משרד החינוך

דוח ביקורת מיוחד - הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות

דוח ביקורת מיוחד - הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות

רקע

רוב המידע שמשרד החינוך אוסף, שומר ומנהל בעניין בחינות הבגרות וציוני הבגרות הוא מידע רגיש על תלמידים ועובדים, שכולל יותר מ-100,000 רשומות, ובהיותו כזה אבטחתו נדרשת להיות ברמה הגבוהה ביותר לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (תקנות הגנת הפרטיות אבטחת מידע), ובכלל זה על משרד החינוך מוטלת החובה לשמור על המידע ולוודא שהוא משמש אך ורק למטרות שלשמן הוא נמסר או לצורכי מילוי חובותיו של המשרד על פי החוק. על המשרד לוודא כי המידע והנתונים לא ישונו או יימחקו, וכי הם ייחשפו רק לפני גורמים המורשים לקבל גישה אליהם, מתוקף תפקידם או מתוקף כך שהמידע נוגע להם, כגון התלמידים או הוריהם, או למוסדות השכלה גבוהה ולגורמים אחרים אשר תעודת הבגרות וציוני התלמידים נדרשים להם.

היבט נוסף המחייב נקיטה של אמצעים כדי למנוע פגיעה במאגרי מידע הוא תקיפות סייבר, ששכיחותן הולכת וגדלה והן גורמות לנזקים ניכרים ורחבי היקף. המניעים לכך שונים, ובהם כוונה לפגוע במערכות עצמן וכך לשבש את הפעילות התקינה והשוטפת של הארגון, החברה ואף המדינה, למטרת סחיטה, למטרת שינוי מידע כדי ליהנות מהטבות ומרווחים ואף במסגרת אתגר טכנולוגי לשמו.

נתוני מפתח

כ-1.39 מיליון
מחברות בחינה של תלמידים שנבחנו בבגרות הוערכו על ידי משרד החינוך בשנת הלימודים התשפ"א (ספטמבר 2020 - אוקטובר 2021)

כ-125,000
תלמידי כיתות י"ב נבחנו בבחינות הבגרות ב-1,299 בתי ספר בשנת הלימודים התשפ"א

כ-12,000
מחברות בחינה נמצאו חשודות כחריגות בשנת הלימודים התשפ"א

832
גרסאות שאלונים גובשו במשרד החינוך עבור 62 מקצועות לימוד בשנת הלימודים התשפ"א

כ-2,200
אירועי סייבר טופלו על ידי מערך הסייבר הלאומי בשנת 2021

33%
הגידול בשיעור אירועי הסייבר שבהם טיפל מערך הסייבר הלאומי בשנת 2021 לעומת השנה הקודמת

כ-467.6 מיליון ש"ח
תקציב אגף הבחינות במשרד החינוך בשנת 2021

כ-5% במקום 8%
שיעור תקציב הגנת הסייבר שהקצה משרד החינוך מתוך תקציב טכנולוגיות המידע בשנת 2020 (5%) לעומת החלטת הממשלה 2443 בעניין הגנת הסייבר המורה על 8%

פעולות הביקורת

בחודשים פברואר 2021 - מאי 2022 בדק משרד מבקר המדינה היבטים באבטחת המידע במשרד החינוך ואת אבטחת המידע של מערכות המידע המרכזיות שתומכות בניהול ובתפעול של ציוני בחינות הבגרות ובסביבות התקשוב שבהן הן פועלות. הבדיקה בוצעה במטה המשרד, באגף הבחינות ובמינהל טכנולוגיות מידע דיגיטליות, במרכז לבדיקת בחינות הבגרות והגמר (מערך המרב"ד) שמתפעלת חברה חיצונית. בדיקת השלמה בוצעה ביחידה להגנת הסייבר בממשלה (יה"ב) ובמשטרת ישראל.

הדוח שבנדון הומצא לראש הממשלה ביום 6.12.22.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על

אבטחת המידע הביטחוני ובתאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו.

תמונת המצב העולה מן הביקורת

- **ביצוע סקר סיכונים ומבדקי חדירה ויישום תוכנית העבודה השנתית** - נכון לאוקטובר 2021, יותר משלוש שנים לאחר שביצע משרד החינוך סקר סיכונים מקיף של מערכות ליבה נבחרות שלו ומבדק חדירה בנוגע למערכת א', משרד החינוך לא ביצע סקר סיכונים מקיף ומבדקי חדירות בנוגע למערכות הליבה שלו בתדירות הנדרשת בתקנות הגנת הפרטיות אבטחת מידע - אחת ל-18 חודשים. מתוך שבע המשימות שהוגדרו ברמת סיכון "קריטית" או "גבוהה" בתוכנית העבודה לשנת 2019 של המשרד ושהמשרד קבע שיש ליישמן בשנת 2019, נכון לאוקטובר 2021, המשרד השלים את הטיפול בשלוש משימות, ובארבע המשימות הנותרות הוא טיפל חלקית.

- **מוכנות משרד החינוך להתאוששות מאסון** - משרד החינוך לא ביצע תרגילים מסוימים לשחזור מידע ולהתאוששות מאסון כנדרש בהנחיית יה"ב "גיבוי ושחזור מידע"; הוא גם לא ביצע תרגיל לשחזור מלא של מערכת מחשב מסוימת שלו.

- **עמידת משרד החינוך בחובות הנקבעות לפי תקנות הגנת הפרטיות אבטחת מידע** - עלה כי שלוש שנים לאחר כניסת תקנות הגנת הפרטיות אבטחת מידע לתוקף (במאי 2018) משרד החינוך גיבש את מסמכי מבנה המאגר, את הגדרות המאגר ואת רשימת המצאי רק עבור חמישה (10%) מ-50 מאגרי המידע שרשומים בפנקס רשם מאגרי מידע. במסמך הגדרות המאגר "תלמידים" לא עודכן מיהו הממונה על אבטחת המידע, ורשימת המצאי אינה מלאה.

- **מינוי של ממונה הגנת סייבר, כינוס ועדת היגוי סייבר והקצאת תקציב להגנת הסייבר** - מסוף שנת 2020 ועד לאוקטובר 2021 משרד החינוך לא אייש את תפקיד ממונה הגנת סייבר. ועדת היגוי סייבר לא התכנסה בתדירות הנדרשת - לכל הפחות פעם בחציון. המשרד גם לא עמד בהנחיה ולפיה יש להקצות לכל הפחות 8% מתקציב תחום טכנולוגיית המידע עבור הגנת הסייבר. בפועל שיעור התקציב הייעודי שהוקצה לכך בשנת 2019 היה כ-5.66%, ובשנת 2020 הוא פחת לכ-5.06%. יצוין כי משרד החינוך מסר בתגובתו כי בחודש יוני 2022 מונתה ממונה הגנת סייבר וכי במהלך שנת 2022 (לאחר סיום הביקורת) הוא כינס פעמיים את ועדות ההיגוי לאבטחת מידע וסייבר.

- **אבטחת המידע ברשת א'** - רשת א' משרתת את כל המשתמשים שאינם עובדי משרד החינוך, ובהם בתי הספר, עובדי ההוראה, התלמידים, ההורים והספקים, והיא נגישה גם

לעובדי המשרד על פי צורכיהם. חברה א' מספקת למשרד את שירותי התשתיות המרכזיות של הרשת. להלן יפורטו עיקרי הממצאים שעלו בנוגע לרשת א':

- עלה שרכיב מסוים וגם ציוד הרשת ואבטחת המידע, הנמצא על פי חוזה ההתקשרות בטיפולה של חברה א', אינו נגיש באופן ישיר למשרד. המשרד גם אינו מבקש לקבל מהחברה דוח עיתי המפרט את ההגדרות והכללים שנקבעו לשאר ציוד הרשת ואבטחת המידע שבשליטתה, אף שהדבר נדרש כדי לוודא שההגדרות והכללים בנוגע לאבטחת המידע עומדים בדרישות המתחייבות מחוזה ההתקשרות, מצרכיו של משרד החינוך ומהנחיות יה"ב שחלות עליו.
- משרד החינוך לא ביקש אסמכתאות המתעדות את אופן הטיפול של חברה א' בקריאותיו; הוא גם אינו דורש ממנה לשלוח לו קובץ של רשומות תיעוד הפעולות (קובץ ה-log) שיאפשר לו לבצע בקרה על רשומות המתעדות את הפעולות שבוצעו במערכות.
- מערכת ה', שאמורה לאפשר ניטור של שינויים בכללי רכיבי הגנה מסוימים ובקרה עליהם, לא הוטמעה על רכיבים שבשליטת חברה א'.
- המשרד לא חיבר את רשת א' ל-SOC הממשלתי[1].

אבטחת המידע ברשת ג' - ברשת ג' מנוהל התהליך הנוגע לבדיקתן ולהערכתן של מחברות הבחינה ששימשו את הנבחנים למענה על שאלוני הבחינה. בנוגע לרשת ג' העלתה הביקורת כלהלן:

- הרשת מוגנת על ידי גרסה מיושנת של מערכת הגנה מסוימת, שבספטמבר 2019 היצרן הפסיק לתמוך בה. נכון לנובמבר 2021 מערכת הגנה מסוימת עדכנית עדיין לא הוטמעה באופן מלא ברשת ג'.
- ברשת זו עלו פערים בנוגע לרכיבים מסוימים לאבטחת מידע.
- בינואר 2020 היצרן הפסיק לתמוך במערכת ההפעלה של שרתים מסוג מסוים שמשמשים, בין היתר, את רשת ג'.
- לרשת ג' אין רכיב שמבצע פעולת בקרה מסוימת ברמת התשתית כפי שהומלץ בהנחיות.
- שרת א' ושרתי ב' של רשת ג' אינם מופרדים; הדבר מקנה לעובדים מסוימים גישה לשרתי ב' אף שלא אמורה להיות להם גישה כזאת. בשרת א' נשמר עותק של מסד נתונים (DB) מסוים, והוא מונגש למשתמשים מורשים שניתנה להם גישה לשרת זה. יוצא כי לאותם משתמשים יש גישה גם למאגר נתונים מסוים אף שאינם מורשים לכך.

אבטחת המידע במערכת ד' - למערכת ד' נטענים קובצי מחברות הבחינה הסרוקות וקובצי מחברות הבחינה המתוקשבות. הגישה למערכת מוקנית, באמצעות המרשתת, לכ-4,000 מעריכים חיצוניים אשר בודקים את מחברות הבחינות ומזינים עבורן ציונים. בנוגע למערכת זו העלתה הביקורת כלהלן:

- עלה כי המעריכים מתחברים למערכת באמצעות מחשבים אישיים שאינם מנוהלים

1 מרכז השליטה והבקרה הממשלתי למול איומי סייבר - Security Operation Center (להלן - ה-SOC הממשלתי).

או מוקשחים על ידי משרד החינוך וכי החיבור שלהם מאובטח חלקית.

- הפעולות הנעשות במערכת ד' נרשמות ומתועדות בקובצי ה-log, אך הן אינן מבוקרות ואינן מנוטרות.
- שישה משמונה משתמשים שתפקידם הוגדר במערכת ד' בהגדרה מסוימת, קיבלו הרשאות החורגות מתפקידם שלא על פי עקרון "הצורך לדעת"[2]; לעיתים אין זיהוי חד-ערכי של משתמשים או פירוט של הפעילות שבוצעה.
- קבצים מועברים בין מערכת ד' לבין משרד החינוך (או ספקים אחרים שלו) בלא שנבדק אם יש בהם סיכון מסוים לפגיעה אף שהתקנות מחייבות ביצוע פעולה מסוימת בעת העברת מידע ברשת הציבורית או במרשתת, יש קבצים שיש בהם מידע רגיש שמועברים ממערכת ד' למשרד בממשקים לא מאובטחים דיים, והדבר מגביר את הסיכון לדלף מידע רגיש ולפגיעה.
- במסגרת בדיקה מיוחדת שביצע משרד מבקר המדינה במערכת ד' עלה שההתקנה של צד המשתמש (לקוח - Client) וצד השרת (Server) ושבדיקת ההרשאות אינן כנדרש בהנחיות יה"ב.

אבטחת המידע במערכת ב' - מערכת ב' משמשת לרישום התלמידים הניגשים לבחינות הבגרות, כ-250 מבתי הספר מזינים באמצעותה גם את הציונים השנתיים הבית-ספריים של התלמידים (ציוני המגן). בנוגע למערכת זו עלה כלהלן:

- 64% מהמשתמשים לא נכנסו למערכת במשך קרוב לחמש שנים - בין מרץ 2017 לינואר 2022; 19% מהמשתמשים נכנסו למערכת לכל המאוחר לפני כשלוש השנים עד חמש שנים (בשנים 2017 - 2019), ורק 12% מהמשתמשים נכנסו למערכת בשנה האחרונה - ינואר 2021 עד ינואר 2022. הדבר מעורר חשש למתן הרשאות גישה למערכת לגורמים שאין להם צורך בכך.
- נכון לספטמבר 2021 משרד החינוך לא סרק במערכת הלבנה קבצים לפני העברתם לסביבה ב'. נכון לנובמבר 2021 גם החברה החיצונית לא סרקה את אותם קבצים לפני שייבאה אותם לסביבה א' או לפני שקלטה אותם במערכת ד'.

מערכת ז' שברשת ב' של משרד החינוך - משרד החינוך לא הסדיר נוהל המגדיר את שלבי תהליך עדכון ציוני הבגרות במערכת ז', את הגורמים המעורבים בו, את האחראים לכל שלב ואת הבקרה על התהליך. בפועל, עלו פערים במנגנוני הניטור והבקרה של משרד החינוך. המשרד גם לא מבצע בקרה בדיעבד - הוא לא הסדיר תהליך לקבלת דוח תקופתי קבוע המציג את הפעולות שבוצעו במערכת והמאתר פעולות החשודות כחריגות. המערכת גם לא מאפשרת בקרה פנימית בהיבט מסוים.

הפצה לא מורשית של בחינות הבגרות - בביקורת נמצאו שבע קבוצות ביישומונים להעברת מסרים מיידים הפעילות במגזר היהודי ובמגזר הערבי, שבהן התבצעה פעילות הפצה לא מורשית של שאלונים ושל הפתרונות לשאלונים. בשנים 2018 - 2020 הגיש משרד החינוך ארבע תלונות בלבד במשטרת ישראל בגין עבירת "קבלת דבר במרמה"

2 "עיקרון הצורך לדעת" - מצמצם במידת האפשר את הגורמים המורשים להיחשף לנכסי המידע הרגישים במיוחד ומקנה שקיפות בתוך המשרד בנוגע לנכסי מידע בסיווג נמוך יותר

בעקבות הפצה לא מורשית של שאלונים או של תשובות של בחינות הבגרות. ובעניין זה יצוין כי בשנת 2020 פסל המשרד יותר מ- 16,000 מחברות בחינה בשל חשד לפגיעה בטוהר הבחינות.

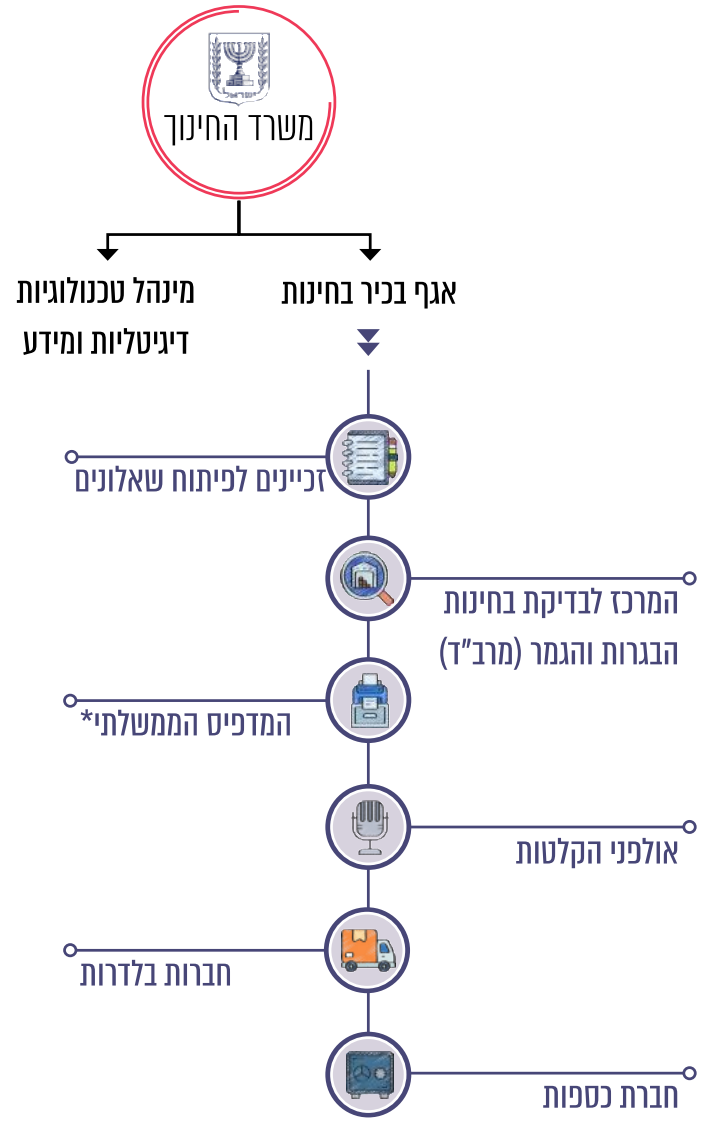
שינוי מודל של הפצת הבחינות - בשנת 2015 הקים המשרד צוות משרדי לבחינת נושא ההיערכות לבחינות הבגרות, ובשנת 2018 ביצע מיפוי וניתוח של תהליכים וסיכונים באגף הבחינות באמצעות חברה חיצונית שעמה התקשר. בעקבות כך המשרד שינה את מודל הפצת בחינות הבגרות, ובין היתר הוא רכש והתקין מאות כספות ברזל בבתי הספר שמאפשרות לו לשלוט מרחוק על שעת פתיחתן, ובהן הוא שומר את שאלוני בחינות הבגרות.

עיקרי המלצות הביקורת

- מומלץ שמשרד החינוך יקפיד על כינוס ועדת היגוי סייבר פעמיים בשנה; יישם את תוכנית העבודה השנתית במועד; יבצע סקרי סיכונים ומבדקי חדירה אחת ל-18 חודשים; יקצה לכל הפחות 8% מתקציב טכנולוגיות המידע לקידום נושא הגנת הסייבר בהתאם להחלטת הממשלה 2443 ולהנחיית יה"ב.
- מומלץ שמשרד החינוך ידרוש אסמכתאות המתעדות את טיפול חברה א' בקריאותיו, וכן מומלץ שיקבל דוחות ניטור ובקרה, דוחות של כללי רכיב הגנה מסוים והגדרות בדבר הציוד שבאחריות חברה א'. עוד מומלץ כי משרד החינוך ישקול להטמיע אמצעים שיאפשרו בקרה מסוימת לגבי אבטחת הרכיבים שנמצאים בשליטת חברה א', וכי הוא יחבר את רשת א' ל-SOC הממשלתי.
- מומלץ כי משרד החינוך יקדם את סיום ההטמעה של הגרסה המעודכנת של רכיב הגנה מסוים ברשת ג', וכי יפעל לשדרוג מערכות ההפעלה של שרתי רשת ג' שהיצרן אינו תומך בהם עוד. מומלץ שמשרד החינוך ידרוש מחברות המפעילות עבורו את מערך המרב"ד להטמיע את מערכות אבטחת המידע החסרות. עוד מומלץ שהמשרד יפעל להקמת יכולת של תיעוד ובקרה מסוימת של רשת א' ויגדיר התרעות שיאפשרו לאתר סיכוני פגיעה של הרשת.
- מומלץ שמשרד החינוך יבצע תרגילי שחזור גיבויים תקופתיים ותרגילי התאוששות מאסון. כמו כן מומלץ שיפעל לביצוע הפרדה בין שרת א' לשרתי ב' של מערכת ד'. בהיבטים מסוימים. מומלץ גם שבשרת א' לא ייעשה שימוש במסד נתונים מסוים.
- מומלץ כי המשרד יבחן מחדש את מודל החיבור של המעריכים למערכת ד' ממחשבים אישיים באמצעות חיבור מאובטח חלקית. עוד מומלץ כי המשרד יבטיח כי חברות המפעילות עבורו את מערך המרב"ד יקפידו לפעול על פי עקרון "הצורך לדעת" ולצמצם את הגישה למידע בהתאם לפרטי מידע הדרושים למשתמש לצורך ביצוע עבודתו בלבד. כמו כן, מומלץ כי המשרד יפעל לשיפור יכולות הניטור והבקרה במערכת ד'.

