22 וה-23", עמ' 1078.

לפגיעה בטוהר הבחירות וייתור של הצורך בשינוע חומרים רגישים (כגון אלפונים) שחושפים את הארגון לדלף מידע.

בסבירות גבוהה במהלך השנים הבאות נושא המעבר לזיהוי הדיגיטלי יעמוד על הפרק. על כן, על משרד הפנים ויחידת המפקח ליזום עבודת מטה לצורך בחינת חלופות ומשמעויות של מעבר עתידי לזיהוי דיגיטלי של בוחרים והיערכות מתאימה שתיתן מענה גם לסיכונים הפוטנציאליים בהיבטי אבטחת מידע הגלומים במהלך. יצוין כי טיבו המבוזר של הליך הבחירות לרשויות המקומיות (כל רשות בפני עצמה) מאפשר מעבר מבוקר והדרגתי ליישומים דיגיטליים תוך יישום מודל של פיילוט.

יצוין כי עוד בדצמבר 2013 הקים שר הפנים דאז ועדה ציבורית לבחינת מחשוב מערכות הבחירות לכנסת ולרשויות המקומיות (להלן - הוועדה הציבורית). הוועדה התבקשה לבחון בין היתר סוגיות הנוגעות לאבטחת המידע, לתשתיות הטכנולוגיות בארץ ובעולם, להגדלת שיעור ההצבעה, להבטחת חשאיות הבחירות, לטוהר הבחירות ולעלויות הצפויות של הטיפול בסוגיות האמורות¹⁶. עבודת הוועדה הופסקה בשנת 2014, ומאז הנושא לא קודם על ידי שרי הפנים והמפקחים על הבחירות, אף שתהליך בחירות ממוחשב מתקיים זה מכבר בהליכי פריימריז של חלק מהמפלגות בישראל ואף מתקיים במספר מדינות בעולם, זאת למעט ניסיון נקודתי בשנת 2023 של משרד הפנים למחשוב הליך הגשת הרשימות ולבדיקתן, במסגרת הצעת חוק שטרם אושרה.



מכל האמור לעיל עולה כי ביצועם של תהליכים ידניים בבחירות לרשויות המקומיות עלול לפגום ביעילות הבחירות ובטוהר הבחירות. מומלץ כי שר הפנים יקדם את הדיגיטציה ואת מיכון תהליכי הבחירות שהם בעלי פוטנציאל מחשובי, כמו זיהוי הבוחרים באמצעים ביומטריים, הצבעה ממוחשבת, מיכון של טופסי הגשת מועמדות ופרוטוקולים של מזכירי קלפי, הקמת מערכת ניהול של רשימת מצביעים ליעול הטיפול במעטפות חיצוניות (שבבחירות הנוכחיות מספרן היה 114,578 בסבב א', ו-7,497 בסבב ב'), ניהול ממוחשב של תהליך שיבוץ הרכב ועדות הקלפי ושימוש בטכנולוגיות של בינה מלאכותית. מיכון תהליכים אלו יאפשר ייעול של משאבי זמן וכוח אדם, יקנה יכולת לנתח ולעבד מאגרי מידע גדולים, יתרום לשיפור אבטחת המידע בתהליך הבחירות ובפרט של חומר רגיש ולהפחתת הצורך בשינוע, ויסייע בניהול הליכי בקרה, בהגברת שקיפות תהליכים והרתעה ובהפחתת הסיכון לטעויות אנוש ולפגיעה בטוהר הבחירות. במסגרת קידום הדיגיטציה יובאו בחשבון עלות הליך הבחירות ברשויות המקומיות בשנת 2024, שנאמדה ב-1.26 מיליארד ש"ח לא כולל עלות יום שבתון, קיומן של בחירות ממוחשבות בארץ בכמה גופים לא מדינתיים (למשל, תהליכי פריימריז למפלגות) ובמדינות שונות כמו ארה"ב ואסטרטוגיה, וטיבו המבוזר של הליך הבחירות לרשויות המקומיות (כל רשות בפני עצמה), שמאפשר מעבר מבוקר והדרגתי ליישומים דיגיטליים תוך יישום מודל של פיילוט. כמו כן מומלץ כי שר הפנים ישקול ייזום שינויי חקיקה בנושא, אם הם יידרשו.

בתשובת משרד הפנים מנובמבר 2024 נמסר כי יחידת המפקח תברך על כל שיפור בתהליכי הבחירות, בדגש על תהליכים דיגיטליים שייעלו את תהליכי הבחירות, וכי היחידה פועלת לשיפור התהליכים במסגרת המדיניות שנקבעת על ידי השר ובהתאם להוראות החוק ומקדמת ככל שניתן את נושא הדיגיטציה במציאות הנוכחית.

היעדר שיתוף ידע ואיגום משאבים בין תהליכי הבחירות לכנסת ובין הבחירות לרשויות המקומיות

בישראל תהליך הבחירות לכנסת ותהליך הבחירות לרשויות המקומיות מנוהלים על ידי שני גופים שונים:

¹⁶ מבקר המדינה, דוח שנתי של מבקר המדינה - מרץ 2022 (2022), "מערכות מידע והגנת הסייבר בבחירות לכנסות ה-21, ה-22 וה-23", עמ' 1080.

1. ועדת הבחירות המרכזית - גוף סטטורי עצמאי, האחראי לניהול מערכת הבחירות לכנסת.
2. משרד הפנים - אחראי לניהול מערכת הבחירות לרשויות המקומיות.

בתרשים להלן מוצגים תהליכים דומים¹⁷ המתקיימים בבחירות לרשויות המקומיות ובבחירות לכנסת ומערכות המחשוב התומכות בכל תהליך.

תרשים 4: מערכות המחשוב התומכות בתהליך הבחירות לרשויות המקומיות ובתהליך הבחירות לכנסת



המקור: נתוני משרד הפנים ודוח מבקר המדינה, מערכות מידע והגנת הסייבר בבחירות לכנסת ה-21, ה-22 וה-23 (2022).

הפרטים המובאים בתרשים מצביעים על כך שהתהליכים העיקריים המתקיימים בשתי מערכות בחירות (בבחירות לכנסת ובבחירות המקומיות) שמתקצבות ומתוחזקות על ידי שני גופים ציבוריים - ועדת הבחירות המרכזית (בבחירות לכנסת) ומשרד הפנים (בבחירות לרשויות המקומיות) המתמודדים עם אתגרים מקצועיים שחלקם דומים, נוהלו ופותחו לאורך השנים ללא כל תיאום ושיתוף ידע ביניהן וללא איגום משאבים - באופן שלא אפשר ניצול יעיל ומיטבי של משאבי הציבור באותם מקומות בהם הדבר יכל להיעשות. עבודה משותפת עשויה לתרום בלימוד הדדי שעשוי לשפר תהליכים דומים ולצמצם סיכונים לפגיעה בטוהר הבחירות, לייעל מערכות ולמנוע כפילות בפיתוח ובתחזוקה של מערכות מידע דומות (יצוין כי בעת הזו שני הגופים נמצאים בתהליכים נפרדים של פיתוח מערכות ממוחשבות חדשות). כמו כן הליך זה יתרום לקידום תהליכי חשיבה ותכנון בתחום הדיגיטציה והמיכון בשתי מערכות בחירות אלו.

בתשובת משרד הפנים מנובמבר 2024 נמסר כי רק חלק מהמערכות שנועדו לשימוש בבחירות בכנסת יכולות להתאים לבחירות ברשויות המקומיות (למשל גיוס, הכשרה, שיבוץ מועמדים ופרסום מידע לציבור). כמו כן נמסר כי במקרים מסוימים השימוש בדיגיטציה בתהליכים שונים במסגרת הבחירות (למשל, מיכון הגשת רשימות) מחייב שינוי חקיקתי ופיתוח מערכות מידע המותאמות לתהליכי הבחירות. בעניין זה, בשנת 2023 החל המשרד לקדם הצעת חוק לצורך שינוי חקיקתי נקודתי בעניין הטמעת מערכת ממוכנת להליך הגשת הרשימות ובדיקתן, אך למועד סיום הביקורת הצעה זו טרם אושרה.

נוכח הדמיון בין הבחירות לרשויות המקומיות ובין הבחירות לכנסת מבחינת התהליכים העסקיים ומערכות המידע המשמשות את שלבי ההיערכות לבחירות ואת ניהול הבחירות, וכן

¹⁷ התהליך העסקי העיקרי דומה, אולם תיתכן שונות בהתאם לסוג הבחירות. למשל: מספר פתקי ההצבעה בבחירות לרשויות המקומיות שונה ממספר פתקי ההצבעה בבחירות לכנסת.

נוכח העובדה שמשרד הפנים וועדת הבחירות המרכזית נמצאים בשלבי תכנון וייזום של מערכות מידע חדשות לניהול תהליכי הבחירות, מומלץ כי שר הפנים בתיאום עם יו"ר ועדת הבחירות המרכזית יחדש את עבודת הוועדה לבחינת מחשוב מערכות הבחירות לכנסת ולרשויות המקומיות שהופסקה בשנת 2014, ויפעל בהסכמה ובשיתוף עם יחידת המפקח ועם ועדת הבחירות המרכזית להקמת פורום לקידום הדיגיטציה והמיכון בתהליכי הבחירות ולשיתוף ידע ואיגום משאבים. זאת כדי לאפשר התמודדות עם האתגרים באמצעות שילוב הטכנולוגיה בתהליך הבחירות לצד הקמת מנגנונים הכוללים היבטי אבטחת המידע והגנת הסייבר.

בתשובת משרד הפנים נמסר כי הוא מקבל את ההמלצה, וכי יחידת המפקח תפעל בהתאם להנחיות השר ולפיהן יש להשלים את עבודת הוועדה לבחינת מחשוב מערכות הבחירות לכנסת ולרשויות המקומיות.

בתשובות ועדת הבחירות המרכזית מפברואר ומספטמבר 2024 נמסר כי לפי עמדתה אין מקום לחידוש עבודת הוועדה הציבורית בשל פרק הזמן הממושך שעבר מאז הופסקה העבודה (עשר שנים) ולנוכח העובדה שהוועדה ביצעה פעילות כה רבה לקידום הדיגיטציה משנת 2021. לטענת ועדת הבחירות, כל פעילות של ועדה חדשה תעכב את התהליכים הקיימים ותביא לירידתם לטמיון של משאבי המדינה שכבר הושקעו. להלן עיקרי התהליכים שהוועדה ביצעה לקידום דיגיטציה בכלל תהליכי הבחירות לכנסת: מינוי ועדת היגוי לאפיון מערכת המחשוב העתידית של הוועדה; הקמת מינהלת שפועלת להקמת מערכת מחשוב עתידית של הוועדה ולגיבוש מכרז שצפוי להתפרסם בקרוב; וקביעת מפת דרכים (roadmap) למחשוב כלל התהליכים המקצועיים. כמו כן הדגישה הוועדה כי לצד היתרונות בשילוב הדיגיטציה בתהליכי הבחירות קיימים סיכונים שיש לבחון, ובכללם תקלות תקשורת, כשלי תוכנה וסיכוני סייבר.

כמו כן מסרה הוועדה כי לדעתה יש ערך בהחלפת דעות מקצועיות בין קבוצות העבודה של משרד הפנים לקבוצות הפועלות מטעמה, אולם כדי למנוע סיכוני סייבר ולהותיר את המערכות מוגנות ועמידות יש להקפיד על הפרדה, שונות ויתירות בין מערכות המידע שישמשו לקיום הבחירות לרשויות המקומיות לבין אלו שישמשו לקיום הבחירות לכנסת.

עוד מסרה הוועדה בהתייחסותה כי נוכח המלצת מבקר המדינה בדוח קודם שהתפרסם במרץ 2022 למחשב את תהליך זיהוי הבחור באמצעים ביומטריים, היא בחנה את השימוש בתעודות זהות חכמות לצורך הבחירות ומצאה כי נכון למועד הבחינה לא הייתה אפשרות להשתמש בתעודות זהות אלה, וכי יש חסרונות רבים בהליך זה, לרבות עלויות אסטרונומיות וחוסר בשלות טכנולוגית לפריסה רחבה.

בהתייחס לתשובות ועדת הבחירות המרכזית מפברואר 2024 ומספטמבר 2024 מעיר משרד מבקר המדינה לוועדה כי הנושא ראוי לבחינה נוספת של ועדה המשותפת לה ולנציגי משרד הפנים, בשים לב לתהליכי פיתוח טכנולוגיים המקודמים בעת הזו ממש הן בוועדת הבחירות המרכזית והן במשרד הפנים. שיתוף המידע והבחינה המשותפת בנושא זה מתבקשים לאור הדמיון שבין התהליכים העסקיים העיקריים בשתי מערכות הבחירות. נוסף על כך מומלץ להביא לפני הוועדה המשותפת את השאלה אם ראוי לפתח תשתית משותפת לשתי מערכות הבחירות או לאפיין תהליכים במשותף ולאחר מכן לפתח תשתיות שונות בשים לב לסיכוני סייבר, ללוחות זמנים ולעלויות.

כמו כן ראוי כי ועדת הבחירות המרכזית תאמץ בעניין זה תפיסה צופה פני עתיד שמעלה על המסילה הליכי בחינה, ניסוי ויישום ממשיים של נדבכים בתחום הדיגיטציה של הבחירות. אופיו ומהותו של הנושא מצדיקים תפיסה כזו תוך יישומה באופן זהיר ומדורג. עוד יוער לוועדת הבחירות המרכזית כי מהבחינה הטכנולוגית ראוי לבחינה האפשרות לזיהוי בוחרים בבואם לוועדת הקלפי באמצעים ביומטריים, בדומה לשימוש שנעשה בביקורת הגבולות לזיהוי העוברים והשבים בכניסה לישראל וביציאה ממנה, ולכן ראוי כי הוועדה המשותפת תבחן פתרונות מגוונים לנושא זה.

ליווי גופים אסדרתיים מדינתיים בתחום אבטחת המידע והגנת הסייבר

המחוקק התייחס לתחום אבטחת המידע והגנת הסייבר בחקיקת החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון); בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות); ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע). כמו כן קיבלה הממשלה כמה החלטות בתחום זה (ב/84, 2443, 2444, 3611)¹⁸. בהתאם להחלטות הממשלה ולחוק להסדרת הביטחון, האחריות להנחיית תחום אבטחת הסייבר נחלקת בין כמה גורמים. להלן רשימת הגופים האסדרתיים המדינתיים בתחום אבטחת המידע והגנת הסייבר שבהם עוסק הדוח:

מערך הסייבר: בשנת 2016, במסגרת מימוש החלטות הממשלה בדבר גורם לאומי בתחום הגנת הסייבר, עודכן החוק להסדרת הביטחון, והאחריות להנחיית רוב הגופים שמוגדרים כתשתיות מדינה קריטיות (להלן - גופי תמ"ק) הועברה למערך הסייבר¹⁹. בהתאם לכך מנחה מערך הסייבר ישירות את גופי התמ"ק המצוינים בתוספת החמישית לחוק, והוא אחראי ללוות את הגופים באופן שוטף ולסייע להם, בין היתר, בהכנת תוכנית העבודה השנתית בתחום הגנת הסייבר, במעקב אחר ביצועה ובפיקוח על אופן היישום של תורת ההגנה הייעודית בגופי תמ"ק (להלן - התו"ל הייעודי). נוסף על כך, מערך הסייבר פרסם למשק הישראלי הנחיות המייצגות סטנדרטים מקובלים בתחום הגנת הסייבר (להלן - תורת ההגנה 2.0 או תורת ההגנה). מערך הסייבר גם מבצע מבדקי חדירה ומחקרי תקשורת בגופים שהוא מנחה. כמו כן, האגף הארצי לניהול אירועי סייבר במערך הסייבר יכול לסייע לגוף כשיש חשש לאירוע סייבר שעשוי להסב לו או לגופים אחרים נזק חמור.

במסגרת תפקידו מערך הסייבר מנחה את מערך הדיגיטל ואת רשות האוכלוסין שתשתיות המחשוב והמערכות המידע שלהן משמשות גם בהליך הבחירות.

היחידה להגנת הסייבר בממשלה (להלן - יח"ב): היחידה הוקמה בעקבות החלטת הממשלה 2443. ייעוד היחידה הוא לכוון ולהנחות מהבחינה המקצועית בתחום הגנת הסייבר את כלל משרדי הממשלה ויחידות הסמך, למעט גופי תמ"ק והגופים המיוחדים המפורטים בהחלטה, ולהקים מרכז שליטה ובקרה ממשלתי להתמודדות עם איומי הסייבר (SOC ממשלתי). יח"ב פרסמה מסמך מדיניות להגנת הסייבר בממשלה והנחיית מסגרת להגנת הסייבר בממשלה, הכוללים נהלים והנחיות המחייבים את המשרדים ומגדירים את אופן הניהול של תהליכים מרכזיים בנושא הגנת הסייבר (להלן - הנחיות יח"ב). היחידה מנחה את משרד הפנים, על כלל מערכותיו, ואינה מנחה באופן ייעודי את תהליך הבחירות.

הרשות להגנת הפרטיות: הרשות מאסדרת את כלל המשק ומופקדת על הגנה על הזכות לפרטיות, ובכלל זה על אבטחת המידע האישי השמור בכלל מאגרי המידע בישראל, בהתאם להוראות חוק הגנת הפרטיות ולתקנות אבטחת מידע. לשם כך הרשות מוסמכת לבצע אכיפה מינהלית ואכיפה פלילית הן בגופים פרטיים והן בגופים ציבוריים, בהתאם להוראות חוק הגנת הפרטיות ולתקנותיו. לפי תקנות אבטחת מידע, מאגר מידע המכיל מידע על מצבם האישי של אנשים ויש בו יותר מ-100,000 רשומות נדרש לעמוד ברמת אבטחה גבוהה. התקנות מפרטות כיצד יש לשמור על רמת האבטחה שנקבעה למאגר.

במסגרת פעילות יחידת המפקח לניהול הבחירות ברשויות המקומיות במשרד הפנים היא משתמשת במערכות מידע המכילות מידע רגיש ומידע שפגיעה בו עשויה לשבש את הבחירות או לפגוע ברמה התודעתית בסמלי שלטון (למשל - פנקס הבוחרים, תוצאות הבחירות, מידע אישי על

¹⁸ החלטת הממשלה 2443 מ-15.2.15 בנושא "קידום אסדרה לאומית ממשלתית בהגנת הסייבר". החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998; החלטת הממשלה 2444 מ-15.2.15 בנושא "קידום ההיערכות הלאומית להגנת הסייבר"; החלטת הממשלה 3611 מ-7.8.11 בנושא "קידום היכולות הלאומית במרחב הקיברנטי"; חוק הגנת הפרטיות, התשמ"א-1981; תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

¹⁹ גופי התקשורת נותרו באחריות השב"כ. רשימת הגופים והאחראים להם מובאת בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

מזכירי קלפי). נוכח זאת, רמת האבטחה של חלק ממאגרים אלו נדרשת להיות גבוהה לפי תקנות אבטחת מידע.

הליווי האסדרתי של תהליך הבחירות והפיקוח עליו בתחום אבטחת המידע והגנת הסייבר

מערכת הבחירות היא תהליך רגיש ומורכב שראוי שילווה על ידי גורם מדינתי מקצועי בכל הנוגע להיבטי אבטחת מידע והגנת סייבר. נוכח זאת, מערך הסייבר ליווה את ועדת הבחירות המרכזית לכנסת וסייע לה במסגרת תהליכי הבחירות הכלליות. בדוח ביקורת משנת 2022 המליץ מבקר המדינה כי מערך הסייבר ילווה את ועדת הבחירות באופן שוטף, בשגרה ובתקופת בחירות, והוועדה גם פנתה למערך בבקשה לבחון ליווי שלו בתקופות שגרה²⁰.

תהליך הבחירות לרשויות המקומיות נשען על שימוש בכמה מערכות מידע, חלקן מפותחות ומתוחזקות בתשתית של משרד הפנים, כאשר יה"ב אחראי להנחיה בעניין בכל הנוגע לאבטחת מידע והגנת סייבר (למשל: מערכת ב' ומערכת ד') וחלקן מפותחות ומתוחזקות על ידי גופי תשתיות מדינה קריטיות כמו רשות האוכלוסין ומערך הדיגיטל, ובהתאם מערך הסייבר הוא האחראי להנחיה בעניין. מכאן שאין גורם אחד שאחראי על ההנחיה הכוללת של כלל המערכות המעורבות בתהליך הבחירות לרשויות המקומיות.

לרוב פעילות הפיתוח של מערכות חדשות ושינויים במערכות הקיימות מתבצעים בתקופה שבין הבחירות. לדוגמה, בשנים 2019 - 2023 פעל משרד הפנים, בהנחיה של יה"ב, להקמת מערכת חדשה לניהול בחירות שהייתה אמורה להיות בשימוש בבחירות 2023. כמו כן, המשרד משתמש במערכות המידע עוד בתקופת ההיערכות לבחירות (כחצי שנה לפני יום הבחירות) ולכן יש קושי לבצע שינויים רבים במערכות בתקופת ההיערכות לבחירות.

באוגוסט 2021 פנה משרד הפנים למערך הסייבר בבקשה לקבל את הסיוע והליווי של מערך הסייבר בהקמה ובהפעלה של מערכת א'. בנובמבר 2021 השיב מערך הסייבר למשרד הפנים כי הקמת המערכת והאפיון המפורט ילוו על ידי יה"ב כמקובל, וכי ניתן יהיה להיוועץ במנחה מקצועי למגזר הממשלתי במערך הסייבר.

בינואר 2023 סוכם בין מערך הסייבר ליחידת המפקח שאם היחידה מעוניינת בליווי של מערך הסייבר בתהליכי הבחירות לרשויות המקומיות, עליה לשלוח למערך בקשה מסודרת בנושא. רק כעבור ארבעה חודשים, במאי 2023, פנתה יחידת המפקח למערך הסייבר בבקשה שילווה אותה בתהליך הבחירות שעתיד להיערך בסוף שנת 2023 - בשלב ההיערכות, בבחירות עצמן ובימים שלאחר מכן. בין ינואר ליוני התקיימו פגישות התנעה בין מערך הסייבר לבין משרד הפנים בנושא. בהמשך, בספטמבר 2023, לאחר ארבעה חודשים נוספים ופחות מחודשיים לפני מועד הבחירות המקורי, נעתר מערך הסייבר רשמית לבקשת הסיוע והליווי של יחידת המפקח, בבחירות אלה וביחס למערכות המחשוב והתהליכים הקריטיים להליך הבחירות, והגדיר במסמך את תחומי האחריות והסמכות של כל גורם (להלן - המסגרת ההסכמית).

בהתאם למסגרת ההסכמית, נקבע כי משרד הפנים הוא המנהל והמפעיל של מערכותיו, הנושא באחריות הכוללת להגנת הסייבר במערכות הממוחשבות של הגוף בכלל, ובמערכותיו הקריטיות בפרט. כמו כן, סוכם כי מערך הסייבר יגבש המלצות להעלאת רמת ההגנה של המערכות הקריטיות, בין היתר בהסתמך על מבדקי החוסן שיבוצעו למערכות ועל אמצעים משלימים בתחום ההגנה האקטיבית ובהתבסס על המידע שנצבר במערך. באחריות משרד הפנים ליישם את מסקנות המבדקים בהתאם למדיניות ניהול הסיכונים שיקבע המשרד. קרי, משרד הפנים יכול לבחור, בהתאם למדיניות ניהול הסיכונים שלו, לפעול על פי שיקול דעתו, ויכול לבחור לאמץ המלצות מסוימות ושלא לאמץ המלצות אחרות.

במסגרת הסיוע והליווי של הבחירות לרשויות המקומיות בשנת 2023 הקים מערך הסייבר צוות מבצעי מיוחד לליווי ולהכוונה בנושא המערכות העיקריות שמשתתפות בתהליך הבחירות. סיוע זה כלל, בין השאר, מיפוי המערכות הקשורות לבחירות בשיתוף עם משרד הפנים, הגדרת איום הייחוס הרלוונטי למערכות, סיווג פוטנציאל הנזק הנשקף מהן, וקיום תדריכים בהיבטי הגנת הסייבר לכלל השותפים, ריכוז תמונת מודיעין בתקופת ההיערכות לבחירות ובתקופת הבחירות וביצוע מבדקי חדירה נוספים על מבדקי החדירה של משרד הפנים למערכות. כמו כן, ביום הבחירות השתתף מערך הסייבר בחמ"ל של משרד הפנים שכלל נציגים ממשרד הפנים וממערך הדיגיטל וספקי המערכות, לצורך ניטור אירועי סייבר וטיפול בהם. כמו כן הוא ליווה את המערך בסבב ב' של הבחירות שהתקיים ב-11.3.24.

נמצא כי אין גורם אסדרתי מדינתי מתכלל בתחום אבטחת המידע והגנת הסייבר שתפקידו להנחות את תהליך הבחירות לרשויות המקומיות בכללותו, על כלל הגופים, המערכות, התשתיות והממשקים ביניהן, ולוודא כי הן עומדות ברמת הגנה ראויה. זאת אף שמדובר בפרויקט לאומי בעל השפעה רבה על הציבור בכללותו, החברה והמשק, שכולל שימוש במערכות מידע שפגיעה בהן עלולה לגרום לדלף מידע רגיש על מיליוני אזרחים, לפגיעה באמינות המידע שבמערכות, לפגיעה ברציפות התפקודית של המערכות ומשכך גם לפגיעה תודעתית בסמלי המדינה ובדמוקרטיה.

אמנם במהלך השנים הייתה מעורבות של מערך הסייבר ויה"ב בנוגע לליווי הפיתוח והתחזוקה של חלק מהמערכות בהיבטי אבטחת מידע ואולם מעורבות זו הייתה חלקית וחסרה והיא אינה נותנת מענה שלם לאור העובדה שהנחיותיו של יה"ב למשרד הפנים אינן ייעודיות לתהליך הבחירות - תהליך מורכב וייחודי, ואינן חלות על כלל המערכות המעורבות בתהליך הבחירות. גם המעורבות של מערך הסייבר על פי המסגרת ההסכמית שנקבעה לקראת הבחירות ב - 2023 מספקת מענה חלקי, שכן ההמלצות של מערך הסייבר להעלאת רמת ההגנה של המערכות הקריטיות חלות רק על חלק מהמערכות ואף מיושמות בהתאם לניהול הסיכונים שקבע משרד הפנים ועל פי שיקול דעתו (המשרד יכול לבחור לאמץ המלצות מסוימות ושלא לאמץ המלצות אחרות).