- מומלץ שמשרד החינוך ישלים את ההטמעה של מערכת הלבנה ברשת א' וברשת ג'. בכל הנוגע להעברת מידע רגיש בין מערכותיו לבין מערכות חיצוניות - על משרד החינוך לשפר את יכולות ההגנה מפני סיכונים המסוגלים לגרום נזק או שיבוש למערכותיו ולמידע שבהן. בהתאם לתקנות הגנת הפרטיות אבטחת מידע.
- מומלץ שמשרד החינוך יבחן את רשימת מורשי הגישה למערכת ב' ואת ההרשאות שניתנו להם. מומלץ גם שהמשרד יבצע בתדירות קבועה בקרת הרשאות בקרב משתמשי מערכת ב', בדגש על שינויים שנעשו במערך ההרשאות, ובכלל זה ישקול הטמעה של מנגנון אוטומטי לביטול הרשאות כניסה למערכת של משתמש שלא נכנס אליה במשך תקופה שתוגדר.
- מומלץ שמשרד החינוך ומשטרת ישראל יבחנו כלים להתמודדות עם תופעת ההפצה הלא מורשית של בחינות הבגרות והפצת פתרונות להן לפני שהן הסתיימו, למשל באמצעות ביצוע מעקב ובדיקות יזומות בפלטפורמות השונות שבהן מתבצעת הפצה של שאלונים ופתרונות ובכלל זה ברשתות חברתיות וביישומונים למסרים מיידיים.

הגורמים העיקריים המעורבים בתהליך הניהול והתפעול של בחינות הבגרות



בסגול-גורמים חיצוניים

על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

* המדפיס הממשלתי הוא יחידת סמך במשרד האוצר. תפקידו העיקרי - ביצוע והפקה של עבודות הדפוס עבור משרדי הממשלה ויחידות הסמך באמצעות ייצור עצמי או באמצעות התקשרויות עם קבלני משנה חיצוניים.

סיכום

משרד החינוך אוסף, שומר ומנהל מידע רב הנוגע לבחינות הבגרות. מדובר במידע רגיש, שאבטחתו נדרשת להיות ברמה הגבוהה ביותר. בביקורת עלו כמה ליקויים בתחום אבטחת המידע - הן מתחום קיום ממשל אבטחת מידע תקין במשרד החינוך ובגופים חיצוניים שמבצעים עבורו חלק מהפעילות במיקור חוץ, והן מהתחומים הטכניים של יישום כלים, מערכות ומנגנוני אבטחת המידע והגנת הסייבר על פי הכללים שחלים עליו מתוקף תקנות הגנת הפרטיות אבטחת מידע והנחיות יה"ב.

ממצאי הדוח והבעיות שבשורש ממצאים אלה עלולים לסכן את שלמותם, זמינותם, סודיותם ואמינותם של ציוני בחינות הבגרות וכן עולה מהם חשש לפגיעה בעקרונות טוהר הבחינות. משרד מבקר המדינה ממליץ למשרד החינוך לפעול לתיקון הליקויים שהועלו בדוח, ובכלל זה לעמוד בלוחות הזמנים שנקבעו בתוכניות העבודה בתחום אבטחת המידע והגנת הסייבר, לשפר ולהעלות את רמת אבטחת המידע והגנת הסייבר בכלל מערכותיו ותשתיותיו. מומלץ גם שבמערכת החדשה לניהול ציוני הבגרות שלדברי המשרד הוא מפתח, יינתן מענה על הממצאים שהועלו בדוח זה בנוגע לאבטחת המידע של בחינות הבגרות וציוני הבגרות.

דוח ביקורת מיוחד - הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות

מבוא

בחינות הבגרות נועדו להעריך את רמת ידיעותיהם של התלמידים על פי קנה מידה אחיד, והן בגדר נקודת הסיום של לימודי התלמיד בחטיבה העליונה. תלמיד זכאי לתעודת בגרות אם עמד בהצלחה בבחינות הבגרות על פי הכללים שקבע משרד החינוך (להלן - המשרד). לזכאות של תלמיד לתעודת בגרות ולציונים שלו בתעודת הבגרות יש השפעה רבה על סיכוייו להתקבל למוסדות להשכלה גבוהה ועל יכולתו להשתלב בעתיד בשוק העבודה.

אגף בכיר בחינות משתייך למינהל הפדגוגי במשרד החינוך (להלן - האגף או אגף הבחינות), הוא מופקד על הארגון והניהול של בחינות הבגרות מטעם המשרד וממונה, בין היתר, על יישום ההנחיות הנוגעות לטוהר הבחינות ואחראי לקיים את הבחינות במועדים שנקבעו. בתום שלב ההיבחנות, אחראי האגף על הפקת תעודות הבגרות לזכאים לכך ועל מתן אישור לציונים בהקדם האפשרי, כדי שלא לעכב את קבלת התלמיד ללימודים במוסדות להשכלה גבוהה.

נתונים כלליים

ככלל, בחינות הבגרות מתקיימות בכתב, באמצעות שאלוני בחינה שגיבש המשרד, והנבחן משיב עליהם במחברת בחינה ייעודית. יש גם בחינות מתוקשבות, שמתקיימות באופן מקוון באמצעות מערכת ייעודית, וכן בחינות בעל פה - במסגרת שאלונים במקצועות מסוימים למשל אנגלית, וכן כהתאמה לנבחנים עם צרכים מיוחדים. ניתן להיבחן במקצוע לימוד לבגרות בכמה רמות קושי, בהתאם למספר יחידות הלימוד שהנבחן למד. זכאי לתעודת בגרות הוא מי שעמד בדרישות הזכאות שקבע משרד החינוך[3]. להלן יוצגו נתונים על פעילות משרד החינוך בתחום בחינות הבגרות בשנת הלימודים התשפ"א (ספטמבר 2020 - יולי 2021).

3 היבחנות בהצלחה במקצועות החובה לפי מסלול הלימודים בבית הספר ולפי המגזר והפיקוח. היבחנות בהצלחה במקצוע מוגבר אחד לפחות, ברמה של חמש יחידות לימוד. עמידה בתנאי קבלת ציון סף במקצועות הפנימיים וצבירה של 21 יחידות לימוד לפחות.

תרשים 1: **נתונים על בחינות הבגרות בשנת הלימודים התשפ"א**

על פי נתוני משרד החינוך, בעיבוד משרד מבקר המדינה.

* מחברות בחינה פיזיות - מחברות נייר שהנבחנים כותבים בהן את תשובותיהם. מחברות בחינה מתוקשבות - קובצי מחשב שכוללים את תשובות הנבחנים שנבחנו באופן מתוקשב.

** תלמידי י"ב שנבחנו בשנת הלימודים התשפ"א.

***מספר התלמידים הזכאים נכון לינואר 2022. המספר עשוי להשתנות בהתאם לתוצאות הערעורים המוגשים.

הצורך בהגנה על מאגרי המידע הנוגעים לבחינות הבגרות: חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), מגדיר את החובות של בעל מאגר מידע, מחזיק מאגר מידע או מנהל מאגר מידע כהגדרתו בחוק, לאבטחת המידע שבו.

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות אבטחת מידע) קובעות את החובות שחלות על בעל מאגר המידע ועל מנהל המאגר, על מחזיק מאגר מידע (למעט החובות לעניין מסמך הגדרות המאגר ומיקור חוץ), בשינויים המחויבים ולפי העניין.

התקנות קובעות שלוש רמות של מאגרי מידע, עליהן חלות שלוש רמות אבטחה שונות: בסיסית, בינונית וגבוהה, בהתאם לסיכוני האבטחה שהם מייצרים[4].

רוב המידע שמשרד החינוך אוסף, שומר ומנהל בעניין בחינות הבגרות הוא מידע רגיש על תלמידים ועובדים, שכולל יותר מ-100,000 רשומות, שלפי תקנות הגנת הפרטיות אבטחת מידע הוא הסף שממנו חלה חובה לרמת אבטחה הגבוהה ביותר, ובהיותו כזה הוא נדרש לרמת האבטחה הגבוהה ביותר שבתקנות, ובכלל זה על משרד החינוך מוטלת החובה לשמור על המידע ולוודא שהוא משמש אך ורק למטרות שלשמן הוא נמסר או לצורכי מילוי חובותיו של המשרד על פי החוק.

נוסף על הצורך להגן על מאגרי המידע מתוקף חוק הגנת הפרטיות ותקנותיו, המשרד נדרש להגן על סודיותו, אמינותו, זמינותו ומהימנותו של המידע בעניין בחינות הבגרות, לרבות השאלונים, מחברות הבחינה והציונים. כמו כן המשרד נדרש לוודא כי הם לא ישונו או יימחקו, וכי הם ייחשפו למי שמורשה לגשת אליהם בלבד, מתוקף תפקידו או מתוקף היותו הגורם שהמידע נוגע לו, כגון התלמידים או הוריהם, או למוסדות השכלה גבוהה ולגורמים אחרים שנדרשים להם תעודת הבגרות וציוני התלמידים.

היבט נוסף המחייב נקיטה של אמצעים כדי למנוע פגיעה במאגרי מידע הוא תקיפות במרחב הקיברנטי[5] (להלן - תקיפות סייבר) ששכיחותן הולכת וגדלה, הגורמות לנזקים משמעותיים ורחבי היקף. המניעים לכך שונים, ובהם כוונה לפגוע במערכות עצמן וכך לשבש את הפעילות התקינה והשוטפת של הארגון, החברה ואף המדינה, למטרת סחיטה, למטרת שינוי מידע כדי ליהנות מהטבות ומרווחים ואף במסגרת אתגר טכנולוגי לשמו. כך, בשנת 2021 טיפל מערך הסייבר הלאומי[6] (להלן - מס"ל) בגילוי, זיהוי, הכלה וסילוק תקיפות סייבר משמעותיות כנגד חברות וגופים במשק הישראלי[7]. מס"ל טיפל בכ-2,200 אירועי סייבר (עלייה של כ-33% ביחס לשנה קודמת). איתר כ- 9,000 חולשות אבטחה חמורות בכ- 3,300 גופים, והעביר כ- 4,400 דיווחים ממוקדים לארגונים בגין הממצאים שאותרו. על פי מס"ל, בשנת 2021 נרשמה עלייה של 20% במספר הדיווחים שאותם הוא קיבל ואימת כאירועי סייבר בהשוואה לשנת 2020[8].

בהחלטת הממשלה על "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית'" מ-2014[9] (להלן - החלטת הממשלה 2097 על ישראל דיגיטלית) הורחבו והוגדרו מחדש היעדים, התפקידים והסמכויות של רשות התקשוב הממשלתי והעומד בראשה. במסגרת התפקידים והסמכויות שהוגדרו: גיבוש מדיניות לניהול סיכוני תקשוב וסיוע בהטמעת מתודולוגיה לניהול סיכוני תקשוב באגפי מערכות המידע והטמעת חובות אבטחת מידע לפי דין; על הממונה על התקשוב הממשלתי הוטל לפרסם הנחיות

4 ראו את המדריך המלא לתקנות הגנת הפרטיות אבטחת מידע באתר: www.gov.il/he/departments/Guides/data_security_guide

5 המרחב הקיברנטי הוא מרחב טכנולוגי הכולל מחשבים, רשתות מחשבים, תוכנות, מידע ממוחשב, תוכן דיגיטלי ובסיסי נתונים, שמתקיים, בין היתר, הודות לרשת האינטרנט ולטכנולוגיית ממשק בין מחשבים.

6 מערך הסייבר הלאומי הוא הוא גוף ביטחוני-טכנולוגי המופקד על הגנת הסייבר בישראל מכוח החלטת הממשלה 3270 מיום 17.12.2017.

7 ראו סיכום שנת 2021 - מערך הסייבר הלאומי.

8 שם.

9 החלטת הממשלה 2097 (10.10.14).

מקצועיות מחייבות בתחומי סמכותו למנהלי אגפי מערכות המידע, שבמשרדי הממשלה וביחידות הסמך, וזאת בתיאום עם הרגולטורים הרלוונטיים לעניין.

על פי החלטת הממשלה 2443 בדבר "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" מ- 2015[10] (להלן - החלטת הממשלה 2443 בעניין הגנת הסייבר או החלטת הממשלה 2443), ייעוד היחידה להגנת הסייבר בממשלה (להלן - יה"ב) הפועלת במסגרת רשות התקשוב הממשלתית, היא להיות הגוף המנחה מהבחינה המקצועית את משרדי הממשלה ויחידות הסמך בתחום הגנת הסייבר[11].

טוהר בחינות הבגרות: לבד מהצורך להגן על שלמות מאגרי המידע הנוגעים לבחינות הבגרות ועל אמינותם, למנוע את הפגיעה בהם ואת חשיפתם למי שאינו מורשה לכך, יש גם צורך לשמור על טוהר הבחינות של בחינות הבגרות. משרד החינוך[12] קבע כי השמירה על טוהר הבחינות היא משימה חינוכית, מוסרית וערכית, אשר נועדה להבטיח שוויוניות, הגינות ומתן ביטוי נאות לרמת הידע של הנבחנים. על הבחינות לשקף את בקיאות הנבחנים באופן עצמאי. פגיעה בטוהרן מקנה יתרון לנבחנים מסוימים, ומשפיעה על כלל הנבחנים ועל התפיסה בעניין אמינות הבחינות ועל ערכן ככלי הערכה.

בחוזר מנכ"ל המשרד "טוהר הבחינות" מדצמבר 2019[13] (להלן - חוזר טוהר הבחינות) הוגדרו תחומי האחריות של כל הגורמים (הנבחן, בעלי התפקידים בבית הספר ומשרד החינוך) לשמירה על טוהר הבחינות. אגף הבחינות, המופקד על הארגון והניהול של בחינות הבגרות מטעם המשרד, ממונה גם על יישום ההנחיות הנוגעות לטוהר הבחינות. אחריותו באה לידי ביטוי הן בעת שקודמת לבחינה, הן ביום הבחינה והן לאחריה. בעידן הדיגיטלי, שבו משרד החינוך משתמש במערכות מידע רבות לצורך ניהול ותפעול של בחינות הבגרות מתחילתן ועד סיומן, קיום ממשל אבטחת מידע והגנת סייבר תקין הם מרכיבים חיוניים לשם שמירה על טוהר הבחינות.

משרד החינוך מדרג מדי שנה את בתי הספר לפי מדד טוהר הבחינות הבוחן את התנהגות התלמידים במהלך בחינות הבגרות, ובה בעת אמור להעיד על מידת הצלחתו של בית הספר להקנות לתלמידים ערכי יושר, אמינות והגינות. מדד טוהר הבחינות מסווג את בתי הספר לשלוש רמות, המשקפות את טוהר הבחינות של אותו בית ספר לאותה שנה. למסלול הירוק משתייכים בתי ספר שלא נמצאה בהם פגיעה בטוהר הבחינות או שהפגיעה בטוהר המידות בהם מועטה יחסית. למסלול הצהוב משתייכים בתי ספר שהשמירה על טוהר הבחינות בהם אינה משביעת רצון, ולמסלול האדום משתייכים בתי ספר שבהם הפגיעה בטוהר הבחינות הייתה רבה, ומשכך המשרד אינו מאפשר להם לנהל בעצמם את הבחינות והן מתקיימות בניהול חברה חיצונית שעמה התקשר המשרד. בשנת הלימודים התשפ"א (ספטמבר 2020 - יולי 2021), כ-12,000 מכ-1.4 מיליון מחברות בחינה נמצאו "חשודות", ולכן נדרש לבחון את אמינותן. הנתונים המובאים בתרשים להלן משקפים את סיווג בתי הספר שמגישים לבגרות לפי מדד טוהר הבחינות בשנת הלימודים התשפ"א:

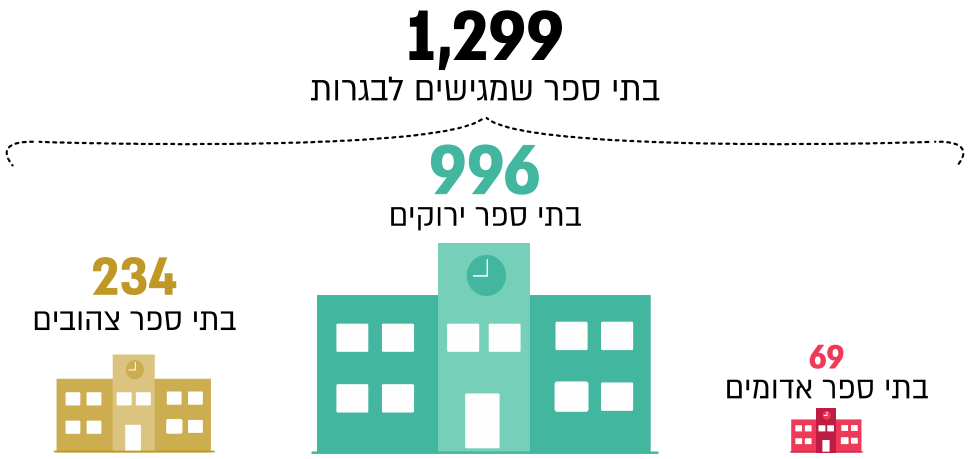
10 החלטת הממשלה 2443 (15.2.15).

11 בדברי ההסבר להחלטת הממשלה נקבע כי הנחיות יה"ב מחייבות את משרדי הממשלה ואת יחידות הסמך.

12 https://apps.education.gov.il/mankal/Horaa.aspx?siduri=391

13 "טוהר הבחינות" הוראת קבע 0237 - החלפה מדצמבר 2019.

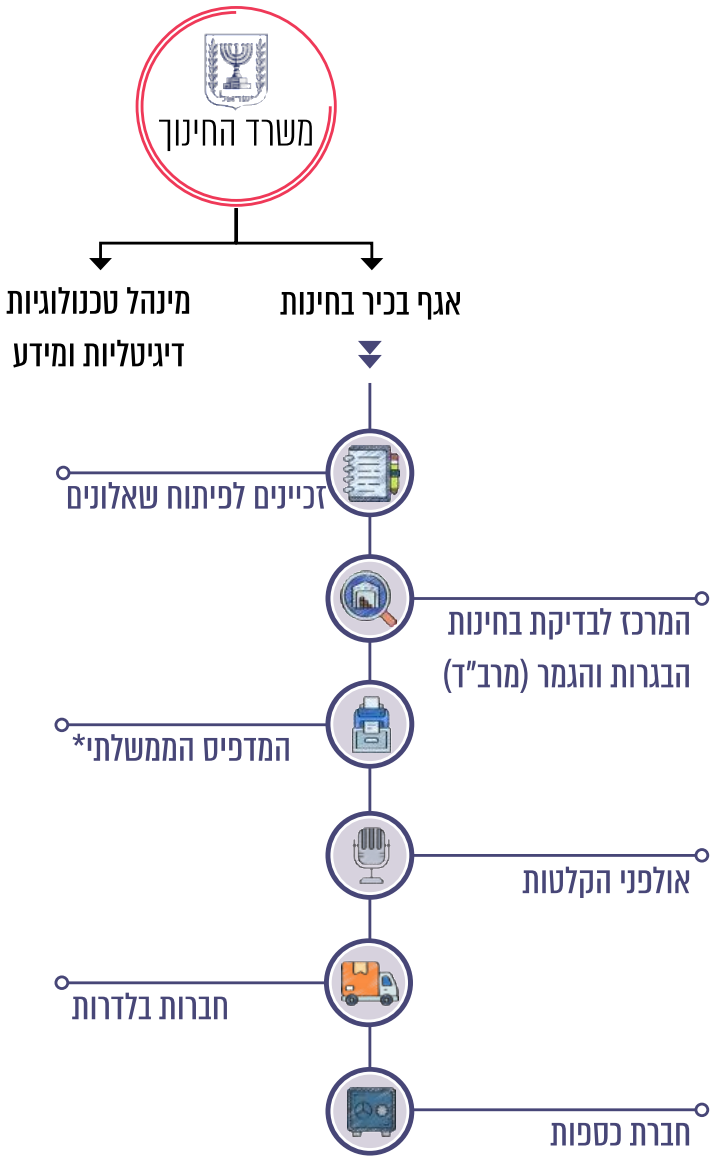
תרשים 2: **סיווג בתי הספר לפי מדד טוהר הבחינות בשנת הלימודים התשפ"א**



על פי נתוני משרד החינוך, בעיבוד משרד מבקר המדינה.

הגופים העיקריים המעורבים בתהליך הניהול והתפעול של בחינות הבגרות: לצורך ניהול בחינות הבגרות, תפעולן ואבטחת המידע שלהן מסתייע אגף הבחינות בגורמים פנים-משרדיים ובגורמים חיצוניים. בין הגורמים החיצוניים נכללים ספקים וזכיינים שעימם התקשר המשרד.