עוד נמצא כי רק במאי 2023, חמישה חודשים בלבד לפני מועד הבחירות המקורי (אוקטובר 2023) פנתה יחידת המפקח במשרד הפנים למערך הסייבר בבקשה רשמית שילוה אותה בתהליך הבחירות הנוכחי - בשלב ההיערכות, בבחירות עצמן ובימים שלאחר מכן. בפועל, רק בספטמבר 2023, לאחר ארבעה חודשים נוספים ופחות מחודשיים לפני מועד הבחירות המקורי, בזמן שכבר נעשה שימוש במערכות, סוכמו בין מערך הסייבר ומשרד הפנים ההסדרים שיעמדו בבסיס הליווי של יחידת המפקח באופן ממוקד בכל הנוגע למערכות המחשוב והתהליכים הקריטיים במערכת הבחירות 2023.

נוכח העובדה כי משרד הפנים הוא הגורם האחראי על פי חוק לניהול תהליך הבחירות בכללותו, על כלל היבטיו, לרבות בנושא הגנת הסייבר ונוכח התרומה של מערך הסייבר לליווי מערכת הבחירות, לשיפור רמת ההגנה ולשיתוף כלל הגורמים המדינתיים בתחום הסייבר במאמצי ההגנה על תהליך לאומי זה, מומלץ כי משרד הפנים ומערך הסייבר יפעלו לשינוי של האסדרה הקיימת, בין בחוק להסדרת הביטחון, בין בחוק הרשויות המקומיות (בחירות), התשכ"ה-1965, ובין במתכונת אחרת שתבטיח ליווי, הנחיה ופיקוח מחייבים ושוטפים של מערך הסייבר בבחירות לרשויות המקומיות על כלל המערכות, התשתיות והגופים המעורבים בתהליך, כפי שהומלץ בדוח מבקר המדינה בנוגע להנחיה השוטפת בעניין הבחירות הכלליות. יודגש כי אין בהסדרת הליווי, ההנחיה והפיקוח, כאמור, כדי לגרוע מאחריותו הכוללת של משרד הפנים להובלה וניהול של מערכת הבחירות ברשויות המקומיות. באופן זה תינתן מעטפת הגנה הוליסטית על כלל המערכות והתשתיות המשולבות בפרויקט (לרבות על הממשקים ביניהן), שכוללת יכולות למיפוי נכסים, להגדרת איום ייחוס, לריכוז תמונת מודיעין, לביצוע תדריכים ותרגילים ולביצוע מבדקי חדירה בכלל הגופים המשתתפים בבחירות. כמו כן, מומלץ כי מערך הסייבר ילווה את פיתוח המערכות גם בתקופה שבין הבחירות.

בתשובת משרד הפנים מנובמבר 2024 נמסר כי הוא מסכים בדבר הצורך בהסדרת הנחיית מערך הסייבר בבחירות לרשויות המקומיות ובביצוע פעולות אופרטיביות כל אימת שיש בידי המערך הכלים והיכולות הנדרשים.

בתשובת מערך הסייבר נמסר כי אין חולק על חשיבות הגנת הסייבר בהליך הבחירות לרשויות המקומיות. המערך רואה חשיבות בהמשך סיוע למשרד הפנים בהגנת הסייבר בתהליך הבחירות בהתאם לצורך שיעלה משרד הפנים ובהתאם לתיאום שייקבע מולו בשיתוף עם יח"ב. מערך הסייבר הבהיר שאף שרואה חשיבות בהמשך טיוב התהליך, אין מקום לסטות מהאיזונים המהותיים שנקבעו בחוק הבחירות לרשויות. בחוק הבחירות לרשויות, נקבע משרד הפנים, כגורם עליו מוטלת האחריות והסמכות החוקית על תהליך הבחירות לרשויות המקומיות בכללותו. הסדרת הגנת הסייבר אינה שונה בהיבט זה מכלל ההליכים הנדרשים לבחינה ותכלול על ידי משרד הפנים בהקשר הבחירות לשם הבטחת הליך בחירות תקין בהתאם לדין. כמו כן, המלצה לשינוי האחריות המתכללת והאיזונים השונים המעוגנים בחוק כאמור, עלולה להיות בעלת השלכות רוחב, תוך פגיעה באחריות הגורם האסדרתי המוביל.

בהתייחס לתשובת מערך הסייבר מעיר משרד מבקר המדינה כי אף שהאחריות על ניהול היבטי הסייבר בבחירות חלה על משרד הפנים, נדרש שיהיה גורם מדינתי בתחום הסייבר שינחה אותו לגבי כלל המערכות המשמשות את תהליך הבחירות והגופים המעורבים בו. מתכונת האסדרה צריכה להיות קבועה, מחייבת ושוטפת ולא להיות מוגבשת מחדש לקראת כל מערכת בחירות. מומלץ שאסדרה זו תחול גם בתקופות שבין מערכות הבחירות, שלרוב משמשת לאפיון ולפיתוח של מערכות לצרכים עתידיים.

פעולות הרשות להגנת הפרטיות להגנה על פנקס הבוחרים

יחידת המפקח מחויבת על פי חוק²¹ להעביר את המידע שבפנקס הבוחרים למועמדים, לסיעות ולבאי כוחם. הפנקס כולל מידע אישי (למשל - שם האב, כתובת, טלפון) על כלל תושבי מדינת ישראל. רשות האוכלוסין בין היתר מבצעת גזירה של פנקס הבוחרים²².

המידע שבפנקס הבוחרים מועבר גם לכנסת, במסגרת תהליך הבחירות הכלליות. במערכת הבחירות הכלליות לכנסת העשרים ושלוש ביצעה הרשות להגנת הפרטיות את הפעולות האלה²³:

1. קיום כנסים עבור מפלגות שהשתמשו במידע מפנקס הבוחרים, כדי להנחותן כיצד למנוע פגיעה בפרטיות של בעלי זכות הבחירה. כנס מפלגות כאמור התקיים גם בבחירות הכלליות לכנסת העשרים וארבע.
2. פרסום הנחיות הגנת הפרטיות בכל הנוגע לאיסוף מידע מפנקס הבוחרים, לעיבודו ולשימוש בו (התהליך נעשה גם בבחירות הכלליות לכנסת העשרים וארבע).
3. פיקוח רוחבי על מידת עמידתן של המפלגות ברמת האבטחה הנדרשת מהן, כבעלות מאגרי מידע מפנקסי בוחרים (ועל פעילותן מול ספקים).
4. פעולת אכיפה שכללה תחקור של אירועי דלף מידע והטלת קנסות: לאחר גילוי אירוע האבטחה של חברת ניהול תומכים בבחירות פתחה הרשות להגנת הפרטיות בחקירה, ובסופה הוטל על החברה קנס מינהלי בסך 25,000 ש"ח.

לקראת הבחירות לרשויות המקומיות ביצעה הרשות להגנת הפרטיות את הפעולות האלה:

21 חוק הרשויות המקומיות (בחירות), התשכ"ה-1965, סעיף 16.

22 גזירת פנקס היא תהליך ההוצאה של רשימת בעלי זכות בחירה ממרשם האוכלוסין.

23 מסמכי הרשות להגנת הפרטיות: דוח ממצאי הליך פיקוח הרוחב בקרב המפלגות שהתמודדו בבחירות הכלליות לכנסת העשרים ושלוש; ריענון הוראות חוק הגנת הפרטיות לקראת הבחירות לכנסת העשרים ושלוש; מגבלות השימוש במידע מפנקס הבוחרים ומוגבלות השימוש במידע אישי; דרישות חוק הגנת הפרטיות לקראת הבחירות לכנסת העשרים וארבע; מגבלות השימוש בפנקס הבוחרים ובמידע אישי אחר ואחריות המפלגות לאפליקציות ולספקים חיצוניים; דוח פעילות 2021 - עמ' 23.

1. החל בינואר 2023 הרשות להגנת הפרטיות ליוותה את תהליך הפיתוח של המערכת המקוונת להפצת פנקס הבוחרים (מערכת ד'), ששימשה תחליף להפצה הפיזית באמצעות תקליטורים, באופן שיתאים לדרישות אבטחת המאגר, ונתנה את אישורה להפצה באמצעות המערכת המקוונת לאחר ביצוע ההתאמות הנדרשות. בכלל זה, הרשות הציבה דרישות להגבלת מספר ההורדות של הקבצים ולביצוע ניטור ובקרה בעניין הורדתם.

2. הרשות סייעה בניסוח המסמכים הנלווים לקבלת פנקס הבוחרים, ובפרט בעדכון מקבל הפנקס בדבר המגבלות שחלות עליו²⁴.

3. בספטמבר 2023, מועד שנקבע בשיתוף עם יחידת המפקח, פרסמה הרשות להגנת הפרטיות מסמך הנחיות הגנת פרטיות²⁵ בכל הנוגע לאיסוף מידע מפנקס הבוחרים, לעיבודו ולשימוש בו, וכן מדריך פעולה ליישום תקנה 15 ותקנות הגנת הפרטיות בעת התקשרות עם גורם חיצוני. ההנחיות הופצו כחודשיים וחצי לאחר המועד שבו מועמדים היו רשאים לקבל את פנקס הבוחרים (יוני 2023, המועד הראשון של גזירת הפנקס).

4. בספטמבר 2023 הנחתה הרשות את יחידת המפקח לבצע את הפעולות האלה:

א. להפיץ את ההנחיות והמדריך לכל אחד מהמתמודדים שקיבל או יקבל עותק מפנקס הבוחרים בתוספת הבהרה שניתן לפנות לרשות לקבלת מענה על כל שאלה.

ב. לפרסם את ההנחיות באתרים של הרשויות המקומיות.

ג. לפרסם את ההנחיות בפורטל הבחירות לרשויות המקומיות.

לדברי הרשות להגנת הפרטיות, בתקופת מלחמת "חרבות ברזל" הרשות התמקדה בעיקר בהליכי פיקוח ואכיפה לנוכח הגידול במספר אירועי אבטחת מידע, וכן לנוכח הצורך לתת מענים נוספים עקב מצב החירום, ואלו השפיעו על אופן תיעודן המשאבים שלה ועל פעילותה היוזמה, לרבות בהקשר של הבחירות לרשויות המקומיות. למשל, בעניין אי קיום כנס מקוון שהיה אמור להתקיים ואי ביצוע פעולות אכיפה.

המידע בפנקס הבוחרים על אודות מיליוני בעלי זכות בחירה - מידע אשר מופץ לקראת הבחירות לגורמים רבים ובהם מאות מועמדים ואלפי רשימות - הינו מידע רגיש. מממצאי הביקורת עולה כי הרשות פרסמה הנחיות בספטמבר 2023, וכן הנחתה את יחידת המפקח להעביר הנחיות אלו למקבלי הפנקס באיחור שכן הדבר נעשה יותר מחודשיים לאחר המועד שמועמדים היו רשאים לקבל את פנקס הבוחרים, כך שממילא מידת הרלוונטיות שלהן הייתה מוגבלת משום שיתכן שבמועד זה כבר נעשה שימוש במידע שלא בהתאם לתקנות. עוד עולה כי הבחירות שתוכננו לאוקטובר 2023 נדחו בשל המלחמה בארבעה חודשים, בין השאר כדי לאפשר היערכות למערכת הבחירות בעת מלחמה ולתת מענה על כל ההיבטים הנדרשים. ואולם הרשות לא ביצעה בקרב מקבלי הפנקס פעולות אקטיביות חיוניות של הסברה ואכיפה אשר ביצעה בבחירות הכלליות לכנסת. זאת אף שפעולות הרשות נדרשות ביתר שאת בבחירות לרשויות המקומיות בהן המידע (פנקס הבוחרים) מופץ למספר רב יותר של מועמדים וסיעות ולפיכך הסיכון לפגיעה בו גדול יותר, ואף שבעת מלחמה חל גידול באירועי אבטחת מידע. לעניין זה מסרה הרשות להגנת הפרטיות כי היא לא נקטה בפעולות בין היתר בשל מגבלות משאבים בתקופת המלחמה, שכן חלק ממשאביה הופנו לטיפול באירועי אבטחת מידע חמורים במשק.

מומלץ כי הרשות להגנת הפרטיות תבצע פעולות משלימות להנחיות שפרסמה במסגרת הפצת פנקס הבוחרים בתהליכי הבחירות, כגון: הסברה פיקוח ואכיפה. כמו כן תבטיח כי הפעולות

²⁴ הנחיות לקבלת מידע פנקס בוחרים שליפה א' ושליפה ב'; טופסי הבקשה וההתחייבות של הסיעות כתנאי לקבלת פנקס הבוחרים, הכוללים פירוט מפורש של האיסורים והמגבלות על השימוש במידע בפנקס הבוחרים; מכתב המפקח הארצי על הבחירות ובו בקשה לקבלת תצהירי ביעור בסיום הבחירות; נספח תצהיר הביעור; מסמך שבו מוצגת עמדת הרשות בסוגיות של פרטיות ואבטחת מידע הקשורות בפנקס הבוחרים; גרפיקת תקליטור פנקס הבוחרים.

²⁵ משרד המשפטים, הרשות להגנת הפרטיות, מסמך הנחיות הגנת הפרטיות לקראת הבחירות לרשויות המקומיות (2023). www.gov.il/he/pages/guidelines_municipal_elections.

מתבצעות מבעוד מועד ובעיקר לפני שמתאפשרת הורדת הפנקס, כך שהפעולות יהיו אפקטיביות ורלוונטיות, בשים לב לסיכונים ולגורמים הרבים המעורבים במערכת הבחירות המקומיות אף מעבר למערכת הבחירות הארצית.

זיהוי אירועי סייבר והתמודדות עימם

מאז תחילת מלחמת חרבות ברזל זיהה מערך הסייבר גידול במספרם של התקיפות, של סוגי התקיפות ושל יעדי התקיפות במדינת ישראל. בשנת 2023 התקבלו 13,040 דיווחים שאומתו כאירועי סייבר, עלייה של 43% בהשוואה לשנת 2022, מתוכם 66% במהלך תקופת המלחמה. מספר האירועים המשמעותיים בתקופת המלחמה (מ-7 באוקטובר ועד לסוף שנת 2023) עמד על 3,380, גידול של פי 2.5 מבשגרה. כמו כן, מטרת מרבית התקיפות הייתה גרימת נזק, בניגוד למיקוד שזוהה לפני המלחמה שהתאפיין במטרות ריגול וגניבת מידע. תהליך הבחירות הוא תהליך דמוקרטי ליבתי בכל מדינה, ועשוי להיות מטרה לתקיפה בידי גורמים עוינים שנועדה לפגוע בתחושות הביטחון והאמון במוסדות המדינה, סיכון שגובר בנסיבות בהן הבחירות מתקיימות בשעת מלחמה, בדומה לבחירות שהתקיימו בפברואר 2024, ארבעה חודשים לאחר פרוץ מלחמת חרבות ברזל.

תורת ההגנה²⁶ מגדירה דרכים לגילוי מתקפות סייבר, להתמודדות עימן ולהתאוששות מהן. השלב הראשון בהתמודדות עם אירועי סייבר הוא הגדרת יעדי הגנה (מיפוי הנכסים שהארגון צריך להגן עליהם), מיפוי הסיכונים הנוגעים לנכסים אלו והגדרת איומי הייחוס על המשאבים הרלוונטיים לתהליך העסקי. המיפוי יאפשר הקצאה ממוקדת ויעילה של המשאבים הנדרשים להתמודדות עם איומים פוטנציאליים, בהתבסס על הצורך העסקי. משרד הפנים ובכלל זה יחידת המפקח, אמונים על ביצוע שלב זה בהליך הבחירות לרשויות המקומיות במסגרת אחריותם הכוללת לניהול תהליך הבחירות ועל בסיס היכרותם עם התהליכים הנכללים בהליך הבחירות, על כל היבטיו, ועם האיומים על תהליכים אלה.

ניתוח סיכונים ואיומים

בספטמבר 2023, כחודשיים לפני מועד הבחירות המקורי, הצטרף מערך הסייבר באופן רשמי כמסייע בקיום מערכת הבחירות וכמלווה שלה מרצון, לאחר שהמערך קיים כמה פגישות התנעה עם משרד הפנים. יחידת המפקח, בשיתוף מערך הסייבר, אגף טד"ם וגורמי האבטחה במשרד הפנים, מיפו חמש מערכות עיקריות ששימשו בבחירות.

כמו כן משרד הפנים (יחידת המפקח בשיתוף עם אגף טד"ם) ומערך הסייבר גיבשו מסמך איומי ייחוס בהיבטי סייבר הנוגע למערכות אלו והציגו אותו לכלל גורמי האבטחה. זאת ועוד, בהתאם לאיום הייחוס גובשה מעטפת הגנה לכל מערכת שהוגדרה במיפוי, ובוצעו פעולות לשיפור חוסנה כמו מבדקי חדירה, בדיקות עומסים ותיקון הליקויים שהועלו בבדיקות. חלק ממערכות אלו אף נוטרו במהלך יום הבחירות. ביום הבחירות נעשה שימוש במערכות נוספות על אלו שנכללו בתהליך המיפוי, אחת מהן משמשת את המשרד לצרכים שוטפים. לדברי משרד הפנים מערכת זו נבחנה בהיבטי אבטחת מידע לצורכי המשרד ולא בהיבט ייעודי לתהליך הבחירות ולסיכונים בו.

חודשיים לפני מועד הבחירות המקורי ביצע משרד הפנים (ובכלל זה יחידת המפקח, אגף טד"ם וגורמי האבטחה במשרד) בשיתוף מערך הסייבר מיפוי של מערכות המידע העיקריות שנעשה בהן שימוש בניהול הליך הבחירות שעל בסיסו גיבשו את איום הייחוס ומעטפת ההגנה שתיושם על כל מערכת במהלך הבחירות. נמצא כי ביום הבחירות השתמשה יחידת המפקח במערכות מידע נוספות שלא נכללו במסמך מיפוי המערכות ולא נכללו בניתוח האיומים והסיכונים. נוכח זאת, לא נבחנה ולא הוגדרה מעטפת הגנה מתאימה למערכות אלה, המערכות לא נבדקו מבחינת היבטי אבטחת מידע והגנת הסייבר לצורכי הבחירות, והן לא נוטרו בזמן אמת כדי לזהות אירועי סייבר. בנוסף עלה בביקורת כי אף שמערך הסייבר ליווה את משרד הפנים בהיבטי הגנת

מדריך יישומי להגנת הסייבר של הארגון אשר גובש על ידי מערך הסייבר הלאומי.

הסייבר, הוא לא ידע כי נעשה שימוש במערכות אלה ביום הבחירות ועל כן לא נתן את הנחיותיו המקצועיות בעניינן.

מומלץ כי במערכות בחירות עתידיות יחידת המפקח תקפיד למפות מבעוד מועד את כלל המערכות שמשמשות את תהליך הבחירות, ובכלל זה את התהליך העסקי והמידע שמנוהל בכל מערכת, את משתמשי המערכת, את הממשקים שלה ואת סיווגה. עוד מומלץ כי יחידת המפקח תשתף במידע זה את הגורמים השותפים לבחינת היבטי אבטחת המידע של המערכות ובכלל זה את אגף טד"ס, אגף ביטחון חירום וסייבר ומערך הסייבר, כדי לאפשר להם לגבש עבור מערכות אלו מעטפת הגנה ייעודית ההולמת את הסיכון הנשקף להן ולבצע בדיקות כדי לוודא שהמערכות עומדות ברמת הגנה זו.

ניטור המערכות המשמשות את הבחירות

לפי תורת ההגנה השלב השני בהתמודדות עם אירועי סייבר הוא הגדרת אירועים חריגים בהתבסס על איומי הייחוס. אירועים אלו יתועדו וינוטרו במערכות המידע השונות, בין היתר באמצעות יצירת לוגים (Logs) לתיעוד פעולות חריגות ואירועים (Events). מידע זה יועבר למערכת SIEM (Security Information and Event Management) וינוהל במערך שליטה ובקרה מרכזי (מערך ה-SOC, Security operations center).

מערך ה-SOC אחראי להגדרה של חוקות שמזהות אירועים חריגים וקורלציה בין אירועים, והוא אף אחראי לניתוח האירועים ולניהולם בעת אירוע סייבר לצורך סיכול התקיפה או לצורך סיום התקיפה ותהליך ההתאוששות. תורת ההגנה בסייבר מכווניה את כלל הגופים במשק כיצד כדאי להקים את מערך ה-SOC.

כאמור, יחידת המפקח משתמשת במערכות מחשוב התומכות בתהליך הבחירות שמבוססות על תשתיות שונות ועל מערכי שליטה ובקרה (SOC) נפרדים - תשתית של משרד הפנים, תשתית של מערך הדיגיטל ותשתית של רשות האוכלוסין.

כשבוועיים לפני מועד הבחירות שלח משרד מבקר המדינה למשרד הפנים מסמך ובו פירוט של הפערים המסתמנים והמלצות לתיקונם בטווח הקצר. כמו כן, הומלץ להגדיר dashboard שיוצג ב-SOC המרכזי ויכלול מידע מכלל המערכות הפועלות ביום הבחירות, או לחלופין להציג, זה לצד זה, כמה מסכים, שבכל אחד מהם מוצג מידע מ-SOC ספציפי.

בתצפית שערך משרד מבקר המדינה ביום הבחירות ובלייל הבחירות נצפה כדלקמן: ביום הבחירות ובלייל הבחירות משרד הפנים הפעיל מרכז שליטה (חדר סייבר) שכלל נציגים משני מערכי ה-SOC הקיימים שצפו בנתוני כל מערכת בנפרד וכן עלו ליקויים נוספים במערכות מסוימות.

נמצא כי משרד הפנים לא הפעיל ביום הבחירות SOC מרכזי שמתכלל את ממצאי הניטור בכל רכיבי המערכות התומכות ביום הבחירות, ולכן לא היה גורם מתכלל שעמדה לרשותו תמונת המצב השלמה ויכל, בין היתר באמצעים ממוחשבים, לזהות קשרים בין אירועים חריגים המתרחשים במערכות השונות המשמשות את הבחירות. יחידת המפקח הפעילה ביום הבחירות פתרון חלקי באמצעות הקמה של חדר סייבר שנציגי מערכי ה-SOC השונים עבדו בו, כל אחד ניטור את המערכת שלו והם יכלו לשתף ביניהם מידע ככל שמצאו לנכון. כאמור הוא לא כלל את כל המערכות.

לדברי משרד הפנים מדובר במערכות שונות ובסביבות שונות, לכן לא ניתן היה להקים ניטור אחד לכולן.

מומלץ כי לקראת מערכות הבחירות העתידיות משרד הפנים יקים מערך SOC משותף שינטר את כלל המערכות המשמשות את הבחירות וישפר את יכולות הגילוי והזיהוי של התקיפות של הליך הבחירות, בהסתמך על תכלול הנתונים מכלל המערכות.

בתשובת גוף מסוים נמסר כי הוא יפעל לתיקון הליקויים הרלוונטיים אלו.

זיהוי אירועים חריגים

הגדרת איום ייחוס במסמך רשמי ומאושר נועדה, בין היתר, להכווין את הארגון להפנות את משאבי ההגנה שלו על נכסי המידע ביעילות ובהתאם לאיומים. בתורת ההגנה 2.0 צוין כי איום הייחוס של גופים כולל בין השאר התייחסות לאיום פנימי (למשל, עובדים ממורמרים שמשתמשים בהרשאות שלהם לביצוע פעולות לא מורשות). לצורך זיהוי איומים, לרבות איומים פנימיים, הארגון נדרש לתעד פעולות שמבוצעות במערכות באמצעות כתיבת לוגים, להטמיע מערכות לגילוי אירועים חריגים, לזיהויים ולהתערע עליהם ולכתיבת חוקי ניטור בנוגע לאירועים אלו. חוקי הניטור מתייחסים לאיום הייחוס אולם ייתכן שיתבססו גם על מידע נוסף, למשל על מודיעין.

משרד הפנים, ובכלל זה יחידת המפקח האחראית לתהליך העסקי במערכת הבחירות, גיבש עם מערך הסייבר מסמך איומי ייחוס הנוגעים להליך הבחירות. המסמך כולל התייחסות לאיומים שנועדו לערער את תחושת הביטחון והמוגנות במדינה באמצעות פגיעה בתהליך דמוקרטי ליבתי - הבחירות לרשויות המקומיות, וגובש על בסיס מודיעין וכוונות תוקף. במסמך זה לא צוין כי איום הייחוס שגיבש מערך הסייבר היה חסר וכי משרד הפנים נדרש להתייחס להיבטים נוספים.

בהתבסס בין השאר על איומי ייחוס אלה, אגף טד"ם במשרד הפנים הגדיר חוקים לניטור.

נמצא כי הגדרת איומי הייחוס שגיבש משרד הפנים בשיתוף עם מערך הסייבר ושימשה בסיס להיערכות מפני התרחשותם של איומים אלה - הייתה חסרה ולא כללה התייחסות לכלל האיומים שעשויים להסב נזק חמור לתהליך הבחירות. כמו כן נמצאו פערים בניטור.

מומלץ כי בהתאם לתורת ההגנה, משרד הפנים יגבש איום ייחוס הכולל את כל תרחישי הייחוס הנוגעים להליך הבחירות לרשויות המקומיות, וזאת כבסיס להיערכות להתממשות איומים אלה. כמו כן, המשרד יגדיר חוקי ניטור אפליקטיביים ותשתיתיים שייתנו מענה שלם לכלל איומי הייחוס.

טיפול באירועים שחשודים כאירועי סייבר

חלק מהותי בעבודה של מערך ה-SOC הוא טיפול באירועים שחשודים כאירועי סייבר. משמתעורר חשד כאמור, על מערך ה-SOC לפעול בהתאם לתהליכי עבודה מוגדרים (playbooks), שמתווים את אופן טיפולו באירועים החשודים כאירועי סייבר. תהליכי עבודה אלו מנחים את מערך ה-SOC כיצד לפעול מרגע זיהוי התקיפה הפוטנציאלית ועד לטיפול בה ולהתאוששות ממנה במידת הצורך. תהליכים אלו נועדו לעזור למערך לגבש פתרון יעיל לסוגיית התקיפות ולמנוע את המשך התקיפות בתוך פרק הזמן הקצר ביותר.