תרשים 3: **הגורמים העיקריים המעורבים בתהליך הניהול והתפעול של בחינות הבגרות**



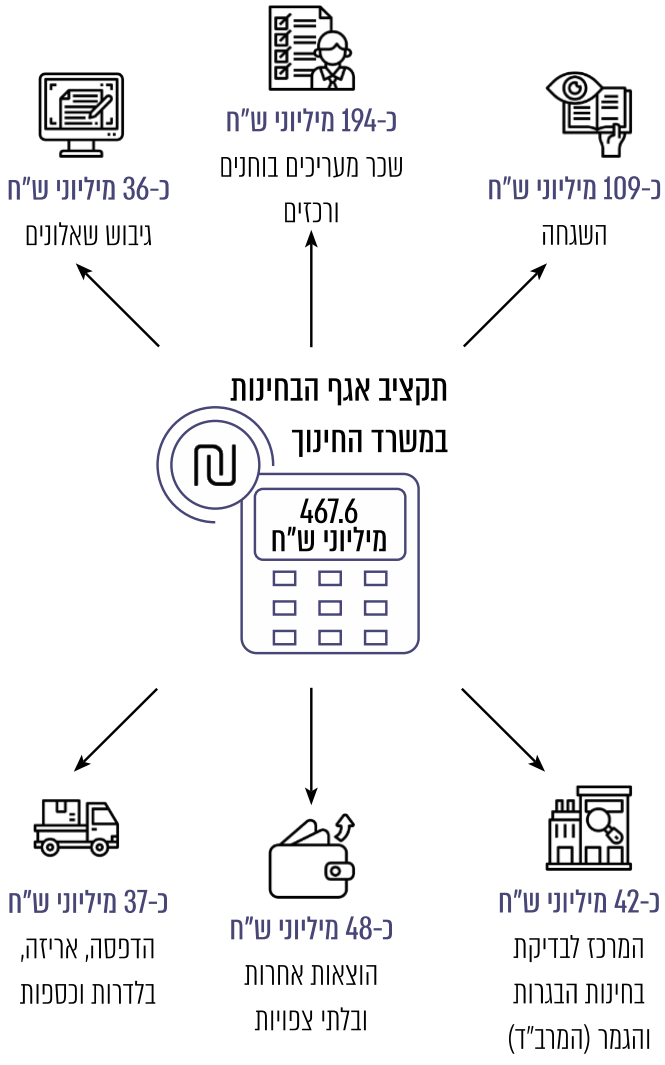
בסגול-גורמים חיצוניים

על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

* המדפיס הממשלתי הינו יחידת סמך במשרד האוצר. תפקידו העיקרי ביצוע והפקת עבודות הדפוס למשרדי הממשלה ויחידות הסמך באמצעות ייצור עצמי או באמצעות התקשרויות עם קבלני משנה חיצוניים.

עלות תפעול בחינות הבגרות: בשנת 2021 הסתכמה עלות התפעול של מערך בחינות הבגרות בכ-467.6 מיליון ש"ח. בתרשים שלהלן מוצגים תחומי ההוצאות העיקריות של משרד החינוך לצורך תפעול וניהול של בחינות הבגרות.

תרשים 4: **תחומי ההוצאות העיקריות על תפעול וניהול של מערך הבחינות, 2021**[14]



על פי נתוני משרד החינוך, בעיבוד משרד מבקר המדינה.

14 המספרים שבתרשים מעוגלים.

ניהול המידע על בחינות הבגרות: מינהל טכנולוגיות דיגיטליות ומידע (להלן - מינהל תקשוב) במשרד החינוך אחראי לתחום מערכות המידע במשרד החינוך. הוא מופקד על פיתוח הניהול וההטמעה של תשתיות המחשוב, מערכות מידע ומאגרי מידע וכן הוא אחראי לאבטחתם, בהתאם למקובל ולדרישות הדין.

למשרד החינוך יותר מ-200 מערכות מידע, חלקן ניהוליות-תפעוליות ומשמשות, למשל, לניהול של מערך התלמידים, מערך עובדי ההוראה ומערך עובדי המשרד עצמו; וחלקן מערכות ייעודיות-מקצועיות המשמשות לצרכים פדגוגיים. בתהליך הניהול והתפעול של בחינות וציוני הבגרות פועלות כמה עשרות מערכות מידע, חלקן בשליטת משרד החינוך וחלקן בשליטה של ספקים חיצוניים (להלן - זכיינים), הנושאים שנבדקו במסגרת ביקורת זו מתייחסים ל-8 מהמערכות.

אבטחת בחינות הבגרות נחלקת לשני תחומים: אבטחה פיזית ואבטחה לוגית (דיגיטלית). על האבטחה הפיזית אחראי תחום אבטחת הבחינות שבאגף בכיר חירום ביטחון ובטיחות במשרד. על האבטחה הלוגית אחראי מינהל תקשוב שבמשרד, אשר מספק לאגף הבחינות את השירותים בתחום טכנולוגיות המידע ובכלל זה את צורכי אבטחת המידע והגנת הסייבר של מערכות המידע שתומכות בתהליך הניהול והתפעול של בחינות הבגרות ומתן הציונים, ובסביבות התקשוב שבהן הן פועלות. הוא מונחה על ידי יה"ב, שתפקידה להכווין ולהנחות מהבחינה המקצועית את משרדי הממשלה ויחידות הסמך בתחום הגנת הסייבר.

פעולות הביקורת

בחודשים פברואר 2021 - מאי 2022 בדק משרד מבקר המדינה את אבטחת המידע של מערכות המידע המרכזיות שתומכות בניהול ובתפעול של ציוני בחינות הבגרות ובסביבות התקשוב שבהן הן פועלות. הבדיקה בוצעה במטה המשרד, באגף הבחינות ובמינהל תקשוב, במרכז לבדיקת בחינות הבגרות והגמר (להלן - מערך המרב"ד) שמתופעל על ידי חברה חיצונית (להלן - החברה החיצונית). בדיקת השלמה בוצעה ביה"ב ובמשטרת ישראל.

במסגרת הביקורת קיים משרד מבקר המדינה היוועצות במומחים חיצוניים מתחום אבטחת מידע (להלן - היועצים) במתכונת דומה לסקר סיכונים "אבטחת מידע וסייבר", בדגש על בדיקת שלושת היעדים העיקריים של אבטחת מידע: שלמות (Integrity); סודיות (Confidentiality); וזמינות (Availability) המידע של ציוני הבגרות.

הדוח שבנדון הומצא לראש הממשלה ביום 6.12.22.

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

ממשל אבטחת מידע במשרד החינוך

סקרי סיכונים ומבדקי חדירות במשרד החינוך

תקנות הגנת הפרטיות אבטחת מידע, קובעות כי בעל המאגר שנדרש לרמה הגבוהה של אבטחת מידע אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים) ומבדקי חדירות למערכות המאגר אחת ל-18 חודשים לפחות. עוד נקבע בתקנות כי בעל המאגר יפעל לתיקון הליקויים שהתגלו, ככל שהתגלו. בהנחיית יה"ב "ניהול סיכוני סייבר במשרדי הממשלה"[15], נקבע ביחס לכלל מערכות המידע של המשרד כי ביצוע סקר הסיכונים, לא יפחת מאחת ל-36 חודשים ויתוקף לפחות אחת ל-18 חודשים.

סקר סיכונים 2018: בשנת 2018 ביצע משרד החינוך סקירה והערכת סיכוני סייבר רוחביים והערכת סיכוני סייבר עבור מערכות ליבה נבחרות (להלן - סקר סיכונים 2018); הוא ביצע את סקר הסיכונים בשיתוף מערך הסייבר (הרשות הלאומית להגנת הסייבר דאז) ויה"ב ובאמצעות חברה חיצונית. ממצאי הסקר העידו כי רמת הגנת הסייבר במערכות המידע של משרד החינוך הייתה נמוכה, וכי נדרש לשפרה במידה רבה. בסיכום הסקר צוין כי נוכח התלות הגבוהה של המשרד במערכות המידע ונוכח היקף המידע הנרחב המנוהל בהן, הרי שבפגיעה במערכות גלום סיכון שעשוי להיות בעל השפעות ניכרות מהבחינה התפעולית הנוגעות לפעילות השוטפת של המשרד, ואף עלולות להיות לכך "השלכות לאומיות משמעותיות".

על פי דוח סקר סיכונים 2018, הערכת רמת בקרות הגנת הסייבר ואבטחת מידע המיושמת במשרד החינוך בוצעה באופן רוחבי (ולא כבדיקה פרטנית למערכת בודדת). במסגרת זו זוהו והוערכו רוחבית 179 בקרות מתחום תורת ההגנה; בתרשים שלהלן מוצגים ממצאי ההערכה:

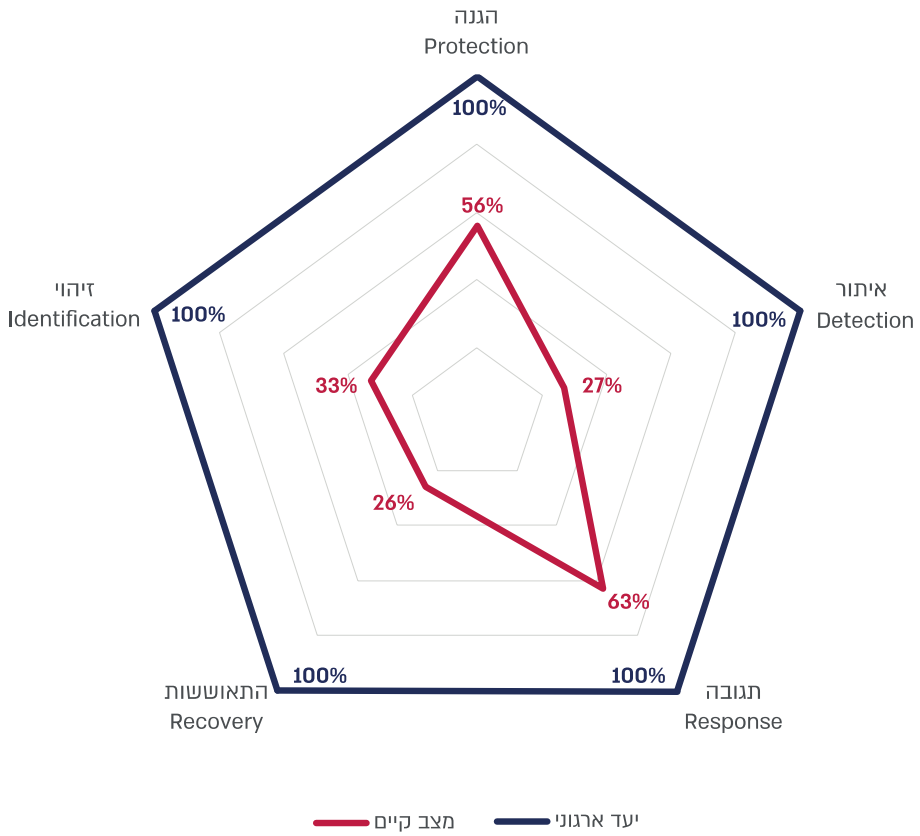
15 הנחיה מספר 5.3 מתאריך 10.07.2017, תאריך עדכון 16.9.2018, גרסה 2.0.

תרשים 5: **ממצאי הערכת הבקרות על פי דוח סקר סיכונים 2018**

על פי נתוני דוח סקר סיכונים 2018, בעיבוד משרד מבקר המדינה.

דוח סקר סיכונים 2018 המחיש גם את הפערים הקיימים במימוש הבקרות על פי פונקציות ההגנה. התרשים הבא מתוך דוח סקר סיכונים 2018 מציג ממוצע של ממצאי ההשוואה בין רמת הבקרות המיושמות בזמן ביצוע הסקר לבין רמת הבקרות הנדרשות על פי תורת ההגנה:

תרשים 6: **השיעור הממוצע של מימוש הבקרות, על פי פונקציית ההגנה**



על פי דוח סקר הסיכונים 2018.

עלה כי על פי סקר סיכונים 2018 שביצע המשרד, שיעור המימוש של הגנות הבקרה בפועל במשרד היה בין 26% מהיעד הארגוני, בכל הנוגע ל"התאוששות" (Recovery), ל-63% בכל הנוגע ל"תגובה" (Response). אשר לפונקציית "הגנה" (Protection) - המשרד מיישם כ-56% מהבקרות הרלוונטיות לפונקציית זו. יצוין כי זו הפונקציה הרחבה ביותר בתורת ההגנה בסייבר לארגון[16], והיא עוסקת בחסימת מתקפות סייבר המנסות לפגוע בארגון. נכללות בה בקרות העוסקות בהרשאות גישה, בהגנה על המידע, בהגנה על תחנות עבודה ועל שרתים, במניעת קוד זדוני, בהצפנה וכו'.

16 מערך הסייבר הלאומי, "תורת הגנה בסייבר לארגון 2.0" שפורסמה ב-19.7.21. המסמך כולל מידע מקצועי תחום הסייבר, והוא נכתב לצורך קידום הגנת הסייבר במשק הישראלי.
https://www.gov.il/he/departments/general/cyber_security_methodology_2

מבדק חדירה אפליקטיבי 2018: בשנת 2018 ביצע משרד החינוך גם מבדק חדירה אפליקטיבי[17] למערכת א', אשר הוגדרה בסקר הסיכונים כאחת ממערכות הליבה של המשרד. המבדק בוצע באמצעות חברה חיצונית, ובפיקוח יה"ב. המבדק העלה ממצאים קריטיים אשר מאששים את מסקנות סקר הסיכונים, לפיהן רמת המוגנות של המשרד אינה מספקת, ומוכיחים כי סיכוני הסייבר עלולים להתממש על ידי גורמים עוינים.

עלה כי באוקטובר 2021, יותר משלוש שנים לאחר שביצע משרד החינוך בשנת 2018, סקר סיכונים מקיף של מערכות ליבה נבחרות שלו ומבדק חדירה בנוגע למערכת א', משרד החינוך לא ביצע סקר סיכונים מקיף עדכני ולא מבדקי חדירות בנוגע לאותן מערכות ליבה, אף שבשתי בדיקות אלו עלו ממצאים שנשקף בגינם סיכון רב, ואף שלפי תקנות הגנת הפרטיות אבטחת מידע חלה עליו חובה לבצעם אחת ל-18 חודשים.

יצוין שבשנים 2020 ו-2021 ביצע משרד החינוך מבדקי חדירות למערכות אחרות; וכן הוא ביצע סקר סיכונים לתשתיות המשרד, ביצע סקר סיכונים ומבדק חדירות בנוגע לרשת ג', וסריקות אבטחת מידע באמצעות מערכת סריקה אוטומטית שהפעילה יה"ב לאתרי המרשתת (האינטרנט) החיצוניים של המשרד, כגון אתר "מומחים".

על משרד החינוך לפעול לעריכת סקרי הסיכונים ומבדקי חדירה למערכות הליבה שלו לכל הפחות אחת ל-18 חודשים כנדרש על פי חוק הגנת הפרטיות ותקנותיו, ולבצע סקרי סיכונים אחת ל-36 חודשים על פי הנחיות יה"ב. אם אלה לא יבוצעו, נשקף סיכון משמעותי לאי-גילוי סיכונים וחולשות של אבטחת מידע, ובכך להביא לחשיפה מוגברת לפגיעה בתשתיות המחשוב של המשרד, במערכות המידע ובמאגרי הנתונים שלו, עד כדי שיבושם, השבתתם וחשיפת הנתונים הפרטיים לגורמים לא מורשים.

בתשובתו למשרד מבקר מדינה מאוגוסט 2022 מסר משרד החינוך (להלן - תשובת המשרד)[18], כי הוא ביצע מבדקים וסקרים בשנים 2020 ו-2021, וכי הוא נערך לבצע סקרי סיכונים על התשתיות ועל כלל מערכות המידע ומאגרי המידע שברשותו בהתאם לתקנות הגנת הפרטיות.

יישום תוכנית העבודה התלת-שנתית

נוכח ממצאי סקר הסיכונים 2018 גיבש המשרד תוכנית עבודה תלת-שנתית לשיפור הגנת הסייבר בתשתיות מערכות המידע שלו (להלן - תוכנית עבודה תלת-שנתית). תוכנית העבודה התבססה, בין היתר, על סקר הסיכונים 2018 והיא כוללת פעילויות שתוכננו לשנת 2018 וטרם בוצעו.

בהנחיית יה"ב "הנחיית מסגרת להגנת הסייבר בממשלה" (להלן - הנחיית המסגרת) נקבע כי יש לבצע מידור בין החלקים השונים ברשת, באמצעות חלוקתה לסגמנטים והגבלת אפשרות

17 במבדק חדירה אפליקטיבי מייצרים מצב שבו תוקף מנסה לחדור לאפליקציה וכך לגלות את החולשות שבה. בין השאר, במבדק נבחנת האפשרות לקבל גישה לבסיסי נתונים, לשנות או לעקוף הרשאות גישה, להשבית או לשבש את פעולת המערכות.

18 משרד החינוך מסר למשרד מבקר המדינה כי הוא כלל בתשובתו גם את תגובת החברה החיצונית על ממצאים שמשרד מבקר המדינה העביר אליה.

הקישור ביניהם בהתאם לרמת הרגישות של המערכות. עוד נקבע בהנחיה כי במסגרת ההגנה מפני תקיפה ופגיעה במערכות, נדרשים, כחובה מינימלית, בין השאר: אמצעי טכנולוגי מתאים להתמודדות עם הדבקה או למניעת הורדה של קוד עוין למחשב; הקשחה[19] ואבטחה של מערכות ההפעלה, היישומים, בסיסי הנתונים, ציוד התקשורת והתקני המחשב באמצעות הסרת רכיבים המותקנים כברירת מחדל ואינם נחוצים לפעילות השוטפת. בהנחיית יה"ב "הקשחת רכיבי תקשורת"[20] נקבע כי על המשרד להטמיע מערכת בקרת גישה לרשת - Network Access Control (להלן - NAC) אשר תנהל את הגישה של מרכיבי הקצה (למשל עמדות עבודה) לרשת הארגונית.

צוות הביקורת בחן את סטטוס הטיפול בשבע המשימות, שהוגדרו ברמה קריטית או גבוהה בתוכנית העבודה התלת-שנתית, מתוך 17 המשימות שהמשרד קבע שיש ליישמן במהלך שנת 2019. הבדיקה התבצעה בהסתמך על דיווח שמסר משרד החינוך לצוות הביקורת באוקטובר 2021.

עלה כי מתוך שבע המשימות שנבדקו והוגדרו ברמת סיכון "קריטית" או "גבוהה" לביצוע ושהמשרד קבע שיש ליישמן בשנת 2019, נכון לאוקטובר 2021, המשרד סיים לטפל בשלוש משימות באופן מלא, ובארבע משימות הוא טיפל חלקית.

על משרד החינוך להשלים את הפעולות הנדרשות כדי לטפל בממצאים שהועלו בבדיקות ונקבעו כמשימות בתוכנית העבודה.

המשרד ציין בתשובתו כי בשנת 2022 הוא המשיך ליישם את תוכנית העבודה. המשרד הוסיף שבעקבות הביקורת "בוצעו חידודים ותיקונים בתוכנית העבודה".

מוכנות משרד החינוך להתאוששות מאסון (DR - Disaster Recovery)

בהנחיית יה"ב "גיבוי ושחזור מידע"[21] משנת 2021 נקבע כי "מערך הגיבוי והשחזור בארגון הינו מנגנון קריטי המאפשר להתמודד עם סוגיות הנוגעות לסודיות, שלמות, אמינות וזמינות המידע". על פי ההנחיה, יש לבצע בדיקה לתקינות שחזור המידע לפחות אחת לחצי שנה, ליזום ניסיונות שחזור מדגמיים כדי לוודא את תקינות מערך הגיבוי וכן להצפין את עותק הגיבויים לפני הוצאתו לשמירה מחוץ לאתר הראשי או לאתר הגיבויים (Disaster Recovery, להלן - DR).

19 הקשחה היא אוסף פעולות פיזיות ולוגיות שמבוצעות בציוד מחשובי (למשל ביצוע שינויים בפרמטרי ההפעלה או הקונפיגורציה של מערכת מחשב) שמטרתן צמצום משטח התקיפה של גורמים עוינים ובכך להקשות את פעולת החדירה הלא מורשית למערכות המחשוב.

20 הנחיה 5.18 מ-13.9.18, תאריך עדכון 8.11.20.

21 הנחיית יה"ב 5.30 גרסה 1.0, תאריך הוצאה 20.5.21.

במאי 2019 הוסמך משרד החינוך לתקן ישראלי ISO/IEC27001:2013(E)[22] (להלן - תקן ISO-27001). במסגרת ההסמכה לתקן נכתבו ואושרו במשרד נוהלי עבודה ובהם נוהל "אבטחת מידע בהמשכיות עסקית" (Business Continuity Plan, להלן - נוהל BCP) ונוהל גיבוי מערכות.

מדיניות הגיבויים של משרד החינוך: על פי הדיווח שמסר משרד החינוך לצוות הביקורת, הוא הקים אתר גיבוי (DR) השוכן בחוות השרתים, אצל חברה חיצונית הנותנת שירותים למשרד. באתר ה-DR משוכפלות באופן רציף ושוטף כל המערכות הקריטיות של המשרד (והמידע הדיגיטלי שלהן), למעט מערכת מחשב ייעודית. בעניינה של מערכת זו מקיים המשרד מדיניות גיבויים נפרדת, על פי התדירות ופרק הזמן לשמירה שהוא קבע, בכלל זה נשמרים עותקים של גיבויים אלו באתרים שונים בלי שהמידע הוצפן.