מערך ה-SOC שהפעיל משרד הפנים פעל בתקופת ההיערכות לבחירות וכן ביום הבחירות. ביום הבחירות מערך ה-SOC נכח במרכז השליטה יחד עם גורמי משרד הפנים, מערך הסייבר וארגונים ביטחוניים, לצורך תכלול תהליך הבחירות. אגף טד"ם הגדיר למערך ה-SOC תהליכי עבודה בעניינם של אירועים חריגים שנוטרו במערכת ה-SOC, שאינם כוללים רשימת פעולות לביצוע בעקבות כל אירוע חריג אלא רק מפורטים בהם אנשי הקשר שיש לדווח להם על אירוע שזוהה. אנשי קשר אלו אינם כוללים גורמים עסקיים (כגון - יחידת המפקח והנהלת משרד הפנים) אלא רק גורמים באגף טד"ם. כמו כן, משרד הפנים לא ביצע תרגול של התנהלות הגורמים הרלוונטיים בהתקיים תרחיש מעין זה. מערכות המידע אינן נגישות למערך ה-SOC, והוא בעל הרשאה לצפייה בלבד ללא הרשאה לבצע פעולות במערכות. מכאן שבהתרחש אירוע חריג יידרש למשרד הפנים זמן רב להבין מה יש לבצע ולטפל בפועל בהסרת האיום ובצמצום היקף הנזק.

בהתרחש אירוע סייבר יפעיל משרד הפנים צוות IR (Incident Response Team) חיצוני (שהיה נוכח ביום הבחירות) לצורך חקירת התקיפה והתאוששות ממנה. צוות IR זה יפעל בשיתוף פעולה עם צוות ה-IR של מערך הסייבר (אם הדבר יתאפשר ובכפוף לדרישות המלחמה).

נמצא כי משרד הפנים לא הגדיר תהליך עבודה וסדר פעולות לביצוע בעת זיהוי אירוע שחשוד כאירוע סייבר (מלבד דיווח של מערך ה-SOC לגורמים באגף טד"ס), לרבות פעולות מנע לביצוע מיידי בעת זיהוי התקיפה. היעדר מתווה פעולה סדור וברור להפעלה מיידי בעת זיהוי התקיפה עלול להוביל להתארכות זמן התקיפה ולהחמרת הפגיעה.

מומלץ כי משרד הפנים יגדיר תהליך עבודה מוגדר וסדר פעולות לביצוע בעת זיהוי אירוע שחשוד כאירוע סייבר, לרבות פעולות מנע לביצוע מיידי בעת זיהוי התקיפה והבאת הנושא לידיעת הגורמים העסקיים.



יוצא אפוא כי משרד הפנים לא נערך כראוי לזיהוי אירועים חריגים שעשויים להעיד על אירוע סייבר ולטיפול בהם: מערך השליטה והבקרה (ה-SOC) שהפעיל לא איפשר לגבש תמונת מצב מלאה בהתבסס על נתוני כלל המערכות; הניטור שיושם היה חסר; ולא הוגדרו פעולות לביצוע בזמן התרחשותו של אירוע סייבר, לרבות פעולות מנע בעת זיהוי תקיפה והבאת הנושא לידיעת הגורמים העסקיים.

מומלץ כי משרד הפנים בשיתוף מערך הסייבר ישפר את יכולות הגילוי והניטור שלו לזיהוי תקיפות בכלל המערכות המשמשות בבחירות לרשויות המקומיות.

הגנה על מידע רגיש

הגנה לוגית

מידע רגיש הוא מידע אשר פגיעה בסודיותו, בשלמותו או בזמינותו עלולה לפגוע בניהולו התקין של הארגון ומשמש יעד לתקיפות סייבר. מידע רגיש נשמר במסדי נתונים של מערכות המידע (למשל, נתונים על בעלי זכות בחירה) או באופן פיזי (למשל, פרוטוקולי הצבעה, אלפונים ופתקי הצבעה). מנגנוני הגנה לוגית הם כלים המאפשרים הגנה על מידע הנשמר דיגיטלית. רובדי ההגנה הלוגית יכולו במערכות ובתשתיות של המחשוב והאחסון את הנדבכים האלו: הזדהות, ניהול הרשאות ובקרת גישה לוגית, הגנה על התקני הקצה וניטורם.

נמצאו ליקויים בהגנה הלוגית (בהגנה על מידע רגיש) בהליך הבחירות לרשויות המקומיות בנושאים שונים ובהם ניהול הרשאות, ניהול סיסמאות, הפרדת סמכויות והגנה על מסדי נתונים.

על משרד הפנים, רשות האוכלוסין ומערך הדיגיטל לפעול לתיקון הליקויים שעלו.

הגנה פיזית

רובד נוסף בהגנה על מידע רגיש ובאבטחת מידע בכלל הוא אבטחת מידע פיזית. רובד זה עוסק בעיקר במניעת גישה פיזית למושא ההגנה (מסמכים, מחשבים, ציוד תקשורת וכו'), למניעת דלף מידע. ממנה הגנת הסייבר בארגון אמון על הגדרת הדרישות ועל אפיון המתחם בהתאם לנתונים ולרשומות שמאוחסנים בו.

בהליך הבחירות לרשויות המקומיות נעשה שימוש בחומרים רגישים בתצורה פיזית (רשומות): חומרי בחירות (פרוטוקולים, אלפונים, קלפי ופתקי הצבעה); חוברות מועמדים (הכוללות פרטים אישיים, חשבון בנק והעתק של תעודת זהות).

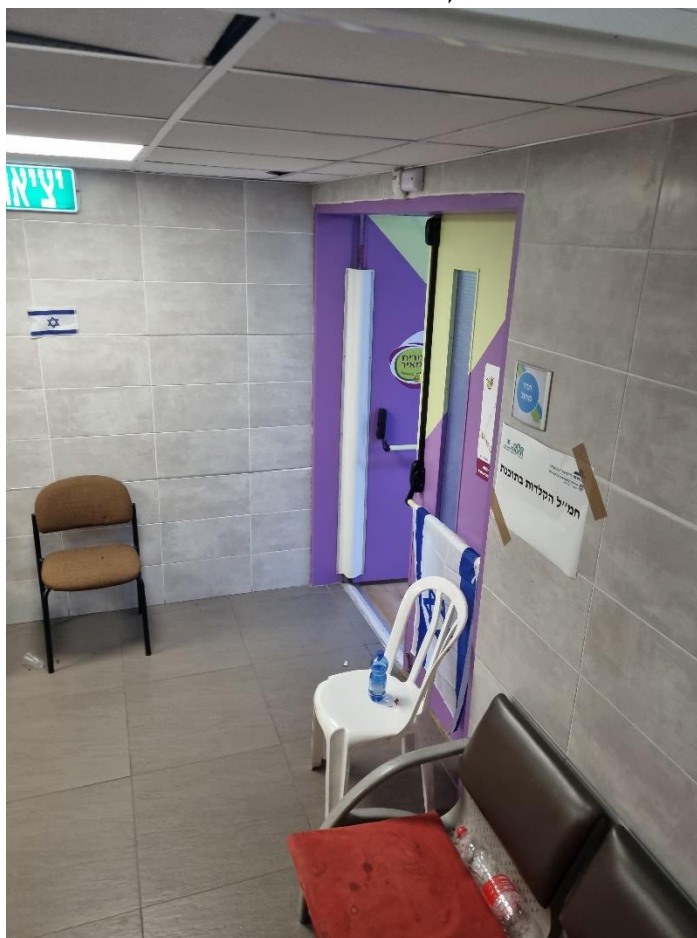
בקרת גישה

על פי הנחיות יה"ב, במסגרת מדיניות הסייבר במשרד הפנים יש ליישם בקרת גישה שנועדה להגן על מכלול הציוד והמידע מפני גישה פיזית של גורמים בלתי מורשים. כמו כן, יש צורך בהגדרת תהליכים ואמצעי טיפול ברשומות כדי להגן עליהן ולמנוע נזקים שעלולים להיגרם מחשיפה למידע בהם.

יחידת המפקח הנחתה את מנהלי הבחירות שביום הבחירות לא ינכחו במתחמי הקליטה של הקלפיות אנשים שאינם בעלי עניין (עובדי היחידה, באי כוחם של המועמדים והסיעות וחברי ועדת הבחירות). כמו כן, הומלץ למנהלי הבחירות לייעד חדר נפרד לקלדנים וחדר נוסף לחומרים הרגישים, כדי למנוע מגורמים חיצוניים גישה לחדרים אלו (למשל כדי למנוע גישה של חברי ועדת הבחירות לחדר הקלדנים).

בתצפית שערך משרד מבקר המדינה ביום הבחירות במתחמי קליטת קלפיות של 13 רשויות מקומיות נמצאו ליקויים בבקרת גישה פיזית אשר אפשרו גישה לגורמים שאינם מורשים למתחמי הקליטה שבהם חומרי בחירות רגישים, שלא בהתאם להנחיות יחידת המפקח ויה"ב. להלן הליקויים: בשלוש (23%) מהרשויות (אריאל, מרחבים וקריית מוצקין) צוותי משרד מבקר המדינה לא נדרשו כלל לעבור בדיקה או זיהוי בכניסה למרכז הקליטה העירוני; בשתיים (15%) מהרשויות (ירכא וכרמיאל) בוצע זיהוי שמי, וללא הצגת תעודה מזהה; בתשע (69%) מהרשויות (אלעד, בני ברק, חיפה, ירכא, כרמיאל, מרחבים, עכו, קריית מוצקין וראש העין) לא נדרש תג ייחודי או אמצעי זיהוי אחר המקנה אישור גישה לאזורים רגישים כמו חדרי ההקלדה, נוכח זאת יש סיכון לכניסה של גורמים לא מורשים לאזורים רגישים.

תמונה 3: כניסה למתחם ההקלדה ללא מאבטח בליל הבחירות בפתח תקווה



צולם על ידי צוותי משרד מבקר המדינה ב-27.2.24, בערך בחצות.

על יחידת המפקח לוודא קיומן של בקורות גישה שנועדו להגן על מכלול הציוד והמידע (מסמכים, מחשבים, ציוד תקשורת וכו') מפני גישה פיזית של גורמים בלתי מורשים בהתאם להנחיות יה"ב.

בתשובת עיריית קריית מוצקין נמסר כי היא תיישם בקרת גישה להגנה על מכלול הציוד והמידע מפני גישה שאינה מורשית. בתשובות עיריות בני ברק, חיפה, כרמיאל וראש העין נמסר כי בעלי התפקידים ענדו תג (אחיד) הכולל פרטים מזהים, וכי הכניסה לאזורים רגישים הותרה למורשים בלבד. כמו כן, בתשובת עיריית פתח תקווה נמסר כי הכניסה למתחם ההקלדה היה מאויש על ידי מאבטח וכן הוצב מאבטח נוסף בסמוך למקום שבו צולמה התמונה.

בהתייחס לתשובת עיריית פתח תקווה, משרד מבקר המדינה מציין כי במועד התצפית שקיים צוות המשרד בליל הבחירות לא נכח מאבטח בכניסה למתחם ההקלדה בפתח תקווה כפי שניתן לראות אף בתמונה, וכי במועד זה לא הייתה בקרת גישה למתחם רגיש זה - לכן יש לוודא שהשמירה במתחמים רגישים תהיה רציפה ותתקיים לאורך כל שעות הפעילות. כמו כן, מומלץ כי יחידת המפקח תנחה את מנהלי הבחירות כי בקרת הגישה למתחמים רגישים תתקיים באמצעות תג ייחודי (למשל בצבע שונה עבור אזור הזנת התוצאות, בדומה לנעשה ברשויות מקומיות אחרות), באופן שיאפשר יישום ובקרה יעילה לעניין הגישה של מורשים בלבד למתחמים אלה.

שמירת חומר רגיש

כאמור, בהתאם להנחיות יה"ב יש ליישם הגנות אבטחה פיזיות ומנגנוני בקרת גישה לרשומות מפני גורמים לא מורשים. נוסף על כך, יחידת המפקח הוציאה למנהלי הבחירות ולמזכירים הנחיות בנוגע לאבטחה הפיזית הנדרשת של חומרי בחירות רגישים (פרוטוקולים ורשימות בוחרים), ובהן ההוראות האלה: אריזת חומרי הבחירות הרגישים בשקיות יעודיות והכנסתם למזוודה לצורך שינועם מהקלפי למרכז הקליטה, תיאום הבאת החומר הרגיש ממרכז הקליטה לאחסון, בליווי משטרה ככל הנדרש; שמירת החומר הרגיש במחסן מיוחד ברשות או במחסן המחוזי, במקום בטוח שאינו נגיש לאיש מלבד מנהל הבחירות או מי מטעמו; הבטחת כל התנאים לאחסון החומר הרגיש.

בליל הבחירות קיימו צוותי משרד מבקר המדינה שיחות עם מנהלי הבחירות של 13 הרשויות שנבדקו בעניין ההנחיות שקיבלו בנוגע לאבטחת החומר הרגיש. אחד מאותם המנהלים מסר כי לא קיבל מיחידת המפקח הנחיות בנושא; ואשר ל-12 המנהלים האחרים: אחד מהם ציין כי קיבל הנחיות רבות בנושא, ויתר 11 (85%) המנהלים (אלעד, אריאל, בני ברק, חיפה, ירושלים, ירכא, כרמיאל, מרחבים, עכו, פתח תקווה וקריית מוצקין) הביאו בתשובותיהם הנחיות שונות, החל מדרישה לחדר נעול בלבד ועד לחדר מצולם ומנוטר.

בפועל, נמצאו ליקויים בהגנה על מידע רגיש במהלך ליל הבחירות כמפורט להלן:

1. **שמירת המידע הרגיש (פרוטוקולים, פתקי הצבעה, אלפונים ועוד) בעת קליטת הקלפיות: בשתיים (18%) מתוך 11 הרשויות שנבדקו (אריאל וקריית מוצקין) המידע הרגיש הושאר בחלל משותף ללא השגחה בזמן שהמזכירים המתינו לתורם.**

2. **שמירת המידע הרגיש לאחר קליטת הקלפיות: בשלוש (23%) מתוך 13 הרשויות (אריאל, בני ברק וירכא) המידע הרגיש נותר בחלל העבודה המשותף, לעומת יתר הרשויות שבהן יושמו מנגנוני הגנה: בשמונה (61%) מהרשויות (אלעד, באר שבע, חיפה, ירושלים, מרחבים, פתח תקווה, קריית מוצקין וראש העין) החומר נשמר בחדר נעול או עם מאבטח, ובשש (46%) מהרשויות (באר שבע, חיפה, ירושלים, עכו, פתח תקווה וקריית מוצקין) היו במרכז הקליטה אמצעי אבטחה מתקדמים (מצלמות או חיישנים).**

3. **סיום הבחירות**: בשמונה (67%) מתוך 12 הרשויות שנבדקו (אלעד, אריאל, בני ברק, כרמיאל, מרחבים, פתח תקווה, קריית מוצקין וראש העין), בסיום יום הבחירות מנהלי הבחירות לקחו או ציינו כי ייקחו את הפרוטוקולים הביתה לפי הנחיית יחידת המפקח. ולגבי כלל החומרים הרגישים - בשש (50%) מהרשויות (באר שבע, חיפה, ירושלים, ירכא, כרמיאל ועכו) החומרים אובטחו במרכז הקליטה או שונעו בליווי משטרה למתחם מאובטח (למשל - בניין עירייה או בניין בית המשפט)²⁷.

תמונה 4: חומרים רגישים שהושארו ללא השגחה בליל הבחירות במרכזי קליטה (מרחבים ופתח תקווה, בהתאמה מימין לשמאל)



צולם על ידי צוותי משרד מבקר המדינה ב-24.2.27.

מכלול הליקויים שפורטו לעיל משקפים פערים משמעותיים בשמירה הפיזית על חומרי בחירות רגישים (שהושארו ללא השגחה), שנשקף בגינם סיכון אשר עלול להגיע לכדי פגיעה בטוהר הבחירות.

מעיריית בני ברק נמסר כי מאחר שלא היה במתחם חדר נעול, החומרים הרגישים רוכזו בפינה צדדית שנתחמה במחיצות גבוהות לצד מאבטח. כמו כן, מעיריית קריית מוצקין נמסר כי היא תיישם נוהלי שמירת חומרים רגישים בעת קליטת הקלפיות, במרכז הקליטה ובסיום יום הבחירות.

נדרשת הקפדה יתרה על שמירתם של חומרים רגישים. מוצע כי יחידת המפקח תחדד אל מול הגורמים הרלוונטיים את ההנחיות בדבר השינוע, האחסון והשמירה של חומרי הבחירות הרגישים (למשל: מקום האחסון, סוג המבנה שבו הם מאוחסנים, אמצעי האבטחה הנדרשים ואישור חריגים במידת הצורך), ותפקח על יישומן. כמו כן, מוצע כי היחידה תנחה כי חומרי הבחירות הרגישים ישונעו באריזה נעולה.

הנחיה של עובדים העוסקים במידע רגיש

איום פנימי (insider threat) מוגדר כסיכון לאבטחת המערכות או המידע שמקורו בארגון. בדרך כלל סיכון זה עלול להתממש בידי עובד הארגון, ספק שירות, קבלן או שותף עסקי המועסק כעת או הועסק בעבר ומנצל לרעה גישה מורשית לרשת הארגון, למערכותיו או למידע שיש בהם כדי לפגוע בסודיות, בשלמות או בזמינות של המידע של הארגון או של מערכות המידע שלו.

על פי הנחיות יה"ב, הארגון נדרש לקיים הדרכות לעובדים בנושא אופן השימוש במערכות המידע ובפרט הנחיות בדבר אבטחת מידע במרחב העבודה.

יחידת המפקח מגייסת קלדנים ככוח אדם זמני ומעניקה להם גישה למערכות ולמידע רגיש. משרד הפנים אחראי להדרכות אבטחת מידע לקלדנים המשתמשים במערכתיו, ובמסגרת זו קלדנים

לא התקבל מידע על אופן סיום הבחירות בבאר שבע.

נדרשו לחתום על "תצהיר אבטחת מידע" שכלל הנחיה בדבר איסור לחיבור רכיבי זיכרון ואמצעי קצה (טלפונים ניידים, מצלמות וכו') וכן בדבר איסור לאפשר גישה למחשב לגורם אחר.

נמצא כי ההנחיות בתצהיר שעליו חתמו הקלדנים בנוגע לאבטחת מידע הן חלקיות ואינן כוללות למשל הוראה מפורשת הנוגעת לצורך בנעילת העמדה בכל עת שאינה מאוישת. כמו כן, בביקור של נציגי משרד המבקר בתהליך הזנת המועמדים נמצא בבדיקה מדגמית שערך הצוות כי הקלדנים לא היו מודעים להנחיות אבטחת מידע בדבר התנהלותם במרחב העבודה.

צוותי משרד מבקר המדינה מצאו ברשויות את הפערים האלה בליל הבחירות:

1. בחמש (62%) מתוך 8 הרשויות הנבדקות (אריאל, חיפה, ירכא, פתח תקווה וראש העין) קלדנים או מזכירים לא עברו הדרכות אבטחת מידע.

בתשובות עיריות חיפה ופתח תקווה נמסר כי הדרכות בנושא אבטחת מידע התקיימו בקרב הקלדנים שעבדו במערכת ששימשה את העירייה.

2. בשש (55%) מתוך 11 הרשויות הנבדקות נצפו על ידי צוותי משרד מבקר המדינה מחשבים של קלדנים או מנהלי בחירות שנותרו פתוחים וללא השגחה (מנהלי בחירות: אריאל וראש העין; קלדנים: אלעד, אריאל, בני ברק, ירכא, פתח תקווה וראש העין).

תמונה 5: עמדת מחשב לא מאוישת ו"פתוחה" - בני ברק, ליל הבחירות



צולם על ידי צוותי משרד מבקר המדינה ב-27.2.24, מעט לפני השעה 20:00.

על יחידת המפקח לקיים הדרכות לעובדים הזמניים לקבל גישה למערכות מידע ולחומרים רגישים, כנדרש בהנחיות יה"ב לגבי אופן השימוש במערכות המידע, וכן על יחידת המפקח לתת לעובדים אלה הנחיות בדבר אבטחת מידע במרחב העבודה ולבצע בקרה על יישום הנחיותיה.

בתשובת משרד הפנים נמסר כי יחודדו נוהלי אבטחת המידע במסגרת ההדרכות לקלדנים ולמזכירים, וזאת מעבר לחוזרים שמועברים למנהלי הבחירות.

מערכת ג'

עמדות משתמש

על פי הנחיות יה"ב, יש צורך בשכבת הגנה פיזית לשם הגנה על מכלול הציוד והמידע מפני גישה של גורמים לא מאושרים.

היבטי הגנה פיזית: בניגוד להנחיות יה"ב בנושא בקרות הגישה, בכניסה למרכז ההקלדה הוצב שומר שזיהה את עובדי מיקור החוץ ברמה השמית בלבד, בלא שהם נדרשו להציג לו תעודה מזהה (למשל, תעודת זהות), מדובר ביותר מ-1,000 עובדים זמניים. זיהוי באופן זה כרוך בסיכון לכניסת גורמים לא מורשים למתחם, אף שיש בו מערכות המכילות מידע רגיש ובכלל זה מידע אישי על מועמדים. כמו כן, יחידת המפקח לא יישמה בקרת גישה לחדר הטכנאים במתחם ההקלדה: החדר היה פתוח לכל באי המתקן, ובחדר עצמו הוצג מידע רגיש בפומבי (למשל, סיסמות הרשת האלחוטית הייתה כתובה על לוח מחיק) לצורך עבודת הטכנאים.

כמו כן, אמנם בדלת הכניסה למתחם מסויים הותקן קורא כרטיסים לצורך בקרת גישה אך צוות משרד מבקר המדינה מצא כי בליל הבחירות דלת הכניסה למתחם הייתה פתוחה בחלק מהזמן, שלא לפי דרישות רשות האוכלוסין, כמתועד בתמונה להלן.

תמונה 6: חדר במרכז השליטה בליל הבחירות



צולם על ידי צוותי משרד מבקר המדינה ב-27.2.24.

בתשובת משרד הפנים נמסר כי בשלב שבו צולמה התמונה נכחו אנשי צוות בחדר.

משרד מבקר המדינה מעיר למשרד הפנים כי שכבת ההגנה הפיזית מחייבת בקרת גישה שנועדה למנוע גישה של גורמים לא מורשים למתחמים רגישים וכן לתעד את הנכנסים למתחם. השארת דלת פתוחה לא אפשרה קיום מנגנוני בקרה אלה.

נוסף על כך, אבטחת ארון התקשורת וכבלי התקשורת של העמדות המרוחקות במרכז השליטה לא עמדה בהנחיות אבטחה נדרשות מבחינת המבנה, המקום של הארון והכבלים ובקרת הגישה אליהם. למשל, ניתן היה לגשת ללא קושי לחומרה של ארון התקשורת דרך החלון של החדר,

שהיה פתוח (ולא מאויש לאורך כל היום), וכבלי התקשורת המסווגת הונחו על רצפת האולם בכניסה לחדר והיו חשופים.

תמונה 7: ארון התקשורת וכבלי התקשורת בחדר במרכז השליטה ביום הבחירות



צולם על ידי צוותי משרד מבקר המדינה ב-27.2.24.

רשות האוכלוסין הציבה בליל הבחירות וביום הבחירות עשרות עמדות מרוחקות של מערכת ג' לצורך הסרה של מועמדים ורשימות מהמערכת ולבדיקת שיוך הרשות הרלוונטית למעטפה החיצונית. נמצא כי העמדות האמורות שמאפשרות גישה מרחוק למערכת ג' הוצבו בלא שיושמו בהן הגנות פיזיות (מניעת גישה ובקרת גישה), שלא כנדרש בהנחיות יה"ב ושלא לפי דרישות רשות האוכלוסין. יישום ההגנות על עמדות מרוחקות אלה הכרחי, שכן גישה מרוחקת מגדילה את משטח התקיפה ואת הסיכון לפגיעה במידע רגיש במודול הבחירות ובמערכת ג' בכללותה.

הפער בין הסיכון הנובע מהיעדר הגנות נדרשות לעמדות לבין התועלת שבהצבתן מקבל משנה תוקף בכל הנוגע לעמדות שהוצבו במרכז מיון המעטפות החיצוניות ובמרכז השליטה אשר אמורות לשמש בליל וביום הבחירות: באתרים אלה השימוש בעמדות היה מועט ונבדקו באמצעותן רק 0.2% ו-8% מהמעטפות, בהתאמה.

בתשובת רשות האוכלוסין נמסר כי מנהל אגף האבטחה הפיזית באגף הביטחון ביצע ביקורות מקדימות באתרים המרוחקים וכי הוא מסר הנחיות, בין השאר בעניין יישום בקרת כניסה ונעילת ארון תקשורת. עוד נמסר כי חודד נוהל העבודה בנושא אחריות מימוש הבקורות למניעת גישה לעמדות מערכת ג', ובעתיד אגף אבטחת מידע וסייבר ידאג כי לאחר פריסת עמדות מערכת ג' יתקבל דיווח על מימוש הבקורות, וזאת לצורך בקרה על יישום הנוהל.



מומלץ כי רשות האוכלוסין תקיים הערכת מצב לגבי השימוש במערכת ג' ביום הבחירות ותיתן מענה על הפערים שנמצאו במערכת ג'. מומלץ כי יחידת המפקח תנהל את הסיכון ותבחן אם יש צורך בשימוש בעמדות זמניות מרוחקות של מערכת ג' לנוכח השימוש המועט שהיחידה עשתה במערכת בליל הבחירות ונוכח העובדה שהקמת עמדות זמניות של מערכת רגישה גורמת לחשיפת המערכת לסיכון.

ממשקים

נמצאו ליקויים בנושא ממשקים שבין מערכות מסוימות.

מומלץ כי משרד הפנים ומערך הדיגיטל יפעלו לתיקון הליקויים.

פיתוח מערכות

מערכת ניהול בחירות

על פי הגדרות PMI (Project Management Institute), במסגרת ניהול פרויקט יש לפעול בהתאם לתוכנית עבודה גמישה הכוללת אבני דרך ומתייחסת לכלל היבטי התוצר, וכן יש להוציא גרסאות פעילות (Release) של התוצר לצורך הפחתת סיכונים (Risk) ועמידה ביעדים ובלוח הזמנים.

כאמור בשנת 2019, לקראת מערכת הבחירות בשנת 2023, פרסם משרד הפנים מכרז להקמת מערכת חדשה - מערכת א' - שתנהל את כל תהליכי הבחירות (הפצת פנקס הבוחרים, אישור מועמדים, סיכום תוצאות וכו'). מערכת א' אופיינה, בין השאר, לניהול תהליך סיכום תוצאות ההצבעה ולפרסומן וכן לקיום ממשק עם המערכת החדשה של רשות האוכלוסין לצורך קבלת מידע על קלפיות ועל בעלי זכות בחירה, מערכת ג' של רשות האוכלוסין היתה צריכה להתבטל ולהיות מוחלפת במערכת א'.