> עלה כי משרד החינוך לא ביצע תרגילים מסוימים לשחזור מידע ולהתאוששות מאסון כנדרש בהנחיית יה"ב "גיבוי ושחזור מידע".
>
> על משרד החינוך לבצע תרגילי שחזור תקופתיים בהתאם להנחיות יה"ב, וזאת כדי לבחון את מידת היערכותו ומוכנותו להתמודדות עם תרחישים אפשריים. מומלץ שהמשרד יקדם את הטיפול להתאוששות מאסון לכלל מערכותיו, לרבות למערכת ג', ויבצע הצפנה של המידע כנדרש.

בתשובתו ציין המשרד, כי ביצע ניסוי להפעלת אתר ה-DR בסביבה מבודדת, וכי במסגרת תכנית העבודה שלו הוא מתכנן לשדרג את מערכת המחשב הייעודית, כך שגם לה יינתן מענה לביצוע גיבוי באתר DR.

עמידת משרד החינוך בחובות הנקבעות לפי תקנות הגנת הפרטיות אבטחת מידע

חוק הגנת הפרטיות מטיל, בין השאר, אחריות לאבטחת המידע במאגרי המידע על כל גורם, ציבורי או פרטי, שהוא בעל מאגר מידע, מנהל מאגר מידע או מחזיק מאגר מידע כהגדרתו בחוק. כמו כן, הוא מטיל על גורמים אלה את החובה לרשום את המאגר אצל רשם מאגרי מידע. תקנות הגנת הפרטיות אבטחת מידע מגדירות את רמת אבטחת המידע הנדרשת מכל גורם בנוגע לכל מאגר מידע, ובהתאם לכך את החובות שחלות עליו. התקנות הותקנו בשנת 2017 ונכנסו לתוקפן במאי 2018, שנה מיום פרסומן.

בדיקה שעשה צוות הביקורת בפנקס רשם מאגרי מידע שברשות להגנת הפרטיות שבמשרד המשפטים העלתה שנכון למרץ 2020 משרד החינוך רשום כבעלים של כ-50 מאגרי מידע.

חובת גיבוש וניהול מסמכים: לפי תקנות הגנת הפרטיות אבטחת מידע, על בעל המאגר לנהל מסמך הגדרות מאגר ועליו לעדכנו בכל עת שנעשה שינוי משמעותי בנושאים המפורטים בהוראה וכן עליו לבחון את הצורך בעדכון המאגר בשל שינויים טכנולוגים ארגוניים או אירועי אבטחה, בכל שנה עד ה- 31 בדצמבר (להלן - מסמך הגדרות המאגר). התקנות קובעות גם כי על בעל מאגר המידע להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת

22 ת"י ISO/IEC27001:2013(E)- תקן ישראלי שאומץ מתקן ISO בינלאומי העוסק במיסוד מערכת לניהול אבטחת מידע ארגונית ושיפורה המתמיד (Information Security Management System) ISMS

של מערכות המאגר, שתכלול, בין השאר, תוכנות וממשקים המשמשים לתקשורת עם מערכות המאגר (להלן - מסמך מבנה המאגר ורשימת המצאי).

משרד החינוך מסר לצוות הביקורת כי הוא פועל למיפוי מידת העמידה של חמשת מאגרי המידע המפורטים להלן בתקנות הגנת הפרטיות אבטחת מידע: מערכת תיק תלמיד, מערכת קידום נוער ברשויות, מערכת פורטל חינוך מיוחד, מערכת משתמשים והרשאות, ומערכת תלמידים החדשה. עוד מסר כי הוא הקים "תיק מאגר" כהגדרתו (שאמור לכלול את מסמך הגדרות המאגר, מסמך מבנה המאגר ורשימת המצאי) לכל אחד מחמשת המאגרים, וכי בתוכנית העבודה שלו לשנת 2022 נכללת הרחבה של מיפוי המאגרים ובדיקת עמידתם בתקנות הגנת הפרטיות אבטחת מידע, זאת בכפוף להקצאה תקציבית.

עלה בביקורת כי, שלוש שנים לאחר כניסת תקנות הגנת הפרטיות אבטחת מידע לתוקף (במאי 2018), משרד החינוך גיבש את מסמכי מבנה המאגר, את הגדרות המאגר ואת רשימת המצאי עבור חמישה (כ-10%) מ-50 מאגרי המידע שרשומים בפנקס רשם מאגרי מידע.

ממצאי בדיקת תיק המאגר "תלמידים"[23], שמסר משרד החינוך לצוות הביקורת, העלו כי מסמך הגדרות המאגר אינו מעודכן בכל הנוגע לזהות ממונה אבטחת המידע, וכי רשימת המצאי אינה מלאה, למשל, לא מתועדים בה תוכנות וממשקי תקשורת עם מערכות המאגר.

המשרד ציין בתשובתו, כי הוא נמצא בתהליך הסדרה של מאגרי המידע, ובכלל זה - ביעור מאגרים ישנים, צמצום מספר המאגרים הרשומים ורישום מחדש של שמונה מאגרים, ובכלל זה הכנת תיק לכל מאגר שיכלול מסמך הגדרות למאגרים, סקרי סיכונים ומבדקי חדירות לכל המערכות הניגשות למאגר.

על משרד החינוך לפעול על פי תקנות הגנת הפרטיות אבטחת מידע ולהשלים לגבי כלל מאגרי המידע שהוא מנהל או מחזיק את גיבוש המסמכים העוסקים בהגדרות המאגר ובמבנה המאגר ואת גיבוש רשימת המצאי לכלל מאגרי המידע שהוא מנהל או מחזיק. כמו כן על משרד החינוך לוודא כי המסמכים והרשומות האמורים שלמים ומעודכנים.

הסמכת המשרד לתקן ISO-27001: רשם מאגרי מידע הורה בהנחיה משנת 2018[24], מכוח סמכותו בסעיף 20(ב) לתקנות הגנת הפרטיות אבטחת מידע, כי ארגון אשר הוסמך לתקן ישראלי ISO-27001 ושמקיים בפועל את הוראותיו לרבות הבקרות שמפורטות בנספח לתקן, יראו אותו כמי שמקיים את תקנות הגנת הפרטיות אבטחת מידע במלואן ביחס למאגרים עליהם ניתנה ההסמכה לתקן וכל עוד ההסמכה עומדת בתוקפה, וזאת אם ימלא סעיפים מסוימים בתקנות כמפורט בהנחיה.

23 תיק מאגר המידע "תלמידים" מס' 980046606.

24 תחולת תקנות הגנת הפרטיות (אבטחת מידע) על ארגונים המוסכמים לתקן ISO/ICE 27001, הנחיה 03/2018.

בנובמבר 2020 ביצע הגוף המסמיך לתקן ISO-27001 בדיקת מעקב בעניין, ובעקבות כך הוארך מועד ההסמכה של המשרד, זאת אף שנרשמה הערה בדבר "אי-התאמה" של המשרד לדרישות התקן לעניין אתר ה-DR ולתוכנית המשכיות עסקית (BCP).

בביקורת עלה כי אף שנכון לדצמבר 2021 למשרד החינוך יש הסמכה בתוקף לתקן ISO-27001, הוא אינו מקיים את כל ההוראות ואת כל הבקרות שמפורטות בתקן, ובפרט לעניין ביצוע תרגילי שחזור תקופתיים, והוא אינו מנהל מסמך הגדרות המאגר, מסמך מבנה המאגר ורשימת מצאי עבור כל מאגרי המידע שברשותו, ואינו מבצע סקרי סיכונים ומבדקי חדירות, כנדרש בסעיפי התקנות וכאמור בהנחיה.

מומלץ למשרד החינוך לקדם את התהליך למיפוי מלא ועדכני של כלל מאגרי המידע. מיפוי זה נדרש לשם קבלת תמונת מצב שלמה של כלל מאגרי המידע ווידוא כי משרד החינוך עומד בדרישות שנקבעו בתקנות הגנת הפרטיות אבטחת מידע.

מינוי של ממונה הגנת סייבר, מנהל הגנת סייבר וועדת היגוי משרדית

בהחלטת הממשלה מס' 2097 על ישראל דיגיטלית, הוחלט בין היתר "להטיל על הממונה על התקשוב הממשלתי... להנחות את משרדי הממשלה ויחידות הסמך למנות אחראי לניהול סיכוני תקשוב ביחידותיהם". בהחלטת הממשלה 2443 בעניין הגנת הסייבר נקבע כי יש להטיל על המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך לפעול לשיפור רמת הגנת הסייבר ולשם כך למנות ממונה הגנת סייבר שיהיה כפוף ישירות למנכ"ל או מי מטעמו[25], עוד נקבע כי המשרדים ימנו מנהל הגנת סייבר ביחידת מערכות המידע שיהיה כפוף ישירות למנהל מערכות המידע במשרד, וכי על משרדי הממשלה להקים ועדת היגוי משרדית לנושא הגנת הסייבר שתפעל לשיפור רמת הסייבר של המשרד ותפקח על הפעילות השוטפת המבוצעת במשרד בנושא זה (להלן - ועדת היגוי סייבר)[26]. מנכ"ל המשרד ישמש יו"ר הוועדה, וחברי הוועדה יהיו נציגים בכירים במשרד בעלי אחריות לתחום הגנת הסייבר, לרבות נציגים של הייעוץ המשפטי של המשרד ונציגים של יה"ב. בהחלטה נקבע כי גם כי על הוועדה להתכנס לכל הפחות פעם בחציון.

בהנחיית המסגרת נקבעו תפקידי ועדת היגוי סייבר, ובין השאר נקבע כי עליה ליזום ביצוע של סקרי הנהלה כדי לבדוק את מידת הישימות והביצוע של הפעילויות המוגדרות למערכת ניהול הגנת הסייבר במשרד, לבחון את ממצאי הסקרים ולשקול הטמעה של ההמלצות וביצוע שינויים רלוונטיים כנדרש. על ועדת ההיגוי לגבש מדדים כמותיים בנושאי הגנת הסייבר, אשר באמצעותם ניתן יהיה לבחון ולמדוד את רמת האפקטיביות של יישום תשתית הגנת הסייבר ולבחון את מידת היישום בתום כל חציון, במסגרת סקר ההנהלה.

ביולי 2015 מינתה מנכ"לית משרד החינוך דאז את סמנכ"ל מינהל תקשוב (דאז) כממונה הגנת סייבר במשרד החינוך (להלן - סמנכ"ל התקשוב).

25 החלטת הממשלה 2443.

26 שם.

עלה כי בסוף שנת 2020 פרש סמנכ"ל התקשוב ממשרד החינוך, ומאז ונכון לאוקטובר 2021 לא מונה לו מחליף כממונה הגנת סייבר במשרד.

עוד עלה כי ועדת היגוי סייבר התכנסה לאחרונה בנובמבר 2019, ומאז ועד לסוף שנת 2021 היא לא התכנסה. עיון בסיכום הדיון של ועדת ההיגוי מנובמבר 2019 מעלה כי בדיון הוצג סטטוס תכנית העבודה לשנים 2018 - 2019, נסקרו אירועי אבטחת מידע בשנים 2018 - 2019, וכי הוועדה אישרה את תכנית העבודה לשנת 2020 בהתבסס על סקר הסיכונים שבוצע. ואולם, לא צוין בסיכום האם הוועדה דנה במרכיבים אחרים שהם בתחום אחריותה לפי הנחיית המסגרת, ובכלל זה בגיבוש מדדים כמותיים בעניין הגנת הסייבר, אשר באמצעותם ניתן יהיה לבחון ולמדוד את מידת היישום של הגנה זו בתום כל חציון.

המשרד בתשובתו ציין כי ביוני 2022 הוא מינה מנהלת מערכות מידע ראשית (מנמ"רית) חדשה למשרד ומינה אותה גם לתפקיד הממונה על הגנת הסייבר. המשרד הוסיף כי בשנת 2022 (לאחר הביקורת) הוא כינס פעמיים את ועדות ההיגוי לאבטחת מידע וסייבר, והיא עתידה להתכנס פעם נוספת לקראת מבדק מחודש של תקן ISO-27001 שהמשרד עתיד לעבור.

על המשרד להמשיך להקפיד על כינוסה כנדרש של ועדת היגוי סייבר - לכל הפחות פעם בחציון, ולוודא שהיא תדון בכלל הנושאים המצויים בתחומי אחריותה כפי שנקבע בהנחיית המסגרת.

הקצאת תקציב להגנת הסייבר

בהחלטת הממשלה 2443 בעניין הגנת סייבר נקבע כי על המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך, במסגרת סמכותם ואחריותם הקיימת, להסדיר את מבנה התקציב השנתי של משרדם באופן שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יוקצה להגנת הסייבר.

החלטת הממשלה באה לידי ביטוי גם בהנחיית יה"ב שבה נקבע, בעניין זה, כי יש להקצות משאבים ליישום דרישות תשתית הגנת הסייבר (לכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר).

עולה כי הנחיית יה"ב המבטאת את החלטת הממשלה 2443, בנוגע לתקצוב הגנת הסייבר מתוך תקצוב תחום טכנולוגיית המידע היא כללית, ואינה קובעת אילו מרכיבים נכללים ב"טכנולוגיות המידע" וב"הגנת הסייבר". עלה גם כי יה"ב אינה מנחה את משרד החינוך בנוגע לאופן יישום הדרישה שנקבעה בהחלטה, ואינה בודקת אם היא יושמה.

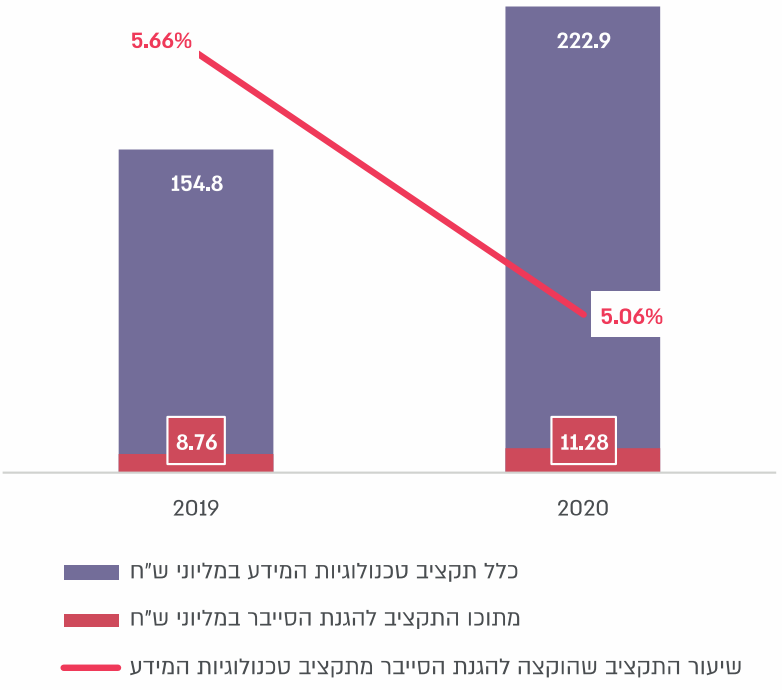
בתשובת יה"ב למשרד מבקר המדינה מאוגוסט 2022 (להלן - תשובת יה"ב) היא ציינה, כי כוח האדם העוסק בפועל בתחום אבטחת מידע כולל עובדים שנמנים עם צוותי אבטחת המידע וכן אחרים העובדים באגף טכנולוגיות המידע ואשר עוסקים בתחומים כמו תקשורת נתונים, פיתוח ומסדי נתונים (DB). על כן, לעיתים קשה לכמת את כלל ההוצאות בגין השימוש במשאבי ההון האנושי ולדעת למה לשייכן. יה"ב הוסיפה שמתבצעות פעולות בתחום הגנת הסייבר גם בנוגע למערכות שאינן מוגדרות בהכרח כמערכות אבטחת מידע. בשל הקושי להגדיר במדויק את המרכיבים הנכללים בתחום הגנת הסייבר, מקנה יה"ב למשרד גמישות בהגדרות אלו. בדיוני

ההנהלה ובישיבות ועדות היגוי שמתקיימים בנושא הגנת הסייבר מעלה יה"ב פערים, אם לדעתה אכן יש פערים, כדי לתת מענה עליהם ולקדם את הנושא.

משרד מבקר המדינה ממליץ ליה"ב להגדיר באופן ברור עבור משרדי הממשלה את המרכיבים שניתן להביאם בחשבון במסגרת תחום טכנולוגיית המידע ותחום הגנת הסייבר ולקבוע אילו מרכיבים הכרחי לכלול בהם; בהתאם לכך, יהיה על כל משרד לעקוב אחר יישום החלטת הממשלה והנחיית יה"ב בדבר הצורך להקצות תקציבים להגנת הסייבר.

בשנת 2019 הסתכם התקציב המקורי של מינהל תקשוב במשרד החינוך ב-169 מיליון ש"ח, סכום התקציב המאושר על שינוייו היה כ-344 מיליון ש"ח, והתקציב שבוצע בפועל היה כ-255 מיליון ש"ח[27]. משרד החינוך מסר לצוות הביקורת את הערכתו לתקציב שהוקצה בפועל לתחום טכנולוגיות המידע, וכמה מתוכו הושקע בתחום הגנת הסייבר (בכלל זה עלות כוח אדם ייעודי לנושא), כפי שמוצג בתרשים שלהלן.

תרשים 7: **חלוקת תקציב טכנולוגיות המידע במשרד החינוך, 2019 ו-2020 (במיליוני ש"ח) על פי נתוני משרד החינוך, בעיבוד משרד מבקר המדינה**



לרבות תקציב טכנולוגיות הגנת סייבר ועלות כוח אדם ייעודי שמוקצה לנושא.

27 על פי מידע שפורסם באתר "ביצוע תקציב מפורט לפי תקנות" של אגף החשב הכללי במשרד האוצר. https://www.gov.il/he/departments/publications/reports/budget-exec-publications

מהתרשים עולה שהמשרד לא עמד בהנחיה ולפיה יש להקצות לכל הפחות 8% מתקציב תחום טכנולוגיית המידע עבור הגנת הסייבר - בפועל שיעור התקציב הייעודי שהוקצה לכך בשנת 2019 היה כ-5.66%, ובשנת 2020 הוא פחת לכ-5.06%.

המשרד בתשובתו ציין, כי התקציב לשנת 2020 היה תקציב המשכי (שכן לא אושר תקציב מדינה לשנה זו), וכי בעקבות התפרצות מגפת הקורונה במרץ 2020 הוקצו תקציבים ייעודיים לטיפול בצרכים שהתעוררו בשל המגפה. עוד הוא ציין, כי בשנת 2022 הוא הקצה 19 מיליון ש"ח (ששיעורם כ-11% מתקציב מינהל תקשוב לפיתוח רכש והתקשרויות, לא כולל עלות כוח אדם בתחום) לאבטחת מידע וסייבר, וזאת בהתאם לתוכנית העבודה שגיבש מנהל אבטחת מידע וסייבר, לצורך צמצום הפערים הקיימים ולצורך הפעילות השוטפת והאתגרים שעמדו לפני המשרד. המשרד הוסיף שצוות עובדי אבטחת המידע הוגדל מחמישה עובדים בשנת 2019 לתשעה בשנת 2022.

בתשובת יה"ב היא ציינה, כי היא תומכת בעמדת משרד מבקר המדינה לגבי הצורך לעמוד בדרישת התקציב הייעודי להגנת הסייבר. יה"ב הוסיפה, כי מדד יה"ב, אשר מטרתו להציג את רמת החוסן של המשרד בהיבט הגנת הסייבר, מציג את העמידה בתקציב והוא אחד הפרמטרים הנכללים בתוכנית העבודה.

על משרד החינוך להקפיד לפעול בהתאם להחלטת הממשלה ולהנחיית יה"ב בנוגע לעמידה בתקציב הייעודי להגנת הסייבר, לקבוע תוכנית עבודה ולגבש מדדים שיאפשרו עמידה בדרישה זו. מומלץ כי יה"ב תעקוב אחר הקצאת תקציבי הסייבר ומימושם.

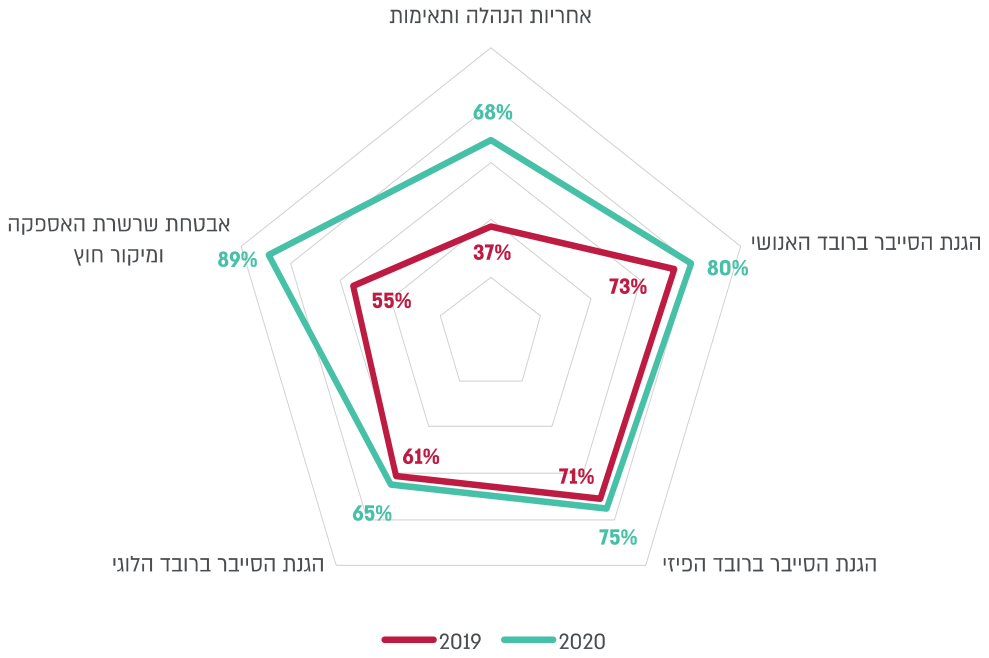
מבדק יה"ב לבקרות בתחום הגנת סייבר

במסגרת ביצוע תפקידה, גיבשה יה"ב סרגל בדיקה אחיד למשרדי הממשלה בתחום אבטחת המידע והגנת הסייבר ושמו מדד יה"ב (להלן - מבדק מדד יה"ב); המדד כולל יותר מ-200 בקרות המתבססות על תורת ההגנה בסייבר, על הנחיות יה"ב, על תקנות הגנת הפרטיות ועל תקן ISO-27001. משרד ממשלתי שמבצע את מבדק מדד יה"ב, אם בעצמו ואם באמצעות חברה חיצונית, מקבל דירוג של רמת הגנת הסייבר שלו על פי תרשים מדד יה"ב (ראו להלן).

יה"ב מסרה לצוות הביקורת כי אין לה הנחיה כתובה לעניין ביצוע מבדק מדד יה"ב, וכי כל משרד ממשלתי שמבצע סקר סיכונים או מחדש עמידה בתקן ISO-27001 מבצע את מבדק מדד יה"ב במסגרת התהליך, וזאת באמצעות חברות ייעוץ חיצוניות, וכי נציג מטעמה בודק בשיתוף עם המשרד את ממצאי הבדיקות.

ציון מדד יה"ב מבוסס על שקלול של חמישה רבדים של הגנה ואבטחה שביחד מייצגים את רמת הגנת הסייבר במשרד. טווח ציוני המדד הוא 1 - 5. בדוח מבדק מדד יה"ב משנת 2019 המדד של משרד החינוך היה 3, ובשנת 2020 - 4. התרשים שלהלן מציג את השיפור, ברמת ההגנה במשרד לפי חמשת רובדי ההגנה של מדד יה"ב כפי שעלו בדוחות המבדק:

תרשים 8: **רמות ההגנה במשרד לפי רובד, 2019 ו-2020**



על פי דוחות מדד יה"ב של משרד החינוך לשנת 2019 ולשנת 2020, בעיבוד משרד מבקר המדינה.

להלן השוואה בין דוחות מדד יה"ב של משרד החינוך לשנים 2019 ו-2020 לבין המצב בפועל בשנים אלו כפי שעלה בביקורת ופורט לעיל:

לוח 1: **השוואה בין דוחות מדד יה"ב לשנים 2019 ו-2020 לעומת ממצאי הביקורת**

הבקרה	שיעור היישום ע"פ מדד יה"ב 2019	שיעור היישום ע"פ מדד יה"ב 2020	הממצאים בפועל שעלו בביקורת
הקצאת תקציב ייעודי של 8% לפחות לתחום הגנת הסייבר.	100%	75%	הוקצו פחות מ 8% מהתקציב בשנת 2019.
כינוס ועדת היגוי סייבר פעמיים בשנה לפחות.			ועדת היגוי סייבר לא התכנסה פעמיים בשנה; ישיבתה האחרונה התקיימה בנובמבר 2019.
מסמך המדיניות יכלול פרק "הגנת הפרטיות" אשר ייתן מענה מלא לדרישות שבתקנות.	0%	100%	מסמך המדיניות אינו כולל פרק "הגנת הפרטיות", ואינו נותן מענה מלא על הדרישות שבתקנות.
בין המשימות שעל ועדת היגוי סייבר לבצע: לדון לפחות פעם בשנה במאגרי המידע ובמאגר מידע שחלה עליו רמת האבטחה הגבוהה - אחת לרבעון לפחות; לאשר בכל שנה את מדיניות אבטחת המידע והגנת הסייבר ולהקצות משאבים לצורך מימושה.	100%	100%	בדיון האחרון של הוועדה בנובמבר 2019 הוועדה לא דנה במאגרי המידע ולא עדכנה ואישרה את מסמך המדיניות.
גיבוש וניהול של המסמכים הנדרשים בתקנות הגנת הפרטיות.	0%	50%	במועד הביקורת סיים המשרד להכין מסמך הגדרות ל-5 (10%) מ-50 המאגרים הרשומים.

מהלוח עולים פערים בין מבדקי מדד יה"ב כפי שדיווח משרד החינוך לבין הממצאים שעלו בביקורת.

נוכח הפערים המוצגים בלוח מומלץ כי יה"ב תבחן את הסיבות לכך, וכי היא תנחה ותדריך את משרד החינוך בנוגע לאופן שבו יש לבצע את הבדיקה לפי מדד יה"ב ואת הרישום והתיעוד בדוח מדד יה"ב. עוד מומלץ כי יה"ב תבצע בקרה על מידת יישום הבקרות בפועל.

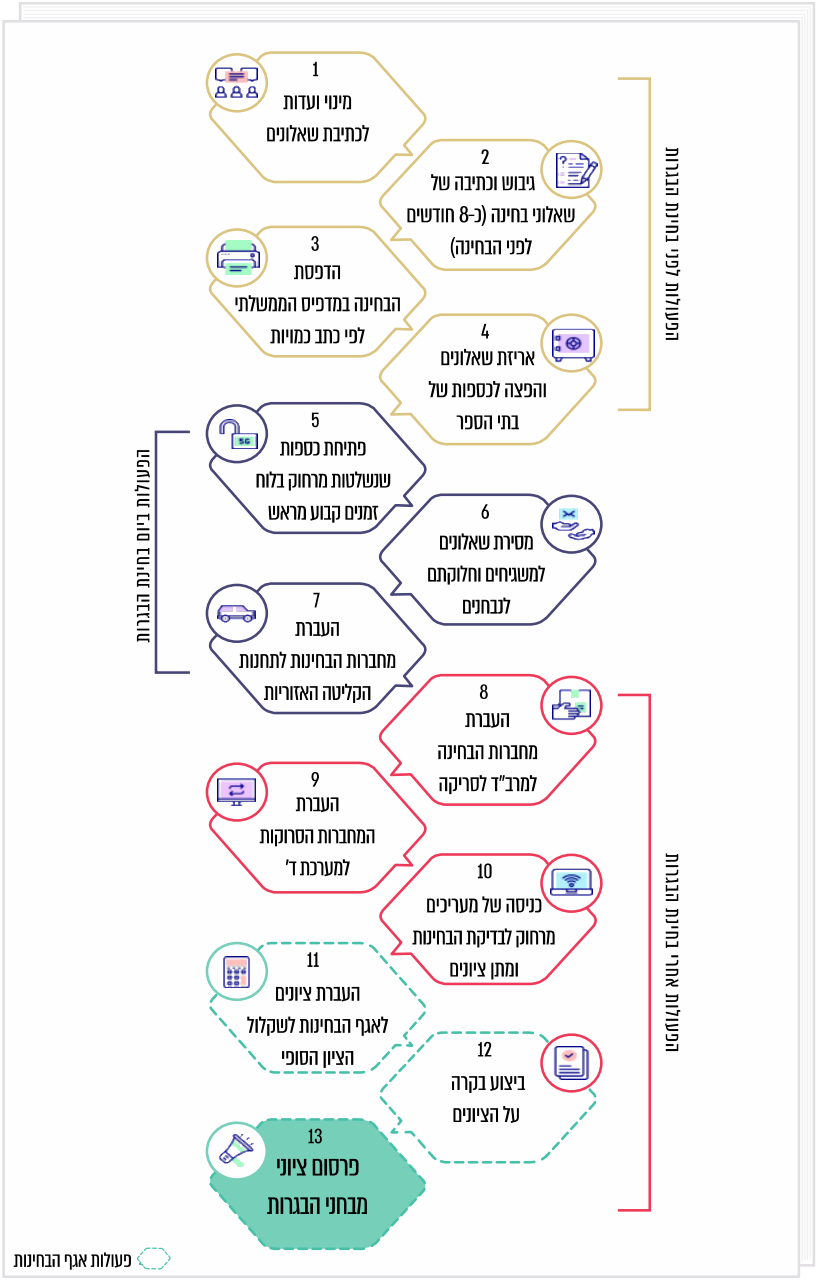
יה"ב ציינה בתשובתה, כי מדד יה"ב עודכן כדי שהתוצאות המתקבלות יהיו מדויקות יותר. עוד ציינה כי המדד מתבסס, בחלקו, על המענה של הגורם המקצועי במשרד, וכי עבור חלק מהבקרות שנכללות במסגרתו, נדרש לצרף אסמכתאות המתעדות את ביצוע הבקרה. יה"ב הוסיפה כי היא תחדד לפני הספקים את הנהלים וההנחיות ותדריך אותם בנוגע למתכונת הנכונה למילוי המדד.

אבני דרך עיקריות בתהליך בחינת בגרות

התהליך שתחילתו בגיבוש שאלון בחינת הבגרות וסיומו במסירת הציון לנבחן הוא תהליך מורכב שנמשך כשנה. מעורבים בו גורמים מתוך משרד החינוך ומחוצה לו, ובהם עשרות אלפי תלמידים ומורים. להלן תיאור אבני דרך עיקריות של התהליך:

גיבוש שאלוני בחינות הבגרות מתחיל כשמונה חודשים לפני מועד הבחינה. רוב השאלונים מודפסים במדפיס הממשלתי ומופצים לכספות פיזיות שבבתי הספר באמצעות חברות בלדרות. הכספות נשלטות מרחוק ונפתחות ביום הבחינה על פי לוחות זמנים קבועים מראש, שקבע אגף הבחינות. לאחר פתיחת הכספות שאלוני הבחינות נמסרים למשגיחים, ואלה מחלקים אותם לנבחנים. בסיום הבחינה אמורים משגיח ונציג של בית הספר להעביר את מחברות הבחינה של התלמידים לתחנות קליטה אזוריות, ותחנות אלה מעבירות את מחברות הבחינה לסריקה במרב"ד. בסיום הסריקה מחברות הבחינה הסרוקות מועברות למערכת המחשוב ד', ומעריכים הפועלים מרחוק מקבלים גישה אליה לצורך הערכת הבחינות ומתן ציונים. כל מחברת נבדקת על ידי שני מעריכים שונים לפחות. בתום תהליך ההערכה, מערך המרב"ד מבצע בקרה על הציונים. בסיום התהליך ציוני המעריכים שהוזנו במערכת ד' והציונים השנתיים (מגן) מועברים לאגף הבחינות, והוא משקלל את ציון הבחינה עם הציון השנתי (להלן - ציון המגן) של התלמידים. הדבר מבוצע במערכת ג'. לאחר בקרה שמבצע אגף הבחינות על הציונים, הוא מפרסם אותם לבתי הספר ולתלמידים. להלן תרשים שמתאר את גלגולה של בחינת בגרות.

תרשים 9: **גלגולה של בחינת בגרות (לא כולל בחינות מתוקשבות)**



על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

אבטחת המידע של ציוני הבגרות

למשרד החינוך יותר מ-200 מערכות מידע המשמשות אותו לניהול תהליכי העבודה הפנים-משרדיים וכן כדי לתת שירות למשתמשים חיצוניים. משתמשי המערכות הם כ-3,500 עובדי המשרד, כ-5,000 בתי ספר, כ-190,000 עובדי הוראה. כמו כן, משתמשים חיצוניים, מיליוני תלמידים והורים, רשתות חינוך, ספקים וזכיינים.

מערכות המידע שבאמצעותן משרד החינוך מנהל ומתפעל את בחינות הבגרות ונסקרו בביקורת פרוסות על פני שלוש רשתות עיקריות נפרדות. הרשתות מוגנות באמצעות רכיבי אבטחה כמפורט בהמשך:

1. רשת א', שהשרתים שלה מותקנים בחוות השרתים של חברה א' (להלן - רשת א').
2. רשת ב' , שהשרתים שלה מותקנים בחוות השרתים של חברה ב'.
3. רשת ג' שהשרתים שלה מותקנים במשרדים השייכים למשרד החינוך, ואשר מתופעלים על ידי החברה החיצונית. רשת ג' פועלת, בין היתר, בסביבה ייעודית ברשת א'.

ציוני הבגרות - מערכות מידע עיקריות

ציון הבגרות הסופי הוא ציון משוקלל של שלושה ציונים עיקריים: ציון מגן פנים-בית-ספרי אשר בתי הספר מדווחים עליו למשרד החינוך, וציוני שני מעריכים שונים שבודקים את מחברות הבחינה של התלמידים[28]:

ציוני המגן - הדיווח על ציוני המגן מתבצע באמצעות מערכת ב' של משרד החינוך או באמצעות מערכות ניהול בית ספריות אחרות של ספקים חיצוניים שקיבלו אישור לכך ממשרד החינוך (להלן - תוכנות אחרות לניהול פדגוגי);

ציוני הבחינה - בדיקת מחברות הבחינה ומתן הציונים מתבצעים באמצעות גישה מרחוק למערכת ד';

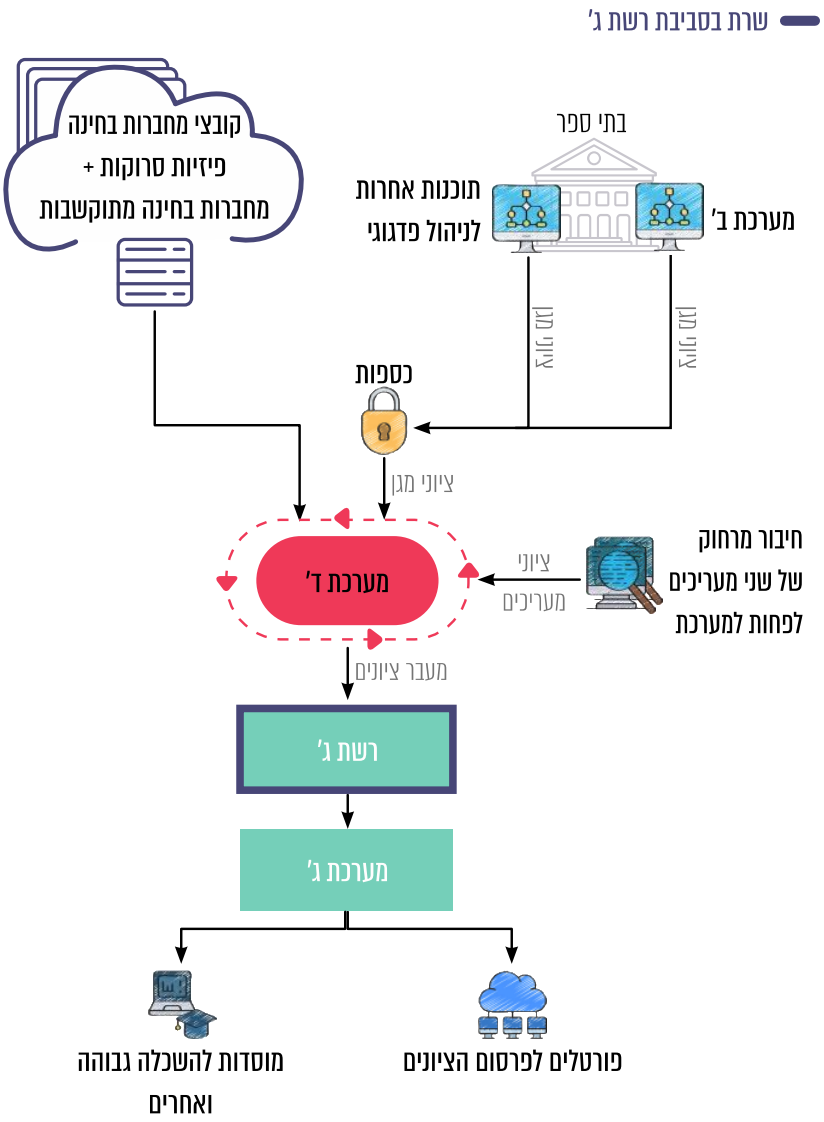
הציון הסופי - שקלול הציון הסופי נעשה במערכת מחשב ייעודית;

הפצת הציונים לבתי הספר, לתלמידים ולגורמים אחרים נעשית באמצעות אתרי המרשתת של המשרד (להלן - הפורטלים). חלק ממערכות המידע הללו פועלות ברשת א', חלקן ברשת ב' של משרד החינוך וחלק מהתוכנות האחרות לניהול פדגוגי פועלות ברשתות חיצוניות אחרות.

28 לעיתים משרד החינוך מעביר מחברת בחינה לבדיקה של מעריך שלישי, בדרך כלל בשל פער בציון בין שני המעריכים שבדקו את מחברת הבחינה.

תרשים 10 להלן מציג את מערכות המידע העיקריות שתומכות בתהליך ואת זרימת המידע בין המערכות:

תרשים 10: **מערכות המידע העיקריות הרלוונטיות לניהול בחינות הבגרות**



על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

אבטחת המידע ברשת א' - חוות המחשבים של חברה א'

רשת א', המופעלת מחוות השרתים של חברה א', משרתת את כל המשתמשים שאינם עובדי משרד החינוך, ובהם בתי הספר, עובדי ההוראה, התלמידים, ההורים והספקים, היא נגישה גם לעובדי המשרד על פי צורכיהם. חברה א' מספקת למשרד החינוך שירותי תשתיות מרכזיות - Infrastructure As A Service (IAAS), המבוססים על טכנולוגיה של שרתים וירטואליים. בין השירותים: אירוח של השרתים הפיזיים והווירטואליים, התקשורת, הניתוב ואבטחת המידע בגישה לרשת זו. חברה א', בתיאום עם משרד החינוך, היא האחראית להקמה, להתקנה ולניהול של השרתים והרכיבים ברשת זו, להגדרות האבטחה בהם, לניהול מערך העדכונים ועוד. משרד החינוך והחברה החיצונית, שמפעילה את מערך המרב"ד, אחראים להתקנה ולניהול של מערכות המידע ושל מאגרי המידע (בסיסי הנתונים) ברשת.

רשת א' כוללת כ-1,000 שרתים וירטואליים. הרשת נחלקת לכמה סביבות לוגיות, ובהן כמה סביבות לוגיות נפרדות שבהן פועלות מערכות מידע שמשמשות את פעילות בחינות הבגרות.

ברשת א' מותקנים כמה רכיבי ניהול ואבטחה, ובהם מערכת לניהול הרשאות כלל המשתמשים שירותי אנטי-וירוס (הגנה מפני פוגענים), מערכות הגנה - רכיבי חומרה או תוכנה שמטרתם להגן על רשתות מחשוב - ניטור וחסימה של גישה לא מאובטחת לרשת מאובטחת. וכן רכיבי ניהול ואבטחה נוספים.

עלה שרכיב מסוים וגם ציוד הרשת ואבטחת המידע, הנמצא על פי חוזה ההתקשרות בטיפולה של חברה א', אינו נגיש באופן ישיר למשרד. כל אימת שמתעורר במשרד החינוך צורך לטפל בהיבט הנוגע לציוד הרשת ולאבטחת המידע, עליו לפנות לחברה א', באמצעות עובדים מסוימים המורשים לכך, כדי להנחות את החברה ולבקש ממנה לבצע עבורו את הפעולות הנדרשות. הפנייה לחברה א' מתבצעת באמצעות פתיחת קריאה במערכת ייעודית המנהלת את הפניות עבור המשרד והחברה (להלן - מערכת ניהול הקריאות).

ביקורת על רשומות תיעוד הפעולות: בהנחיית יה"ב "הגנת התשתיות הוירטואליות"[29] נקבע כי על המשרד לבצע מפעם לפעם ביקורת על רשומות תיעוד הפעולות (להלן - רשומות ה- log) שנעשות במערכות של הסביבות הווירטואליות, הכוללות מערכות ניהול, מתגים וירטואליים, מערכות הגנה פיזיות ווירטואליות ומערכות הגנה אחרות הפועלות במשרד. עוד נקבע כי אחת לרבעון יש לבצע ביקורת על רשומות ה-log של פעילות משתמשים בעלי הרשאות גבוהות באותן מערכות, ובכלל זה ניסיונות גישה כושלים.