בפברואר 2023, כשמונה חודשים לפני מועד הבחירות המקורי, החליט משרד הפנים להפסיק את הפיתוח של מערכת א' נוכח עיכוב בקבלת גרסה של המערכת, שלא איפשר ביצוע בדיקות מערכת בזמן, וקבע שלאחר הבחירות יידון נושא המשך פיתוח המערכת. במאי 2023 החליט המשרד על הקפאת פיתוח המערכת עד לקבלת החלטה בנושא. עלות הפרויקט הסתכמה בשלב זה בסך של 1.8 מיליון ש"ח, מתוך כ-40.9 מיליון ש"ח (עלות ההזמנה שהוקמה עבור הפרויקט, כ-4.5%). בעקבות החלטה זו החלה יחידת המפקח להיערך לניהול מערכת הבחירות הנוכחית (2023) באמצעות מערכת ב' שפותחה עבור הבחירות בשנת 2018 ונעשה בה שימוש בבחירות אלו, וכן באמצעות מערכת ג'. לאורך תקופת הבחירות טופלו בעיות במנגנון ניהול משימות מנהלי הבחירות במערכת ב', למשל בעיה בהעלאת קבצים גדולים. כמה ימים לפני הבחירות ביצעה יחידת המפקח בדיקה מצומצמת של תקינות מערכת ב', שכללה מספר קטן של רשויות.

כשבוע לפני מועד הבחירות לרשויות המקומיות, בפברואר 2024, קיים משרד הפנים חזרה גנרלית חלקית, שכללה בדיקות בנוגע לתהליך דיווח סטטוס ממינהלות הבחירות המחוזיות וכן בדיקות בנוגע לתהליך דיווח וטיפול באירועים חריגים. כמו כן, בוצע תרגול בנושא תהליך הדיווח על שיעורי הצבעה.

בליל הבחירות נפגשו צוותי הביקורת עם 13 מנהלי בחירות, ותשעה מהם (69%)²⁸ דיווחו כי במהלך תקופת ההיערכות לבחירות וביום הבחירות עצמו הם חוו בעיות בעבודתם עם מערכת ב': שלוש (33%) מתוך תשע הרשויות (באר שבע, חיפה ומרחבים) ציינו כי המערכת קורסת בעת העלאת קבצים גדולים; בארבע (44%) מהרשויות (כרמיאל, מרחבים, קריית מוצקין וראש העין) לא נכללו במערכת כל הרשימות המשתתפות בבחירות, ולכן בליל הבחירות בחלק מהרשויות חל עיכוב בהזנת התוצאות; בשתיים (22%) מהרשויות (חיפה ומרחבים) הייתה בעיה בהרשאות הנדרשות לצורך כניסה למערכת, והיא גרמה לעיכוב; ובשלוש (33%) מהרשויות (אלעד, באר שבע וירושלים) הייתה בעיה בזמינות של המערכת והיו תקלות כלליות.

כמו כן, ביום הבחירות נעשה שימוש בכמה מערכות מקבילות למערכת ב':

אלעד, באר שבע, בני ברק, חיפה, ירושלים, כרמיאל, מרחבים, קריית מוצקין וראש העין.

1. **מערכת גיבוי:** כשבוע לפני הבחירות יחידת המפקח הנחתה את מנהלי הבחירות להשתמש ביום הבחירות במערכת גיבוי חדשה למערכת ב' (מערכת יז'). שש (46%) מתוך 13 הרשויות (אריאל, ירכא, כרמיאל, מרחבים, עכו וקריית מוצקין) השתמשו במערכת גיבוי זו, ובשתיים (33%) מתוך שש הרשויות האלו (מרחבים וקריית מוצקין) המידע הוזן תחילה למערכת הגיבוי ולא ישירות למערכת ב'.

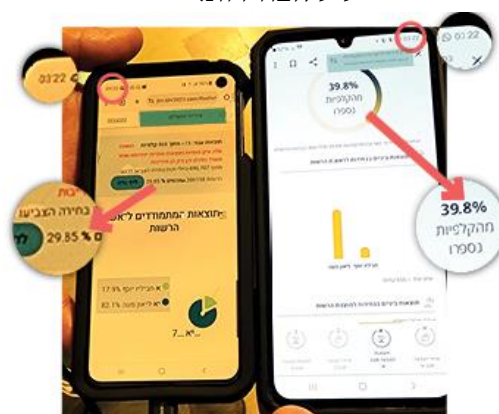
2. **מערכת הרשויות המקומיות:** שבע (54%) (אלעד, באר שבע, בני ברק, חיפה, ירושלים, פתח תקווה וראש העין) מתוך 13 הרשויות שנבדקו בליל הבחירות השתמשו במערכת של הרשויות המקומיות במקום במערכת הגיבוי של יחידת המפקח. צוותי הביקורת העלו כי בפועל בשתיים (33%) (באר שבע וירושלים) מתוך שש הרשויות האלו הזינו את המידע תחילה למערכת של הרשויות המקומיות ולא ישירות למערכת ב'.

מעיריות ירושלים, בני ברק ובאר שבע נמסר כי השימוש במערכת הרשויות המקומיות להזנת תוצאות הבחירות נעשה לצורך גיבוי וכן לצורך ניהול מקומי של תהליך הבחירות, בשל קשיים מהותיים בשימוש במערכת ב': תקלות, בעיית זמינות, אמינות נמוכה, יכולות מוגבלות של המערכת וחוסר מענה על צרכים של ניהול מערכת בחירות ברשות גדולה. עוד נמסר מעיריית באר שבע כי לא מוכרת לה ההנחיה ולפיה תוצאות ההצבעה יוזנו תחילה במערכת ב'.

3. **מערכת ניהול משימות:** ביום הבחירות יחידת המפקח השתמשה במרכז השליטה במערכת ניהול משימות של משרד הפנים, במקום מערכת ב', לצורך ניהול האירועים החריגים, לנוכח העובדה שמערכת ב' לא התאימה לצרכים הנדרשים בנוגע לתיעוד של אירועים חריגים.

במרכז קליטת קלפיות בירושלים, כאמור, הזינו תחילה את תוצאות הבחירות במערכת הרשות המקומית המקבילה למערכת ב' (מערכת יח'). בפועל, הפלט של מערכת יח' שימש מקור להזנת הנתונים במערכת ב'. עקב כך, בליל הבחירות היתה שונות בנתונים בכל אחת מהמערכות בכל רגע נתון. בליל הבחירות היה אפשר לצפות בשיעורי ההצבעה בירושלים באחת מהדרכים האלה: (א) נתוני מערכת ב' בפורטל התוצאות של יחידת המפקח; (ב) נתוני מערכת יח' בפורטל עיריית ירושלים. בפורטל זה צוין כי התוצאות המוצגות אינן תוצאות רשמיות והוסיפו קישור לתוצאות הרשמיות בפורטל התוצאות של יחידת המפקח. בתמונה שלהלן מוצגים נתוני ההצבעה השונים בירושלים שהופיעו בזמן נתון בשתי המערכות בליל הבחירות.

תמונה 8: נתוני הצבעה בפורטל תוצאות הבחירות של יחידת המפקח ובפורטל עיריית ירושלים, ליל הבחירות.



צולם על ידי צוותי משרד מבקר המדינה ב-27.2.24.

נמצא כי יחידת המפקח ואגף טד"ם במשרד הפנים החלו בשנת 2019 בפיתוח מערכת (א') לניהול תהליכי הבחירות שהיו צפויות להתקיים בשנת 2023 - מערכת שעלות ההזמנה שהוקמה עבורה נאמדה בכ-40.9 מיליון ש"ח והייתה אמורה להחליף בבחירות בשנת 2023 את המערכות ששימשו בבחירות הקודמות ולתת מענה על חוסרים ועל קשיים בהן. בפועל, פיתוחה של

המערכת החדשה באמצעות ספק חיצוני לא הושלם נכון למועד הבחירות, ולכן, כשמונה חודשים לפני מועד הבחירות, החליט משרד הפנים בהמלצת אגף טד"ם להפסיק את פיתוחה, לשלם 1.8 מיליון ש"ח (כ-4.5% מכלל עלות ההזמנה שהוקמה לפרויקט) עבור האפיון שבוצע עד לשלב זה ולהשמיש את המערכת הקודמת (מערכת ב').

בביקורת נמצא כי המשרד קיבל החלטה זו בתזמון שלא הותיר שהות מספקת להיערכות הנדרשת לצורך השמשת מערכת ב' באופן תקין. כך למשל המערכת עלתה מבלי שנבדקה באופן מלא, בתקופת ההיערכות לבחירות נמצאו בה תקלות שונות כמו חוסר זמינות וכן חוסר התאמה לצורכי המשתמשים ובלייל הבחירות נמצאו בה או בתפעולה בעיות משמעותיות שלא איפשרו להזין את תוצאות ההצבעה (חוסר בהרשאות של בעלי תפקידים וכן חוסר בהגדרת רשימות מועמדים). נוכח זאת, נעשה שימוש במערכות אחרות (מערכת הגיבוי או מערכת הרשויות המקומיות) והדבר גרם לעיכוב של שעות בהזנת כלל התוצאות ובפרסומן.

עוד נמצא כי 217 (90%) מתוך 242 רשויות לא מפרסמות באתר הרשות את נתוני ההצבעה ברשות שלהם. 25 הרשויות הנותרות פרסמו נתונים באתר הרשות, אך ב-6 (24%) מתוכן היה הבדל של יותר מ-1% בין התוצאות שהן הציגו לבין תוצאות ההצבעה שהיו בפורטל התוצאות של יחידת המפקח שהוא האתר הרשמי. נוכח זאת עולה חשש כי המקור לנתונים הוא לא האתר הרשמי של יחידת המפקח.

מומלץ כי משרד הפנים (יחידת המפקח בשיתוף עם אגף טד"ם) יקדם פיתוח של מערכת מעודכנת לניהול בחירות. עוד מומלץ כי לפני מועד הבחירות יחידת המפקח בשיתוף מנהלי הבחירות יבדקו, במסגרת חזרה גנרלית, את תקינות כלל המערכות לניהול הבחירות, ובכלל זה יגדירו את ההרשאות של כל העובדים וכן את כלל המועמדים ורשימות המועמדים במערכות, כדי לוודא שהמערכות מוכנות ביום הבחירות. זאת, כדי למנוע תקלות בלייל הבחירות ועיכובים בהזנת נתונים ובפרסומם. כמו כן מומלץ כי יחידת המפקח תנחה את מנהלי הבחירות להזין את תוצאות הבחירות תחילה למערכות הרשמיות שלה ולבצע עליהן בדיקות תקינות ורק לאחר מכן במערכות גיבוי וכן תנחה את הרשויות להציג את נתוני ההצבעה מפורטל התוצאות של היחידה ותפתח עבורן ממשק מתאים.

פיתוח מאובטח

לפי הנחיית יח"ב 5.13, במסגרת פיתוח מערכת (קיימת או חדשה) נדרש להטמיע בתוכנה היבטי אבטחה. כמו כן, לפני עלייה לייצור ובכל פעם שמתבצע שינוי מהותי במערכת יש לבצע מבדקי חדירה אקטיביים שניתן ללמוד מהם אם יש פערי אבטחה בגרסה הנוכחית של התוכנה. על מנהל התהליך העסקי לפעול בהתאם לפערים שנמצאו, לפי החלטתו - קבלת הפערים, תיקונים או יצירת בקורות מפצות.

לקראת הבחירות ביצע משרד הפנים סדרת מבדקי חדירה על המערכות: במרץ 2023 על מערכת ב' באמצעות חברות חיצוניות ובמאי 2023 על מערכת ד' באמצעות חברה חיצונית אחרת. לאחר שמערך הסייבר הצטרף כמלווה, הוא ביצע בספטמבר ובאוקטובר 2023 - כשבוע לפני מועד הבחירות המקורי - מבדקי חדירה נוספים על כלל המערכות והיכולות (Features). כפועל יוצא מכך נעשו שינויים ובדיקות המשך רק לאחר מועד הבחירות המקורי ובסמוך למועד הבחירות בפועל (פברואר 2024). משרד הפנים המשיך בביצוע בדיקות המשך עד פברואר 2024. במועד הבחירות הנדחה כבר תוקנו רוב הממצאים (42 מתוך 50), ובהם כל הממצאים ברמת חומרה גבוהה וקריטית.

נמצא כי משרד הפנים ורשות האוכלוסין לא יישמו בחלק ממערכות המידע שפותחו ונרכשו לצורך ניהול הליך הבחירות לרשויות המקומיות היבטי אבטחה הנדרשים בנוהלי פיתוח מאובטח.

עוד נמצא כי משרד הפנים ביצע מבדקי חדירה בסמוך למועד הבחירות המקורי ונדרש לבצע שינויים במערכות בעקבות מציאת פגיעויות (למשל - העלאת קבצים זדוניים) באופן שלא הותיר שהות מספקת ליישום תיקונים מהותיים או לשילוב בקורות מפצות, שנדרשו לצורך פעילותן

התקין של המערכות אילו התקיימו הבחירות במועדן המקורי (31.10.23). בפועל, נוכח דחיית מועד הבחירות התאפשר ביצוע התיקונים לפני מועד הבחירות.

על משרד הפנים להטמיע היבטי אבטחה בהתאם להנחיות יח"ב וכן לבצע מבדקי חדירה במועד שיאפשר הטמעת תיקונים מהותיים, שילוב הבקורות המפצות הנדרשות והקפאת תצורה די זמן לפני מועדי הבחירות.