אשר לאבטחת המידע של רשת א', עלה בביקורת כלהלן:

29 הנחיה מספר 5.14 מתאריך 15.11.2017, תאריך עדכון 25.02.2019, גרסה 1.1.

- משרד החינוך אינו מבקש לקבל אסמכתאות המתעדות את אופן הטיפול בקריאותיו[30];
- המשרד אינו דורש לקבל מהחברה קובץ log שיוכל לאפשר לו לבצע בקרה על רשומות המתעדות את הפעולות במערכות, כנדרש בהנחיית יה"ב בעניין "הגנת התשתיות הוירטואליות".
- המשרד אינו מבקש לקבל מחברה א' דוח עיתי המפרט את ההגדרות והכללים שנקבעו לרכיב אבטחת מידע מסוים, שהוא כאמור קריטי להגנת המערכת, או של שאר ציוד הרשת ואבטחת המידע שבשליטתה, זאת כדי לוודא שההגדרות והכללים בנוגע לאבטחת המידע עומדים בדרישות המתחייבות מחוזה ההתקשרות, מצרכיו ומהנחיות יה"ב שחלות עליו.
- מערכת ה', שאמורה לאפשר ניטור של שינויים בכללי רכיב הגנה מסוים ובקרה עליהם, הוטמעה רק מול רכיב הגנה מסוים שבשליטת המשרד ומותקנות בין רשת א' לבין רשת ב' ולא הוטמעה מול רכיבי הגנה החיצוניים האחרים שבשליטת חברה א'.

מומלץ שמשרד החינוך ידרוש לקבל מחברה א' אסמכתאות המתעדות את הפעולות שביצעה בהמשך לקריאות שהתקבלו ושבהן היא טיפלה. עוד מומלץ שהמשרד ידרוש לקבל מהחברה דוחות ניטור ובקרה, דוחות של כללי רכיב הגנה מסוים והגדרות הציוד שבאחריות החברה. כמו כן, מומלץ שהמשרד ישקול את האפשרות להטמיע אמצעי בקרה מסוים גם על האבטחה של רכיבים שנמצאים בשליטת חברה א'.

מומלץ גם שיה"ב תבהיר בהנחיותיה, ובכלל זה בהנחיה בעניין הגנת התשתיות הווירטואליות, את הפעולות הנדרשות מהמשרדים בכל הנוגע לפעולות בתחום אבטחת מידע שהן באחריות המשרדים, אך בפועל מבוצעות על ידי חברות פרטיות שעימן התקשרו המשרדים. נוסף על כך, מומלץ שההנחיה תבהיר שעל נושא זה לבוא לידי ביטוי בחוזי ההתקשרות.

בתשובת המשרד, הוא ציין כי ימשיך לפרוס ולחבר למערכת ה' את כלל רכיבי אבטחת המידע. עוד מסר כי יבקש דוחות תקופתיים על פעילות מערכת ניהול הקריאות.

בתשובת יה"ב היא ציינה, כי היא מקבלת את הצעת משרד מבקר המדינה, וכי תעדכן את הנחיית יה"ב "הגנת התשתיות הוירטואליות" בנוגע לאחריות המשרד בחוזי התקשרות עם ספקים חיצוניים וכן היא תתייחס לעניין זה בהנחיית יה"ב בנושא שרשרת האספקה.

חיבור רשת א' ל-SOC הממשלתי: מרכז השליטה והבקרה הממשלתי למול איומי סייבר - Security Operation Center (להלן - ה-SOC הממשלתי) - הוקם מכוח החלטת הממשלה 2443 בעניין הגנת הסייבר, והוא עוסק בגיבוש תמונת מצב ממשלתית שוטפת בהיבטי הגנת הסייבר ומתן מענה לטיפול באירועי סייבר במשרדי הממשלה.

על פי החלטת הממשלה 2443 והנחיית יה"ב "הנחיית מסגרת להגנת הסייבר בממשלה", על משרדי הממשלה לדווח ל-SOC הממשלתי על אירועי סייבר. בהנחיה נוספת של יה"ב "דיווח ל-

30 מחברה א' נמסר שככלל היא אינה שולחת אסמכתאות המתעדות את הפעולות שבוצעו כנוהג מוסכם אך לעיתים, אם פעולה מסוימת אינה מביאה לתוצאה הרצויה, כחלק מתחקור הסיבה לכך נמסרות אסמכתאות המתעדות את הפעולה שבוצעה.

SOC הממשלתי על אירועי סייבר", נקבע כי אחד היעדים של ה-SOC הממשלתי הוא איתור וזיהוי של אירועי סייבר המתרחשים במשרדי הממשלה וביחידות הסמך שלהם.

עלה שמשרד החינוך חיבר את רשת ב' שלו למערכות הניטור של ה-SOC הממשלתי, באופן שמאפשר איתור וזיהוי של אירועי סייבר, אולם הוא לא חיבר אליהן את רשת א'.

משרד מבקר המדינה ממליץ למשרד החינוך להשלים את חיבור רשת א' ל-SOC הממשלתי כדי לתת מענה לחוסר הניטור הקיים בתחום האבטחה.

בתשובת המשרד הוא ציין, שבמסגרת תוכנית העבודה לחיבור מערכות המידע שלו ל-SOC הממשלתי, הותקנו הרכיבים התומכים בקבלת נתונים ממערכות ההגנה של רשת א'; הוא הוסיף שהוא מאפיין את האירועים שמתרחשים במערכות אלו, לרבות אלו של רכיב אבטחת מידע מסוים ושל התשתיות הווירטואליות ושבנוגע אליהם צריך להתקבל דיווח.

בתשובת יה"ב היא ציינה, כי המדיניות שלה היא לחבר מגוון מקורות רחב ככל האפשר ל-SOC הממשלתי, וכי היא ערוכה לנטר את רשת א'.

אבטחת המידע ברשת ג'

במרב"ד מנוהל התהליך הנוגע למחברות הבחינה ששימשו את הנבחנים לצורך המענה על שאלוני הבחינה. בשנת 2012 זכתה החברה החיצונית במכרז של משרד החינוך לארגון ולהפעלה של מערך המרב"ד, באמצעות ציוד פיזי ומחשובי, ועל מערכות מידע ותשתיות שכולן של משרד החינוך, ומאתר השייך למשרד החינוך (להלן - המכרז להפעלת מערך המרב"ד) [31]. בעקבות הזכייה במכרז, חתמה החברה החיצונית על חוזה התקשרות[32] מול מדינת ישראל באמצעות ממשלת ישראל המיוצגת על ידי אגף א' במשרד החינוך וחשב משרד החינוך (להלן - חוזה ההתקשרות). על פי הנקבע במכרז להפעלת מערך המרב"ד, המהווה חלק בלתי נפרד מחוזה ההתקשרות, החברה הזוכה אחראית לתהליך הלוגיסטי של איסוף מחברות הבחינה; סריקת המחברות; תפעול בדיקת הבחינות והערכתן; פיתוח, הפעלה ותחזוקה של מערכת ד'; עיבוד הנתונים בה והעברת ציוני הבחינה לאגף הבחינות שבמשרד החינוך. החברה אחראית גם להעסקת המעריכים והבוחנים. במסגרת זו על החברה לוודא שכל המחברות התקבלו, נסרקו ונקלטו במערכת, שכולן הוערכו וניתנו להן ציונים, עליה לאתר שגיאות, חסרים ושיבושים.

חוק הגנת הפרטיות מגדיר "מחזיק, לעניין מאגר מידע" כ"מי שמצוי ברשותו מאגר כדרך קבע והוא רשאי לעשות בו שימוש"[33]. החוק קובע כי האחריות לאבטחת המידע במאגר המידע מוטלת גם על המחזיק. תקנות הגנת הפרטיות אבטחת מידע קובעות כי החובות שבתקנות שחלות על בעל מאגר מידע יחולו גם על המחזיק (למעט התקנה לעניין מסמך הגדרות המאגר והתקנה לעניין מיקור חוץ) בשינויים המחויבים, ולפי העניין.

31 מכרז 29/10.2011: ארגון והפעלה של מרכז בדיקות בחינות (מרב"ד) וניהול מאגר מעריכים ובוחנים.

32 חוזה (בעקבות מכרז) שנחתם במקור ביום 28.8.2012 והוארך ממעת לעת. במרץ 2022 נחתם הסכם עם חברה אחרת שזכתה במכרז.

33 חוק הגנת הפרטיות. כמו כן, ראו, במונחון הפרטיות שפרסמה הרשות להגנת הפרטיות לגבי מחזיק "הישות אשר מעבדת את המידע עבור בעל המאגר, קרי ספק מיקור חוץ".

עוד נקבע בתקנות כי בעל המאגר ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני (שעימו התקשר לצורך קבלת שירות הכרוך במתן גישה למאגר המידע) בהוראות התקנות והסכם ההתקשרות שביניהם, בהיקף הנדרש בשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות.

לפי חוזה ההתקשרות עם החברה החיצונית, הוטלה עליה האחריות לרישום מאגר המידע, החזקתו והשימוש בו בהתאם לחוק. מכאן שהחברה החיצונית היא המחזיקה במאגר המידע על פי חוק הגנת הפרטיות ותקנות הגנת הפרטיות אבטחת מידע והנקבע בהם חל עליה. היא גם "גורם חיצוני" שעימו התקשר המשרד לקבלת שירות הכרוך במתן גישה למאגר המידע ולכן על המשרד לוודא שהחברה תעמוד בהוראות המחייבות.

רשת ג' פרוסה בשלושה אתרים מרכזיים. שניים מהם נמצאים ברשת א' בחברה א', והשלישי במשרדים השייכים למשרד החינוך.

שימוש במוצרים שהיצרן אינו תומך בהם והטמעת רכיבי אבטחת מידע במרב"ד: מפעם לפעם נוהגות חברות המפתחות מערכות ורכיבי מחשוב לעדכן את גרסאות המוצרים שלהן. לעיתים הן גם מפסיקות לתמוך בגרסאות הישנות. עדכון גרסה נעשה מסיבות שונות, ובהן בשל חולשות אבטחה שהחברות זיהו במוצרים שלהן. דבר העדכון מתפרסם בקרב אנשי המקצוע שבתחום, בקהילות ייעודיות ובקרב הצרכנים, וזאת על מנת להביא לידיעתם את דבר החולשה שהתגלתה ולהציע להם להתקין את הגרסה המעודכנת. פרסומים מעין אלו יכולים לשמש זרזים לגורמים עוינים, לפצחנים ולאחרים שיש להם עניין לפגוע במערכות, והם אף ממקדים את הפגיעה באותן חולשות שהתגלו.

תקנות הגנת הפרטיות אבטחת מידע בעניין ניהול מאובטח ומעודכן של מערכות קובעות כי לא ייעשה שימוש במערכות שהיצרן אינו תומך בהיבטי האבטחה שלהן, אלא אם כן ניתן מענה אבטחתי מתאים לכך. עוד קובעות התקנות כי בעל המאגר לא יחבר את מערכות המאגר למרשתת או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

הנחיית יה"ב "מדיניות עדכון מערכות מידע בממשלה" קובעת כי אין להשתמש בגרסאות מערכת, שהגיעו לסיום מחזור חיים ואשר היצרן כבר אינו תומך בהן. בהנחיית יה"ב "הקשחת Domain Controller" נקבע כי גרסת מערכת הפעלה מסוימת אינה נתמכת עוד, ולכן יש להימנע משימוש בה.

בהנחיית המסגרת נקבע כי איתור הניסיונות לביצוע פעולות לא מורשות ברשת המשרד יתמקד בשני מישורים, ובהם, באיתור בזמן אמת של פעילויות לא מורשות ברשת ובשרתי המשרד על ידי שימוש במוצרי אבטחת מידע לאיתור חדירה (Intrusion Detection) ובמערכת לניהול אירועי אבטחת המידע ונתוני אבטחת המידע (Security Information and Event Management, להלן - מערכת SIEM).

בביקורת עלה כלהלן:

- רשת ג' מוגנת על ידי גרסה מיושנת של רכיב הגנה מסוים, שהחל בספטמבר 2019 היצרן הפסיק לתמוך בה.

- ברשת עלו פערים בנוגע להתקנת רכיבים מסוימים לאבטחת מידע.
- במרץ 2021 פנתה החברה החיצונית למשרד החינוך בדרישה לרכוש רכיב הגנה מסוים שהיצרן תומך בו. באוקטובר 2021 נרכש רכיב ההגנה, אך נכון לנובמבר 2021 הוא לא הוטמע באופן מלא.
- בינואר 2020 היצרן הפסיק לתמוך במערכת ההפעלה של שרתים מסוג מסוים שמשמשים, בין היתר, את רשת ג'; בכלל זה הופסקה התמיכה בשרתים מסוימים להפעלת מערך בחינות הבגרות.
- יש מערכת המנטרת את הביצועים של רשת ג' ואת השרתים של רשת זו; גישת העובדים מאותה רשת למרשתת מתבצעת באמצעות מערכות משרד החינוך ומנוטרת על ידי ה-SOC הממשלתי; כמו כן, חברה א' מספקת שירותי ניטור אבטחתי לחלקים שבאחריותה ברשת א'; עם זאת, לרשת ג' אין רכיב שמבצע בקרה מסוימת כפי שהומלץ בהנחיית המסגרת.

היעדר בקרה מסוימת מלאה ומעודכנת של רשת ג' עלול לאפשר לתוקף לפעול בתוכה באופן הנסתר ממנהלי המערכת; השימוש של משרד החינוך והחברה החיצונית במוצרי אבטחת מידע ישנים ובשרתים שהיצרן אינו תומך בהם מבלי שניתן מענה אבטחתי מתאים, אינו מתיישב עם דרישת תקנות הגנת הפרטיות אבטחת מידע והנחיות יה"ב. משמע שיש חולשות שלא יאפשרו מענה מלא במקרה של תקיפה של המערכות.

בתשובת המשרד הוא ציין, כי שדרוג מערכת ההפעלה של השרתים ברשת ג' נמצא בשלבים אחרונים, ובמסגרת זו הוקמו סביבות דמה מסוימות. כמו כן, הוקם שרת שישמש תבנית להחלפת התשתית של רשת א', וכי התקבל והותקן רישוי לשרתי רשת ג'.

על משרד החינוך לקדם את סיום ההטמעה של הגרסה המעודכנת של תוכנת ההגנה ברשת ג' ולהשלים את שדרוג מערכות ההפעלה של שרתי רשת ג'. מומלץ שמשרד החינוך ידרוש מחברות המפעילות את מערך המרב"ד עבורו להטמיע את מערכות אבטחת המידע החסרות. מומלץ גם שהמשרד יפעל להקמת יכולת בקרה מסוימת ויגדיר התרעות שיאפשרו לאתר סיכוני פגיעה של הרשת, וכן מומלץ להשלים את הפער ביכולת הניטור.

הקשחת שרתים ועמדות קצה במערך המרב"ד: בתורת ההגנה בסייבר לארגון נקבע שעל הארגון להגדיר דרישות הקשחה למערכותיו ולתעד את הדרישות במסגרת-על שתשמש בסיס לכתיבת נוהלי הקשחה. כמו כן נקבע כי על הארגון להגדיר נוהלי הקשחה לכל סוג מערכת ושרת על בסיס פרקטיקות מקובלות, ובין השאר: כיבוי שירותים לא נחוצים, חסימה של התקנת תוכנה על ידי משתמשים לא מורשים.

בהנחיית יה"ב "הקשחת עמדות קצה" נקבעו פעולות ההקשחה שיש לבצע בעמדות קצה (כגון הטמעת מנגנון שמגביל הרצת תוכנות על עמדת קצה ושולט בהרצתן). בהנחיית יה"ב "הקשחת Domain Controller" נקבע כי יש לצמצם ככל הניתן את מתן הרשאות הגישה לשרת Domain Controller באופן שיינתנו הרשאות לתפעול בלבד, וזאת לקבוצת מורשים מצומצמת ומוגדרת.

בביקורת עלה כי משרד החינוך והחברה החיצונית לא גיבשו נוהל להקשחת שרתים במערך המרב"ד כפי שהומלץ בתורת ההגנה בסייבר לארגון.

בסקר הסיכונים שביצעה החברה החיצונית ביוני 2021 בנוגע לרשת ג' (להלן - סקר סיכונים לרשת ג') נמצא, כי עמדות הקצה אינן מוקשחות מספיק וקבוצת מנהלי הדומיין רחבה מדי.

בתשובתו מסר משרד החינוך, כי נכון למועד תשובתו משתמשים בעמדות הקצה אינם יכולים להריץ תוכנות ללא הגבלה אם הן אינן מותקנות, וכי במרבית עמדות הקצה אין כלל גישה למרשתת ואין בהן גישה לחיבור מסוג "USB" (Universal Serial Bus). המשרד הוסיף כי למשתמשים אין הרשאת מנהל (ADMIN) על אותן עמדות.

משרד מבקר המדינה ממליץ למשרד החינוך לגבש נוהל הקשחה לכל סוג מערכת, תחנת קצה ושרת אשר תואם את תורת ההגנה בסייבר והנחיות יה"ב, לדרוש מחברות המפעילות את מערך המרב"ד עבורו לפעול לפיו. עוד מומלץ שהמשרד ינקוט אמצעי בקרה ופיקוח לעניין יישום דרישות ההקשחה.

עוד מומלץ כי משרד החינוך ישלים בחינה של מערך ההרשאות בכדי לוודא, בין היתר, כי גם למשתמשים שלהם אין הרשאת מנהל (ADMIN) על אותן עמדות, אין הרשאת התקנה שלא לצורך.

ביצוע סגמנטציה בשרתי רשת ג': בהנחיית המסגרת הומלץ על חלוקה מקובלת של הסביבה, ובין היתר, על הפרדה בין רשת הייצור (הרשת התפעולית שבה מותקנות ופועלות מערכות המידע בגרסתן הסופית והמאושרת) לבין רשת הבדיקות והפיתוח (להלן - רשת הבדיקות) שבה מתבצעים תהליכי הפיתוח והבדיקות של המערכות לפני התקנתן ברשת הייצור.

בביקורת עלה כי שרת א' ושרתי ב' אינם מופרדים; הדבר מקנה לעובדים מסוימים גישה לשרתי ב' אף שלא אמורה להיות להם גישה כזו. עוד עלה כי בשרת א' נשמר עותק של מסד נתונים מסוים, והוא מונגש למשתמשים מורשים מסוימים; יוצא כי לאותם משתמשים יש גישה גם למאגר אף שאינם מורשים לכך. עוד עלה כי הפעולות המתבצעות בשרת א' אינן מנוטרות.

מומלץ למשרד החינוך לפעול לביצוע הפרדה בין שרת א' לשרתי ב'. מומלץ גם שבשרת א' לא ייעשה שימוש במסד הנתונים המלא והעדכני של הנתונים.

ביצוע סקרי סיכונים ומבדקי חדירות: כאמור, משרד החינוך כבעל מאגרי מידע הכוללים מידע רגיש על תלמידים ועובדים, ושהעתק שלהם נשמר במערכת ד'[34], נדרש לרמת האבטחה הגבוהה ביותר לפי התקנות, ובשל כך עליו לבצע סקר סיכונים ומבדק חדירות בנוגע למערכות המידע של אותם מאגרי המידע אחת ל-18 חודשים[35].

34 מאגר מידע "נבחני הבגרות" שמספרו 980046729, ומאגר מידע "ציוני הבגרות" שמספרו 990057652.

35 ראו תקנה 5(5) ותקנה 5(ד).

עלה, כי משרד החינוך, לא ביצע סקר סיכונים בנוגע לרשת ג' או מבדק חדירות למערכת ד' בשלוש השנים שקדמו למאי 2021, בין בעצמו, ובין באמצעות חברות המפעילות את מערך המרב"ד עבורו. וכי במהלך הביקורת ובעקבותיה, במאי 2021, ביצעה החברה החיצונית[36], מבדק חדירות לאתרים החיצוניים ולסביבה ו' (להלן - מבדק חדירות סביבה ו'), כמו כן, ביוני 2021, היא ביצעה סקר סיכונים לרשת ג'.

במבדק החדירות סביבה ו' משנת 2021 נמצא שהסיכון לפגיעה באתרים החיצוניים ולעקיפת מנגנוני ההגנה וההפרדה הפנימיים היה קטן. עם זאת, עלו חמישה ממצאים שכללו: ממצא קריטי אחד; ממצא ברמת חומרה גבוהה; וממצא ברמת חומרה בינונית.

מממצאי סקר הסיכונים רשת ג' משנת 2021 עלה שנשקף סיכון גבוה לרשת, שכן 13 מ-21 הממצאים שעלו היו ברמת חומרה גבוהה, ושישה ברמת חומרה בינונית. למשל: כללי רכיב אבטחת מידע מסוים אינם מוקשחים דיים; קבוצות מינהלני רשת (Admins) היו מתירניות מדי; בחלק מעמדות הקצה אין מערכת אנטי-וירוס מעודכנת; וגרסאות מערכות מסוימות אינן מעודכנות.