ניהול מערכות בענן ציבורי

מדינות רבות, ובהן ישראל, התחילו בהעברה של שירותי המגזר הציבורי שלהן לתשתית ענן ציבורי. טכנולוגיית מחשוב המבוססת על ענן ציבורי היא בעלת יתרונות רבים, ועם זאת טמון בחובה גם מגוון סיכונים, ובהם בעלות של גורם זר על המידע (כאשר הארץ שבה נשמר המידע אינה ישראל), תלות בספק ובקווי תקשורת וכפיפות לרגולציה של מדינות זרות. מערך הדיגיטל הלאומי מעודד העברת מערכות מידע במגזר הממשלתי לענן ציבורי, למעט מערכות מידע קריטיות המנהלות מידע מסווג או רגיש, או מערכות שהפגיעה בהן היא בגדר פגיעה במשילות ובסמלי שלטון²⁹. בינואר 2021 פורסם מכרז להקמת ענן ציבורי עבור משרדי ממשלה ויחידות סמך, המחייב הקמת אתר מקומי בשטח מדינת ישראל (נימבוס); ביולי אותה השנה זכו במכרז שני ספקים.

העברה או הקמה של מערכת ממשלתית לענן ציבורי כפופה לבחינתה ולאישורה של ועדת ענן ממשלתית העוסקת בהקמת מערכת ממשלתית בענן ונועדה לבחון האם המערכת עומדת בקריטריונים למעבר לענן, בין השאר, על בסיס המידע והממשקים של המערכת והערכת האיומים עליהם ובהפעלת אמצעים לאבטחת מידע המאוחסן בשירותי הענן בהתאם לסיכונים הנשקפים למערכות המידע בענן.

כאמור, מערכת ב' משמשת לניהול תהליך הבחירות ומכילה מידע רגיש (למשל - מידע על מועמדים, מידע על עובדי הבחירות, ובכלל זה על מזכירי קלפי, ומידע על תוצאות ההצבעה הזמניות). מערכת ב' פותחה בשנת 2018 לקראת הבחירות.

ביולי 2018 ועדת ענן בחנה את העלאת מערכת ב' לענן והמליצה על העלאת המערכת בהתאם ליישום המלצותיה. ייעוד המערכת כפי שהוצג בוועדת הענן כלל קבלת דיווחים ממנהלי הקלפיות ביום הבחירות, מצב הקלפיות ביום הבחירות ועל שיעורי ההצבעה לפי איזור גיאוגרפי. כמו כן צוין כי נתוני ההצבעה הם על בסיס ספירה ידנית של קולות.

בשנת 2021 הוגשה לוועדת ענן בקשה להעלאת מערכת א' (המערכת החדשה שפיתח משרד הפנים והייתה אמורה לשמש את הבחירות בשנת 2023) לענן ציבורי. הוועדה דחתה את הבקשה והגדירה, לנוכח דרישות התהליך העסקי, את הפיתוחים הנדרשים לצורך אישור העלאת עתידית. בפועל הוחלט כאמור שהמערכת שתשמש בבחירות לא תהיה מערכת א' אלא מערכת ב'.

באוגוסט 2023 הוקמה מערכת ב' מחדש על גבי ענן ציבורי בחו"ל. המערכת כללה פיתוחים חדשים במערכת, וזאת ללא אישורה מחדש של ועדת ענן. כמו כן, לא בוצעו במערכת ב' שני פיתוחים שנדרשו ממערכת א' כדי להעלותה לענן וגם לא התקיימה דרישת אבטחת מידע בסיסית של ועדת הענן משנת 2018.

נמצא כי בבחירות שהתקיימו בשנת 2024 משרד הפנים הקים מחדש את מערכת ב', על גבי ענן ציבורי בחו"ל לאחר הוספת פיתוחים חדשים במערכת. זאת, בלי שהיא נבחנה מבחינת היבטי אבטחת מידע והגנת הפרטיות ובלי שקיבלה אישור מחדש של ועדת ענן ממשלתית, שהיא הגורם המקצועי המוסמך למתן אישור זה לנוכח הסיכונים הפוטנציאליים הגלומים בשימוש בפלטפורמת הענן.

²⁹ מבקר המדינה, דוח שנתי 72 א (2021), חלק ראשון, "שימוש משרדי ממשלה בענן ציבורי וההיערכות להקמת ענן מרכזי", עמ' 585 - 640.

עוד נמצא שמערכת ב' - אשר הושמשה לצורך ניהול הבחירות בשנת 2024 כתחליף למערכת א' החדשה - אף היא אינה כוללת בקורות מפצות שנדרשו ממערכת א' כתנאי לעלייתה לענן. על כן, הסיכונים שבעטיים לא ניתן האישור למערכת א' החדשה נותרו בעינם גם בניהול הליך הבחירות בשנת 2024 באמצעות מערכת ב'.

בטרם שימוש במערכות לניהול הבחירות בענן ציבורי או הוספת שינויים מהותיים במערכות אלה, על משרד הפנים לקבל את אישורה של ועדת ענן ממשלתית, הגורם המקצועי המוסמך למתן אישור זה, לנוכח הסיכונים הפוטנציאליים הגלומים בשימוש בפלטפורמת הענן הציבורי בחו"ל כמו משילות המידע, בהיבטי אבטחת מידע והגנת הפרטיות.



מכלל הממצאים עולה כי משרד הפנים יזם כבר בשנת 2019 את הקמתה של מערכת חדשה שתשמש את ניהול הבחירות בשנת 2023 ולא ניהל את הפרויקט בהתאם ללוחות הזמנים ולתכולה הנדרשת.

מומלץ כי משרד הפנים יגבש בהקדם תוכנית עבודה לפיתוח מערכת שתשמש את הבחירות הבאות תוך קביעת אבני דרך ולוחות זמנים שיאפשרו לקבל את כל האישורים לפיתוח המערכת בענן, להטמיע היבטי אבטחה בהתאם להנחיות יה"ב וכן לבצע מבדקי חדירה במועד שיאפשר הטמעת תיקונים מהותיים, שילוב הבקורות המפצות הנדרשות (לרבות בכלי ענן) והקפאת תצורה של המערכת די זמן לפני מועדי הבחירות. כמו כן, מומלץ כי בהתאם למתודולוגיה שלפיה תפותח המערכת יופקו תוצרי ביניים (למשל, ממצאי בקרה על בחירות שהתקיימו באחת הרשויות המקומיות) שיהיה אפשר לבחון אותם ולהשתמש בהם גם קודם לבחירות המקיפות (שיתקיימו ברשויות המקומיות בכל הארץ בעת ובעונה אחת) ובכך לוודא כי המערכת תומכת באופן מלא בכלל תהליכי הבחירות ונותנת מענה על הקשיים והתקלות שהיו במערכות הישנות.

סיכום

הבחירות לרשויות המקומיות הן אבן יסוד מרכזית שעליה מושתתת הדמוקרטיה המקומית, ותוצאות הבחירות משפיעות על היבטים נרחבים בחיי היום-יום של כלל תושבי מדינת ישראל. תנאי ניהולו בהצלחה של פרויקט לאומי זה הוא קיומן של מערכות ממוחשבות תקינות ומאובטחות, אשר תומכות באופן מלא בכל אחד מהשלבים בתהליך הבחירות.

משרד מבקר המדינה ביצע ביקורת בזמן אמת על מערכות המידע והגנת הסייבר בבחירות שהתקיימו בפברואר 2024 וליווה את התהליך החל בשלב ההיערכות לבחירות, עבור דרך יום הבחירות וכלה בימים שלאחריו. בביקורת עלו ליקויים הן בהיערכות התקשובית לבחירות והן בהתנהלות בפועל תוך כדי הבחירות ובכלל זה:

1. חלק ניכר מההליכים המבוצעים בהליך הבחירות מבוצע באופן ידני ולא באופן ממוכן, ובכלל זה הליך זיהוי הבוחר. ההתפתחות הטכנולוגית מאפשרת מעבר לזיהוי דיגיטלי ומובילה לכך בשנים הבאות. מהלך זה מצריך היערכות מוקדמת שתניח את התשתית למימוש היתרונות במעבר כאמור לצד בחינת ייזום שינויי חקיקה ככל הנדרש ומתן מענה על סיכונים פוטנציאליים בהיבטי אבטחת מידע.

2. היעדר גורם אסדרתי מדיני מתכלל בתחום אבטחת המידע והגנת הסייבר אשר מנחה ומלווה את תהליך הבחירות לרשויות המקומיות ומוודא שכלל המערכות והתשתיות שנעשה בהן שימוש בתהליך עומדות ברמת ההגנה הראויה. היעדרו של גורם מדיני מתכלל כאמור בולט במיוחד לנוכח העובדה שמדובר בפרויקט לאומי בעל השפעה רבה על המשק אשר נשען, בין היתר, על תשתיות מחשוביות שהוגדרו כתשתיות מדינה קריטיות, אשר מנוהלות בידי גופים ממשלתיים שונים והפגיעה בהן עלולה לגרום לדלף מידע רגיש על מיליוני אזרחים ולשיבושו של הליך הבחירות.

3. נמצאו פערים בהיבטים של אבטחת מידע והגנת הפרטיות במערכות המידע שהופעלו בתהליך הבחירות. חלק מהפערים שוקפו על ידי צוות הביקורת למשרד הפנים בזמן אמת ועוד לפני הבחירות. חלקם תוקנו במהלך הביקורת, ועל משרד הפנים להמשיך לפעול למתן מענה על הפערים שנותרו.

4. פיתוחה של מערכת חדשה לניהול הבחירות (א') לא הושלם במועד שנקבע לכך. בנסיבות אלה, החליט משרד הפנים להפסיק את פיתוחה, לשלם עבור האפיון שבוצע עד לשלב זה 1.8 מיליון ש"ח (כ-4.5% מכלל עלות ההזמנה שהוגדרה עבור הפרויקט, שהסתכמה בכ-40.9 מיליון ש"ח) ולהשמיש מערכת קודמת (ב'). תזמון קבלת החלטה זו לא הותיר שהות מספקת לבדיקתה לפני תפעולה, ובפועל אף נמצאו בה בעיות משמעותיות בליל הבחירות אשר הובילו בסופו של דבר לעיכוב בהזנת תוצאות הבחירות ובפרסומן.

הפערים שהועלו בביקורת זו משקפים נקודות תורפה משמעותיות בניהול הליך הבחירות לרשויות המקומיות, שמחייבות מתן מענה. יש לתת את הדעת על הצורך שעולה מממצאי הביקורת לליווי והנחיה שוטפים ומחייבים של גורם מדינתי, באופן שתיתן מעטפת הגנה הוליסטית על כלל המערכות והתשתיות המשולבות בפרויקט לאומי חשוב זה.

על מנכ"ל משרד הפנים והמפקח הארצי על הבחירות ברשויות המקומיות, בשיתוף עם הגופים האסדרתיים המדינתיים (מערך הסייבר והרשות להגנת הפרטיות) ויתר הגופים המעורבים בהליך הבחירות (מערך הדיגיטל ורשות האוכלוסין), לנתח לעומק את מכלול הליקויים שהועלו בדוח זה ולפעול לתיקונם בלוח זמנים שיבטיח כי מערכת הבחירות הבאה תנוהל מהבחינה התקשורתית באופן תקין ומשופר. לצורך כך יש להטמיע פעולות תיקון בתכניות העבודה השנתיות של משרד הפנים ושל יחידת המפקח עד לקיום מערכת הבחירות הבאה.

מומלץ כי שר הפנים יחדש את עבודתה של הוועדה לבחינת מחשוב מערכות הבחירות לכנסת ולרשויות המקומיות שהחלה בדצמבר 2013 ועבודתה הופסקה בשנת 2014. לצורך כך מוצע כי יקדם את הפעולות בנושא בהסכמה ובשיתוף של יחידת המפקח וועדת הבחירות המרכזית. במסגרת העבודה יתבצע שיתוף ידע וייבחנו בין היתר התהליכים העיקריים והמערכות המשמשים בכל סוג בחירות והמשותף להם, בשים לב לכך ששני גופים אלו עמלים בעת הזו על החלפת המערכות לניהול הבחירות, וכן תיבחן האפשרות למכן את התהליכים או את חלקם באמצעות מערכות משותפות באופן שייתן ביטוי להיבטי לוחות הזמנים, העלויות, היכולת להפעיל כמה מערכות בחירות בד בבד והיבטי סייבר ושרידות של המערכות. להלן דוגמאות לתהליכים שאפשר למכן, אשר מקצתם יושמו בוועדת הבחירות המרכזית: זיהוי בוחרים באמצעים ביומטריים, מיכון של טופסי הגשת מועמדות (בעניין זה מקודמת הצעת חוק) ופרוטוקולים של מזכירי קלפי, הקמת מערכת ניהול של רשימת מצביעים, ניהול ממוחשב של תהליך לשיבוץ הרכב ועדות הקלפי ושימוש בטכנולוגיות של בינה מלאכותית. מחשוב תהליך הבחירות יאפשר לייעל משאבי זמן וכוח אדם; לנתח ולעבד מאגרי מידע גדולים; לשפר את אבטחת המידע בתהליך הבחירות, ובפרט מידע רגיש, ולהפחית את הצורך בשינועו; לנהל הליכי בקרה; להגביר שקיפות תהליכים והרתעה; להפחית את הסיכון לטעויות אנוש ולפגיעה בטוהר הבחירות.