מומלץ שמשרד החינוך ידרוש שסקר הסיכונים והמבדקים יבוצעו במועדים ובתדירות הנדרשים ועל ידי גורם מקצועי שיהיה בלתי תלוי. עוד מומלץ כי המשרד יוודא כי הממצאים שעלו בסקר הסיכונים רשת ג' ובמבדק החדירה לסביבה ו' משנת 2021 יתוקנו.

עמידה בתקנות הגנת הפרטיות: כאמור, תקנות הגנת הפרטיות אבטחת מידע[37] קובעות כי החובות החלות על בעל המאגר יחולו גם על מנהל המאגר וגם על המחזיק בו בשינויים המחויבים ולפי העניין. במכתב להפעלת מערך המרב"ד, שקדם למועד התקנת התקנות, נכתב כי האחריות לרישום המאגר, להחזקתו ולשימוש בו על פי חוק הגנת הפרטיות תחול על החברה.

בביקורת עלה, כי אף שתקנות הגנת הפרטיות נכנסו לתוקפן בשנת 2018, משרד החינוך לא פעל להבטיח כי החברה החיצונית תבצע בדיקה באשר לעמידתה בדרישות התקנות, סקרי סיכונים ומבדקי חדירה במועד, תשתמש רק במוצרים שנתמכים על ידי היצרן, ותהיה בעלת מערכות אבטחת מידע מסוימות.

מומלץ שמשרד החינוך יפעל להבטיח כי החברות המפעילות את מערך המרב"ד עבורו, במסגרת ההתקשרות עמן, יעמדו בכל החובות שחלות עליהן בחוק הגנת הפרטיות ובתקנות הגנת הפרטיות אבטחת מידע.

הסמכה לתקן ISO-27001: בהנחיית יה"ב "שרשרת האספקה" נקבע, כי על "ספק מהותי"[38] של משרד ממשלתי לעמוד בתקן אבטחת מידע ארגוני ממשפחת תקן ישראלי ISO-27001. החברה החיצונית היא ספק של משרד החינוך ומספקת, בין השאר, שירותי מחשוב, אחסון מידע והעברת מידע, ועל כן היא נחשבת לספק מהותי. גם בחוזה ההתקשרות נקבע כי על החברה

36 באמצעות חברה בת שלה.

37 תקנה 19(א).

38 ספק מהותי/קריטי - ספק המספק שירותים, כגון שירותי תמיכה או תחזוקה למערכות מידע, שירותי אחסון של נתונים רגישים מחוץ למשרד ושירותי מיקור חוץ טכנולוגיים, או במקרה בו פגיעה בספק עלולה לגרום לנזק מהותי עבור המשרד.

החיצונית לקבל תו תקן ממשפחת תקני ISO בתוך חצי שנה, אחרי ביצוע מבדקים ועדכון נהלים כנדרש. בשנת 2020 ביצעה החברה החיצונית מבדק הסמכה לתקן ISO-27001. יצוין כי לחברה יש עיסוקים ופעילויות נוסף על פעילות מערך המרב"ד.

בביקורת עלה, שמבדק ההסמכה של החברה החיצונית לעמידה בתקן ISO-27001 לא כלל את פעילות מערך המרב"ד שהיא מבצעת עבור משרד החינוך. עוד עלה שהחברה ביצעה את מבדק ההסמכה בהתייחס לסביבת מחשוב שהיא אחרת ונפרדת מזו של סביבת המחשוב של מערך המרב"ד.

מומלץ כי משרד החינוך יפעל להבטיח כי החברות המפעילות את מערך המרב"ד עבורו, שהן "ספק מהותי" שלו, יעמדו בתקן ISO-27001.

גיבוי ושחזור של נתונים: תקנות הגנת הפרטיות אבטחת מידע קובעות כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל מאגר המידע נהלים לביצוע גיבוי, וכן נהלים להבטחת שחזור הנתונים, ובלבד שביצוע השחזור יהיה באישור מנהל המאגר.

הנחיית המסגרת והנחיית "גיבוי ושחזור מידע" קובעות כי יש לגבש תוכנית להמשכיות תפקודית (BCP) אשר תכלול גם תוכנית להתאוששות מאסון (Disaster Recovery Plan), המבוססת על הערכת סיכונים נאותה ומפרטת את כלל האמצעים שיש לנקוט בהתרחש אירוע חירום, המסכן את פעילותו התקינה של המשרד. עוד נקבע בהנחיית "גיבוי ושחזור מידע" כי יש לבצע תרגילי שחזור תקופתיים, וכי לפני הוצאתו של עותק הגיבויים אל מחוץ לאתר הראשי או אתר ה- DR יש להצפינו.

בביקורת עלה כי המשרד והחברה החיצונית לא קבעו נוהל הנוגע לגיבוי ולשחזור של מערכת ד', ולא קבעו תוכנית המשכיות עסקית - BCP לפעילות מערך המרב"ד. עוד עלה כי עותק של הגיבויים נשמר ללא הצפנה ברשת א' וכן ברשת ג'. החברה החיצונית מסרה לצוות הביקורת כי בשנת 2021 בוצע תרגיל שחזור מגיבוי למערכת ד'.

על משרד החינוך לקבוע נהלים לנושא הגיבוי והשחזור ולנושא ההמשכיות העסקית - BCP במרב"ד, ועל המשרד לוודא כי החברות המפעילות את מערך המרב"ד עבורו פועלות לפיהם ולפי הנחיות יה"ב.

אבטחת המידע במערכת ד'

למערכת ד' נטענים קובצי מחברות הבחינה הסרוקות וקובצי מחברות הבחינה המתוקשבות. הגישה למערכת מוקנית, באמצעות המרשתת, לכ-4,000 מעריכים חיצוניים אשר בודקים את מחברות הבחינות ומזינים עבורן ציונים. למערכת ד' נטענים גם כל ציוני המגן של התלמידים שהזינו בתי הספר במערכות השונות. כל הציונים (ציוני מעריכים ומגן) נשמרים ב-DB של מערכת ד'. לאחר סיום תהליך ההערכה וביצוע תהליכי בקרה במרב"ד הם מועברים למשרד החינוך

ונשמרים במערכת ז' שבמחשב ייעודי; בד בבד "ננעלים" הציונים במערכת ד', לא ניתן לשנותם ואף לא לשלוח אותם שוב למשרד החינוך[39].

גישה מרחוק של משתמשים למערכת ד': אפשרות הגישה מרחוק למערכות מידע עלולה להביא להיווצרות סיכונים ואיומים מוגברים, שכן היא מעצימה את הסיכויים לפגיעה בה, למשל בשל ציתות לתעבורת מידע במערכת, זליגת מידע לגורמים לא מורשים והתחזות לגורמים מאושרי גישה. הסיכונים והאיומים למערכת נוצרים בעיקר בשל קושי בשליטה על פעילות המתרחשת מחוץ לחצרי הארגון.

מטרת הנחיית יה"ב "גישה מרחוק" היא להנחות את קהל היעד בדבר קביעת מדיניות לגישה מאובטחת מרחוק לרשת הפנים-ארגונית ולמערכות המידע של המשרד. על פי ההנחיה, על המשרד לספק למשתמשים את תחנות העבודה שיאפשרו גישה מרחוק לרשת הפנימית, וזאת לאחר שהוא הקשיח את מערכת ההפעלה והצפין את הכוננים במחשבים הניידים של המשתמשים. כחלופה לכך נקבע בהנחיה שניתן להגדיר סביבת עבודה ייעודית שתאפשר לגשת מרחוק למערכות. עוד נקבע בהנחיה כי על כל תעבורת הרשת בחיבור מרחוק אל המשרד לעבור דרך חיבור מאובטח מלא שאינו מאפשר גלישה בד בבד ברשת ציבורית (במרשתת) אלא אם כן הדבר נעשה באמצעות תווך תקשורת מאובטח.

כניסת משתמש למערכת ד' דורשת הזדהות דו-שלבית (Two Factor Authentication, להלן - 2FA).

בביקורת עלה כי משרד החינוך והחברה החיצונית אינם מנהלים את מערך המחשבים האישיים הפרטיים של המעריכים שדרכם מתחברים למערכת ד', וכי החיבור שלהם מאובטח חלקית.

על משרד החינוך לפעול על פי מתכונת עבודה שנקבעה בהנחיית יה"ב, ובכלל זה לדרוש מהחברות המפעילות את מערך המרב"ד עבורו למנוע אפשרות לגלישה חופשית לא מאובטחת במרשתת בעת החיבור למערכת ד'.

ניטור ותיעוד של פעולות במערכת ד': תקנות הגנת הפרטיות אבטחת מידע קובעות כי במערכות מידע של מאגר מידע שחלה עליו רמת אבטחת מידע בינונית או גבוהה ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר, ובכלל זה על זהות המשתמש במערכות, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה ואם הגישה אושרה או נדחתה. על פי התקנות, על מנגנון הבקרה למנוע ככל האפשר ביטול או שינוי של הפעלתו, לאתר ניסיונות כאלו ולהתריע עליהם.

בהנחיית המסגרת נקבע כי איתור הניסיונות לביצוע פעולות לא מורשות ברשת המשרד יתמקד, בין השאר, בניתוח בדיעבד, ובסמוך ככל שניתן לזמן אמת, של הלוגים במערכות ובמוצרי האבטחה השונים.

39 לעיתים נדרש לבחון שוב ציונים או מחברות בחינה, למשל בשל עררים. במקרים כאלה מתבצע תהליך מבוקר ובו בעל הרשאה יחיד שמוגדר במערכת יכול "לשחרר" ציונים מנעילה לאחר אישור פורמלי של משרד החינוך, וזאת לצורך שינוי הציון ודיווח עליו מחדש.

עלה כי הפעולות הנעשות במערכת ד' נרשמות ומתועדות בקובצי ה-log, אך הן אינן מבוקרות ואינן מנוטרות: לא באמצעות מנגנון מסוים לניטור ובקרה, כפי שהומלץ בהנחיית המסגרת, ולא באמצעות מנגנון בקרה אחר.

מומלץ שמשרד החינוך יפעל לשיפור יכולת הניטור והבקרה של מערכת ד', ושינתח בסמוך ככל הניתן לזמן אמת את קובצי ה-log של המערכת לאיתור של חריגה מהרשאות ושל ניסיונות תקיפה.

הרשאות גישה למערכת ד': מערכת ד' הינה מערכת מבוזרת שבצד אחד משתמש (לקוח - Client) ובצד השני - שרת (Server).

בתקנות הגנת הפרטיות אבטחת מידע נקבע כי הרשאות הגישה של בעלי הרשאות למאגר המידע ולמערכות המאגר לכל תפקיד יהיו במידה הנדרשת לביצוע התפקיד בלבד.

גם בהנחיית המסגרת נקבע כי יש לתת הרשאות על בסיס "פרופיל הרשאות" מתאים לכל תפקיד שמאפשר למשתמש גישה לפרטי מידע הדרושים לו לביצוע עבודתו בלבד, וכי על המידור להתבצע בהתאם לעקרון "הצורך לדעת", המצמצם במידת האפשר את הגורמים המורשים להיחשף לנכסי המידע הרגישים במיוחד ומקנה שקיפות בתוך המשרד בנוגע לנכסי מידע בסיווג נמוך יותר. עוד נקבע כי יש ליישם כלים שמאפשרים זיהוי חד-ערכי של משתמשים אשר ביצעו שינויים במידע או בתוכנה או אשר ניגשו למידע רגיש, וכן שיפרטו את הפעילות שבוצעה.

בהנחיית יה"ב "פיתוח מאובטח"[40] נקבע כי יש לדאוג להפרדה מוחלטת בין סביבת הייצור לסביבת הפיתוח וסביבות הניסוי (הבדיקות), וכי אין לאפשר לתכניתנים (מפתחים) גישה לבסיסי נתונים בסביבת הייצור. עוד נקבע בהנחיה זו, כי יש לבצע הפרדה ברורה בין מידע הנועד לשימוש ע"י צד המשתמש (לקוח - Client) למידע שנועד לשימוש ע"י צד השרת (Server). וכי יש לאכוף דרישת הזדהות בכל העמודים והמשאבים של היישום, מלבד אלו אשר נועדו להיחשף.

בביקורת עלה כי לעובדים מסוימים במרב"ד, שעל פי מהות תפקידם נזקקים להרשאות גישה לסביבה ז' וה' של מערכת ד': ניתנו הרשאות גישה גם לסביבה ו' הנמצאת ברשת א'. הרחבת ההרשאות באופן שהן יוחלו על סביבה ו' מקנה לעובדים אלו גישה למערכת ד', ובכלל זה לבסיס הנתונים שלה. עוד עלה כי אין בקרה מסוימת על גישת אותם עובדים לסביבה ו'. יצוין כי גם ממצאי סקר הסיכונים רשת ג' שביצעה החברה החיצונית ביוני 2021 הצביעו על הרשאות יתר לאותם עובדים, שבגינן מתאפשרת להם גישה חופשית לשרתים.

במסגרת בדיקה מיוחדת שביצע משרד מבקר המדינה במערכת ד' עלה שההתקנה של צד המשתמש (לקוח - Client) וצד השרת (Server) ושבדיקת הרשאות אינן כנדרש בהנחיות יה"ב.

כדי לבחון את מערך ההרשאות בפועל, ניתח צוות הביקורת את רשימת המשתמשים כפי שמופיעים במערכת ניהול המשתמשים (ב-Active Directory, להלן - רשימת משתמשים ב-AD)

40 הנחיה מספר 5.13 מתאריך 21.05.2019, תאריך עדכון 24.09.2019, גרסה 1.1.

שיש להם הרשאות גישה למערכת ד'[41], וגם את הרשימה המתעדת את מועד הפעולה האחרונה שנרשמה לכל אחד מהם במערכת ד' (להלן - רשימת תיעוד פעולה אחרונה במערכת ד'). להלן פירוט של הממצאים שהועלו:

- שדה ה-Name ברשימת המשתמשים ב-AD של אחת המשתמשות (עובדת פעילה במרב"ד) אינו הזיהוי שנדרש אלא זיהוי אחר.
- שישה מתוך שמונה משתמשים ברשימת המשתמשים ב-AD, שתפקידם הוגדר במערכת ד' לתפקיד מסוים, קיבלו הרשאות החורגות מתפקידם.

בתגובתו מסר המשרד, שהגדרת התפקיד כאמור מאפשרת לתת לאותו עובד הרשאות רחבות. הרחבה כזו נדרשת כדי לנהל את ההרשאות של העובדים בתפקידים בדרגים נמוכים שלהם הרשאות מצומצמות.

משרד מבקר המדינה ממליץ למשרד החינוך לשקול לשנות את שיטת הקצאת ההרשאות, באופן שכל משתמש יקבל גישה לסביבת המחשוב שלה הוא נדרש לצורך מילוי תפקידו בלבד, וכך לשמור על עקרון "הצורך לדעת". לחלופין, מומלץ שהמשרד ככלל ימנע מעובדים מסוימים גישה לסביבה ו', זאת על מנת שלא לאפשר שינויים שלא בסביבה ז' וחשיפה למידע שעובדים אלו אינם נדרשים לו.

- ברשימה שבה מתועדות הפעולות האחרונות במערכת ד' נמצאו שלושה משתמשים שהגדרת תפקידם הייתה "תלמיד", ואולם במערכת לא הוגדר תפקיד כזה; עלה שהם הוגדרו לצורך ביצוע בדיקות אך בפועל הם אינם נכללים ברשימות ה-AD.
- נמצא כי שני משתמשים שנכללו ברשימה המתעדת את הפעולה האחרונה במערכת ד' לא נכללו ברשימת המשתמשים ב-AD, וכי הפעולה האחרונה של אחד מהם הוא משנת 2011 ושל השני - משנת 2016. הבדיקה העלתה כי אין מדובר במשתמשים בעלי זהות אמיתית.
- נמצא כי זיהוי מסוים של אחד המשתמשים, ששמו נכלל ברשימה המתעדת פעולה אחרונה במערכת ד', הופיע ללא ערך (NULL). עלה כי לחברה החיצונית אין יכולת להתחקות על הסיבה לכך.
- ברשימה המתעדת את הפעולה אחרונה במערכת ד' נמצאו 18 משתמשים[42] שתפקידם הוגדר כ"סגן מנהל אגף ומנהל מחלקת נבחנים". עלה שאין מדובר במשתמשים בעלי זהות אמיתית, וכי הם נרשמו במערכת לצורך שימוש בה בעת התכנסות ועדות ערעורים לעניין טוהר הבחינות.

מהממצאים עולים ליקויים בכל הנוגע לניהול מערך הרשאות המשתמשים: מתן הרשאות החורגות מהנדרש לתפקיד ושלא על פי עקרון "הצורך לדעת". זיהוי שלעיתים אינו חד-ערכי של משתמשים ומקרים שבהם עלה חוסר פירוט של הפעילות שבוצעה.

41 מספר המשתמשים משתנה מעת לעת וביולי 2021 עמד על למעלה מ- 5,300 משתמשים.

42 מספר הזיהוי שלהם מתחיל ב- 55555.

על משרד החינוך לפעול להבטיח כי חברות המפעילות את מערך המרב"ד עבורו יקפידו לפעול על פי עקרון "הצורך לדעת" ולצמצם את הגישה למידע בהתאם לפרטי מידע הדרושים למשתמש לצורך ביצוע עבודתו בלבד. בכלל זה מומלץ למשרד לדרוש לבטל את גישת עובדים מסוימים לסביבה ו' שלא לצורך, לוודא כי כל ההרשאות שניתנו הן לבעלי זהות אמיתית ולממש יכולת ניטור והתרעה אפקטיביות, בסמוך ככל הניתן לזמן אמת, על ביצוע פעולות לא מורשות במערכת בסביבה ו'. עוד מומלץ, לבצע התקנה של צד המשתמש (לקוח - Client) וצד השרת (Server), ולבדוק הרשאות גישה לכל עמוד ומסך במערכת כנדרש בהנחיות יה"ב.

אבטחת ציוד המחשוב בתחנות הקליטה: כאמור, בסוף כל יום בחינה מעביר כל בית ספר את מחברות הבחינה שלו לתחנות הקליטה, ובתחנת הקליטה מתבצעת ספירה לצורך בדיקת התקינות והשלמות של מחברות הבחינה והחומר הנלווה ונעשית, בין השאר, קליטה ראשונית של מחברות הבחינה למערכת ד' באמצעות התחברות מרחוק למערכת ד' וסריקת הברקוד של כל מחברת ישירות למערכת.

בכל תחנת קליטה מותקנת מערכת הגנה פיזית הכוללת אזעקות ומצלמות, המאובטחת באמצעות מערכת הגנה מסוימת ייעודית; מערכת ההגנה הפיזית מקושרת למערכת מחשוב עצמאית. החיבור למערכת ד' מבוצע ממחשב בתחנת הקליטה שהחברה החיצונית מנהלת, בתקשורת אינטרנטית ייעודית לרשת ג' העוברת דרך רכיב תקשורת[43] שמנהלת חברה חיצונית אחרת.

עלו פערים בתחנות קליטה מסוימות הנוגעים להיבטי אבטחה, בקרה וניטור.

משרד מבקר המדינה ממליץ למשרד החינוך לשקול לדרוש מהחברות המפעילות את מערך המרב"ד עבורו להטמיע את מערכות ההגנה הבקרה והניטור החסרות גם לגבי ציוד המחשוב שבתחנת הקליטה.

העברת קובצי מידע למערכת ד' וממנה - הצפנה והלבנה של הקבצים: מערכת אנטי-וירוס היא אחד הכלים הבסיסיים המשמשים להגנה על מערכות מחשוב ועל מאגרי מידע; באמצעותה נסרקים קבצים קודם לכניסתם לרשת או להעלאתם למערכת כדי לוודא שאין בהם קוד עוין.

תקנות הגנת הפרטיות אבטחת מידע קובעות, בעניין אבטחת התקשורת, כי בעל המאגר לא יחבר את מערכות המאגר למרשתת או לרשת ציבורית אחרת בלא שהתקין במערכת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב[44] (להלן - תוכנות הלבנה). עוד קובעות התקנות כי יש להשתמש בשיטות הצפנה מקובלות לצורך העברת מידע ממאגר המידע, ברשת הציבורית או במרשתת.

43 מודם שמנוהל על ידי חברה חיצונית.

44 ראו במסמך "המדריך המלא ליישום תקנות אבטחת מידע", שפרסמה הרשות להגנת הפרטיות במשרד המשפטים. על פי מדריך זה, יש להתקין אמצעי הגנה מפני חדירה לא מורשית ותוכנות מזיקות, בין השאר תוכנת אנטי-וירוס, הן בממשקים שבין מערכות המאגר למרשתת, והן בממשקים שבין מערכות אחרות למערכות המאגר.

העברת קבצים בין מערכת ד' שבמערך המרב"ד לבין משרד החינוך (או ספקים אחרים שלו) מתבצעת באמצעות כ-30 ממשקים ייעודיים; באמצעות ממשקים אלו מועברים, בין השאר, מידע רגיש כמו מחברות בחינה מתוקשבות, ציוני מעריכים, ציוני מגן, התאמות והקלות לתלמידים; כשני שלישים מהממשקים מבוססים על כספות וירטואליות, כשליש - על העברה בדוא"ל וממשק אחד מבוסס שרת קבצים.

אשר להעברת קבצים אלו באותם ממשקים, עלה כלהלן:

- הקבצים נקלטים במערכת ד' בלא שנבדקו באמצעות תוכנות הלבנה לצורך זיהוי פגיעות מסוימת.

יצוין כי במהלך הביקורת מסר משרד החינוך לצוות הביקורת כי הוא החל להטמיע מערכת הלבנה ברשת ב' של המשרד, וכי התהליך נמצא בשלב בדיקות מקדימות שלפני התקנת המערכת ברשת ג'.

- אף שהתקנות מחייבות הצפנה של מידע המועבר ברשת הציבורית או במרשתת, בפועל רק אחד הקבצים מועבר בממשקים כשהוא מוצפן. שאר הקבצים (כ-33) מועברים כשהם אינם בעלי דרישת הגנה מסוימת.
- כל הקבצים שיש בהם מידע רגיש מועברים ממערכת ד' למשרד החינוך באמצעות הכספות הווירטואליות, אולם יש קבצים כאמור המכילים מידע רגיש שמועברים ממשרד החינוך למערך המרב"ד בדואר האלקטרוני של משרד החינוך, והדבר שמעלה את הסיכון לדלף מידע רגיש ולפגיעה בפרטיות.
- קובץ מסוים המכיל מידע רפואי רגיש על תלמידים מועבר מספק חיצוני למשרד החינוך, ומשם למערכת ד' במערך המרב"ד בדואר האלקטרוני הציבורי, שאינו של משרד החינוך, וזאת בלי שהוצפן.

כדי לצמצם את הסיכון הכרוך בהעברת קובץ שיש בו סיכון לפגיעה מסוימת לרשת ג' ולמערכת ד', מומלץ שמשרד החינוך ישלים את ההטמעה של מערכת הלבנה ברשת א' וברשת ג'. בכל הנוגע להעברת מידע רגיש בין מערכותיו לבין מערכות חיצוניות - על משרד החינוך להתקין אמצעי הגנה מסוימות וכן לפעול להגנה על המידע המועבר בממשקים אלו בהתאם לתקנות הגנת הפרטיות אבטחת מידע. מומלץ כי המשרד יפסיק להעביר את הקובץ שמכיל מידע רגיש על תלמידים ברשת הציבורית כשאינו בעל דרישת הגנה מסוימת ויפעל לכך שקבצים שיש בהם מידע רגיש יועברו באמצעות פתרון מאובטח כגון כספות וירטואליות.

אבטחת מידע במערכת ב' ובמערכות ניהול בית-ספריות

מערכת ב' משמשת את כל בתי הספר, ובין היתר היא משמשת לרישום התלמידים הניגשים לבחינות הבגרות. כ-250 מבתי הספר מזינים באמצעותה גם את הציונים השנתיים הבית-ספריים של התלמידים (ציוני המגן). שאר בתי הספר-כ-1,250, מזינים את ציוני המגן בתוכנות אחרות לניהול פדגוגי[45].

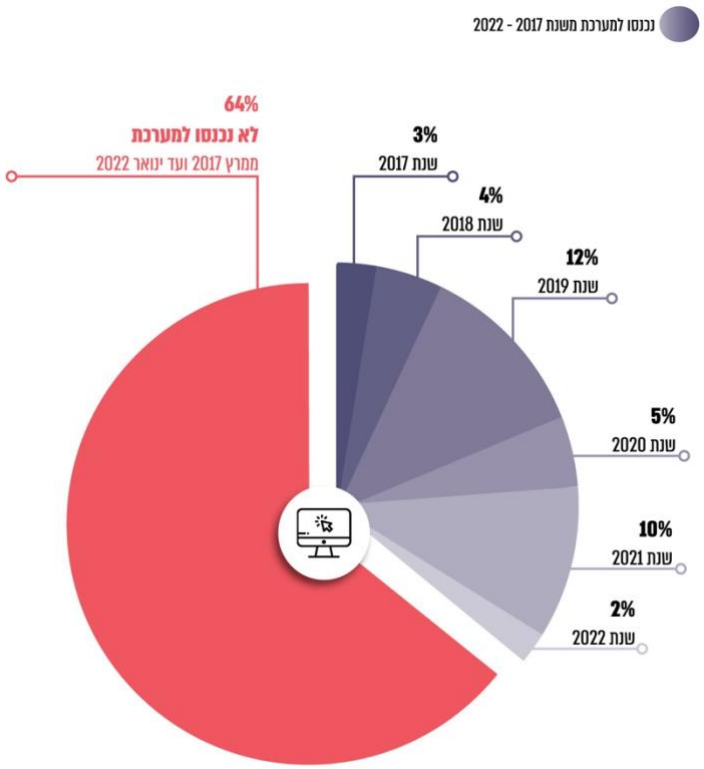
הרשאות גישה למערכת ב': מערכת ב' מותקנת ומנוהלת בתת-סביבה לוגית נפרדת ברשת א'. הגישה למערכת מבתי הספר מתבצעת באמצעות אתר מרשתת ייעודי (להלן - גישה אינטרנטית). משתמש בעל הרשאת גישה למערכת יכול להיכנס אליה באמצעות הזדהות אישית דו-שלבית (2FA).

בהנחיית יה"ב "ניהול ותפעול הרשאות" נקבע שתפקיד העובד הוא הבסיס למתן הרשאות גישה למשאבי מערכות המידע, וזאת עפ"י עיקרון הצורך לדעת בכל הנוגע לחשיפה למידע הארגוני, ועל פי מינימום הרשאות לצורך ביצוע עבודתו בכל הנוגע לקביעת פרופיל פעולות אקטיביות. עוד נקבע כי על המשרד לבצע אחת לחצי שנה בחינת הרשאות של משתמשים בעלי הרשאות גבוהות כדי להימנע ממתן הרשאות עודפות.

מתן הרשאות גישה שלא לצורך: צוות הביקורת בדק את כניסות המשתמשים המורשים למערכת ב' בחודשים מרץ 2017 עד ינואר 2022, בסך הכול מדובר בכ-216,000 משתמשים בעלי הרשאת כניסה למערכת. בתרשים שלהן מוצג מועד הכניסה האחרון של משתמשים אלו:

45 נכון לנובמבר 2021 יש 14 מערכות לניהול בית ספר אותן אישר המשרד והן שונות ממערכת ב'.

תרשים 11: **מועד הכניסה האחרון של משתמשי המערכת בחודשים מרץ 2017 עד ינואר 2022**



על פי נתוני משרד החינוך, בעיבוד משרד מבקר המדינה.

עלה כי 64% מהמשתמשים לא נכנסו למערכת במשך תקופה של קרוב לחמש שנים - בין מרץ 2017 לינואר 2022; עוד עלה שכניסת 19% מהמשתמשים הייתה לכל המאוחר לפני כשלוש השנים עד חמש שנים (בשנים 2017 - 2019) וכי רק מקצת המשתמשים (12% מהם) נכנסו למערכת בין ינואר 2021 עד ינואר 2022. עולה מכך חשש למתן הרשאות גישה למערכת למי שאינו נדרש להן.

כך למשל עלה כי לארבעה משתמשים ניתנה הרשאה גבוהה לכל פרופילי הרשאות התפקידים במערכת; אחד מהם הוא עובד של חברה חיצונית שהוגדר ארבע פעמים במערכת עוד בשנת 2014, בכל פעם עם ערך פיקטיבי שונה בשדה "ישות", ואין תיעוד לכניסתו האחרונה למערכת. שלושת המשתמשים האחרים הם עובדי מינהל תקשוב במשרד החינוך, אשר משמשים בתפקידי תמיכה ולכן לא נזקקים להרשאות הגבוהות אלא להרשאות מוגבלות המתאימות לתפקידם, זאת על פי עקרון "הצורך לדעת" ומינימום הרשאות לצורך ביצוע התפקיד.

משרד החינוך מסר בתשובתו, שכחלק ממדיניותו ובהתאם לתהליכי הפדגוגיה מוגדרות ההרשאות למערכת ב' ולמערכות ניהול בית-ספריות לכל עובד הוראה בהתאם לתפקידו במערכת החינוך.

נוכח ממצאי הביקורת, שמהם עולה כי מורשי גישה מעטים מאוד משתמשים בהרשאות שקיבלו - כשני שלישים מהם לא נכנסו למערכת ב' בחמש השנים האחרונות ורק כ-12% נכנסו אליה בשנה האחרונה, מומלץ למשרד החינוך לבחון את הסיבות לשיעור הנמוך של הנכנסים למערכת ואת הצורך לעדכן את רשימת מורשי הגישה למערכת ב' ואת ההרשאות שניתנו להם ולפעול, בעניין זה, לפי עקרון "הצורך לדעת" - מתן הרשאה מצומצמת בהתאם להגדרת תפקיד המשתמש. מומלץ גם שהמשרד יבצע אחת לתקופה בקרת הרשאות בקרב משתמשי מערכת ב', בדגש על שינויים שנעשו במערך ההרשאות, ובכלל זה ישקול הטמעה של מנגנון אוטומטי לביטול הרשאות כניסה למערכת למי שלא נכנס אליה במשך תקופה שתוגדר.

העברת קובץ ציוני המגן לסביבה ב' ולמערכת ד': לאחר שבתי הספר מזינים את ציוני המגן של התלמידים למערכת ב' או לאחת מהתוכנות האחרות לניהול פדגוגי, המערכת מייצרת קובץ הכולל את פרטי התלמידים וציוני המגן (להלן - קובץ ציוני מגן); הקובץ מיובא בתהליך אוטומטי לסביבת ב', ונבדקת תקינותו לפי פרמטרים שהוגדרו מראש. לאחר מכן, עותק של הקובץ מועבר מסביבה ב' לסביבה א' ומשם נטען למערכת ד'.

עלה כי שלא בהתאם לתקנות הגנת הפרטיות אבטחת מידע ושלא בהתאם להנחיית המסגרת בנוגע לאמצעי הגנה שיש להתקין כנגד תקיפה ופגיעה במערכות המחוברות לרשתות חיצוניות, נכון לספטמבר 2021 משרד החינוך לא סרק במערכת הלבנה קבצים לפני העברתם לסביבה ב'. עוד עלה כי נכון לנובמבר 2021 גם החברה החיצונית לא סרקה את אותם קבצים לפני שייבא אותם לסביבה שלו או לפני שקלט אותם במערכת ד'.

יצוין כי במהלך הביקורת מסר משרד החינוך לצוות הביקורת כי הוא החל להטמיע מערכת הלבנה לסריקת קבצים כדי לוודא כי אין בהם סיכון לפגיעה מסוימת לממשקים החיצוניים שבאמצעותם מועברים קבצים לרשת ב' שלו, וכי התהליך נמצא בשלב הבדיקות המקדימות הקודמות להתקנת המערכת ברשת ג'.

משרד מבקר המדינה ממליץ למשרד החינוך להשלים את פריסת מערכת ההלבנה בכל הסביבות, המערכות ותחנות הקצה שבאחריותו, שכן מדובר באמצעי אבטחת מידע בסיסי וחיוני ביותר.

מבדק חדירות למערכת ב': בספטמבר 2021 ביצע המשרד, באמצעות חברה חיצונית, מבדק חדירות למערכת ב'.

עלה כי אף שבהתאם לתקנות הגנת הפרטיות אבטחת מידע, על המשרד לבצע מבדקי חדירה אחת ל-18 חודשים, בפועל בשלוש השנים שקדמו לספטמבר 2021, המשרד לא ביצע את מבדק החדירה הנדרש במערכת ב' וכי בספטמבר 2021 ביצע המשרד, באמצעות חברה חיצונית, מבדק חדירה למערכת ב'.

על משרד החינוך להקפיד על ביצוע מבדקי חדירה בתדירות שנקבעה בתקנות הגנת הפרטיות אבטחת מידע, וכן עליו לתקן ליקויים שעלו במבדקים אלו.

בדיקות אבטחת מידע לתוכנות האחרות לניהול פדגוגי: במסגרת מתן אישור המשרד לשימוש בתוכנות אחרות לניהול פדגוגי בבתי הספר הוא מחייב את ספקי התוכנות לעמוד בדרישות מסוימות שהוא קבע, כגון תקן תוכנה לניהול פדגוגי[46] ותקן אבטחת מידע[47]; הוא גם מחייב אותם לעבור אחת לשנה בדיקות אבטחת מידע, שמבצעת חברה חיצונית שעימה הוא התקשר (להלן - חברת הבדיקות). במסגרת הבדיקה נדרשה חברת הבדיקות החיצונית לבצע בדיקות אלו:

1. בדיקת חדירות, אשר מבוצעת על פי ההגדרה של עשרת סיכוני אבטחת המידע הקריטיים ביותר למערכות המבוססות על אפליקציית מרשתת, שאותם קבע ארגון Open Web Application Security Project Foundation (להלן - OWASP), העוסק בתחום אבטחת יישומי מרשתת (להלן - עשרת סיכוני-העל)[48]. אם נמצאו בבדיקה חולשות אבטחת מידע, על הספק לטפל בחולשות, ולאחר שיעמוד במבדק חדירה חוזר הוא יוכל לקבל אישור לשימוש במערכת.
2. בדיקות עמידה בתקן אבטחת מידע של משרד החינוך.
3. הצהרה על עמידה בתקנים של משרד החינוך, לרבות תעודת הסמכה לתקן ISO-27001.

צוות הביקורת בדק את החומרים הקשורים לתהליך האישור של שתי התוכנות הנפוצות ביותר בשימוש בבתי הספר ושתי התוכנות הפחות נפוצות.

עלה כי שלוש הבדיקות הנדרשות בוצעו לכל אחת מארבע התוכנות, וכי אם מבדק החדירה העלה ממצאים שהצביעו על חולשות אבטחה, בוצע מבדק חדירה חוזר שלא העלה ממצאים כלל.

הלבנת קובצי השאלונים לפני טעינתם למערכת ו'

מערכת ו' משמשת ממשק של אגף הבחינות במשרד החינוך מול בתי ספר ביום הבחינה. כשעה לפני הבחינה אגף הבחינות טוען את קובצי השאלונים למערכת ו' ובאמצעותה מופצים קובצי שאלוני בחינות הבגרות לבתי ספר שלא קיבלו עותקים פיזיים בכספות; בתי ספר אלו מדפיסים בעצמם את השאלונים.

בהנחיית יה"ב "הקשחת עמדות קצה" נקבע כי הכנסת קבצים באמצעות מדיה חיצונית למשרד תורשה אך ורק באמצעות מערכת הלבנה אשר מבצעת סינון ובדיקה של קבצים אלו טרם

46 משרד החינוך, "תקן תוכנה לניהול פדגוגי", גרסה 1.3 מ-22.2.01.

47 משרד החינוך, "תקן אבטחת מידע", גרסה 2.5 מ-14.2.16.

48 The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

העברתם לרשת הארגונית. בהנחיית יה"ב "אבטחת גלישה באינטרנט" נקבע שהסריקה תיעשה באמצעות מערכות הלבנה בעלות מנגנונים מסוימים.

עלה שנכון למועד סיום הביקורת (מאי 2022), קובצי השאלונים, שנשלחים למשרד החינוך מסביבות מחשוב חיצוניות של הספקים המגבשים את השאלונים, לא נסרקו במערכת הלבנה שמאתרת אם יש בהם סיכון לפגיעה מסוימת לפני העתקתם לרשת ב' וטעינתם במערכת ו'.

בתשובתו ציין משרד החינוך כי נכון לאוקטובר 2022 הוא מיישם פתרון שמבצע סריקה של קבצים המועלים למערכת לשם איתור סיכון לפגיעה מסוימת.

על משרד החינוך להטמיע תהליך של בדיקה, סריקה והלבנה של הקבצים באמצעות מערכת הלבנה בעלת מנגנונים מסוימים לפחות כנדרש בהנחיות יה"ב, לפני העתקתם לרשת ב', וקודם להעלאתם למערכת ו' ולהפצתם לבתי הספר.

רשת ב' של משרד החינוך

רשת ב' של משרד החינוך משרתת את עובדיו. שרתיה נמצאים בחוות השרתים של חברה ב', אשר מספקת למשרד את התשתיות הפיזיות הנדרשות - מקום עבודה, חשמל, מיזוג אוויר ואבטחה פיזית. ברשת פועלים כ-1,000 שרתים וירטואליים, והיא מחוברת ל-SOC הממשלתי.

מערכת ז' שברשת ב' של משרד החינוך

מערכת ז' של משרד החינוך מותקנת ברשת ב' במערכת מחשב ייעודית. נאגרים בה כל ציוני הבגרות של התלמידים משנות השבעים של המאה העשרים, ובהם ציוני המגן, ציוני המעריכים את בחינות הבגרות וציונים נוספים הרלוונטיים לציון הסופי; במערכת משוקלל ציון הבגרות הסופי לכל מקצוע.

מערכת ז' נחשבת למערכת ליבה רגישה, מאחר שהיא מנהלת מידע רגיש רב על כל התלמידים שלמדו במערכת החינוך במשך השנים, ועל כן נדרש לבצע בקרה מוקפדת על מורשי הגישה אליה ועל הפעולות שמבוצעות בה.

בהנחיית המסגרת נקבע כי איתור הניסיונות המוצלחים או הכושלים לביצוע פעולות לא מורשות במערכות המשרד יתמקד בשני סוגי בקרות: (א) ניתוח בדיעבד ובזמן סמוך ככל שניתן לזמן אמת של מנגנוני הבקרה שבמערכת ובמוצרי האבטחה השונים. בקרה רגילה תתמקד באיתור ניסיונות כניסה כושלים למערכת ולרשת ובפעילות בשעות חריגות, ואילו בקרה במערכות רגישות תבוצע ברמה גבוהה יותר, כדוגמת מעקב אחר משתמשים בעלי הרשאות גבוהות במערכת ומעקב אחר ביצוע פעולות מסוימות; (ב) איתור בזמן אמת של פעילויות לא מורשות ברשת ובשרתי המשרד.

עדכון של ציוני בגרות: על פי הסברי משרד החינוך לצוות הביקורת, בקשות לשינוי, עדכון או מחיקה של ציונים מתקבלות בדרך כלל בדואר האלקטרוני ממנהלי בתי הספר אל אגף הבחינות,

וניתן לבצען רק במערכת ז' והן מתועדות בה. רק מי שהמשרד נתן לו הרשאה לכך יכול לבצע את הפעולות. בספטמבר 2021 בוצעו במערכת יותר מ-900 פעולות לשינוי ציונים.

עלה כי אף שעדכון של ציוני התלמידים הוא תהליך רגיש ביותר, שלשם ביצועו נדרשים רמת אמינות גבוהה ותהליך סדור ומבוקר, משרד החינוך לא הסדיר לשם כך נוהל המגדיר את שלבי התהליך, את הגורמים המעורבים בו, את האחראים לכל שלב ואת הבקרה על התהליך. בפועל, עלו פערים במנגנוני הניטור והבקרה של משרד החינוך. המשרד גם לא מבצע בקרה בדיעבד - הוא לא הסדיר תהליך לקבלת דוח תקופתי קבוע המציג את הפעולות שבוצעו במערכת והמאתר פעולות החשודות כחריגות. כמו כן, עלו פערים באגף הבחינות בהיבטי בקרה פנימית.

העברת בקשה לשינוי ציונים בדואר האלקטרוני חשופה לסיכונים מסוימים. משרד מבקר המדינה ממליץ למשרד החינוך לקבוע נוהל המסדיר את תהליך עדכון הציונים במערכת ז'. בכלל זה מומלץ שהנוהל יגדיר את הגורמים המעורבים בתהליך עדכון הציונים, את רמת ההרשאות שלהם ואת הפעולות הרגישות שיש לבצע מעקב קבוע אחריהן. כמו כן, מומלץ שהנוהל יעסוק בסגירת הפערים הנובעים מהשימוש בדואר האלקטרוני. מומלץ גם שהמשרד יטמיע את הנוהל הן במשרד והן בקרב מנהלי בתי הספר.

המשרד מסר בתשובתו כי הוא יפעל להוצאת דוחות תקופתיים לאיתור פעילות חריגה ויבחן יישום של תהליך מוסדר. עוד מסר שהוא מפתח מערכת ציוני בגרות חדשה, שתעשה שימוש בטכנולוגיות חדשות ותיתן מענה טוב יותר לנושאי אבטחת מידע.

אתגרי השמירה על טוהר הבחינות בעידן הדיגיטלי

השמירה על טוהר הבחינות בכלל ועל ניהולן התקין של בחינות הבגרות בפרט היא משימה חינוכית, ערכית ומוסרית, והיא תנאי הכרחי לשמירה על הגינות ועל שוויוניות בין הנבחנים. קבלת סיוע מכל סוג, ובכלל זה פתרונות לשאלות הבחינה, בין שנותן הסיוע הוא נבחן אחר או גורם אחר, גניבת שאלון, החזקת שאלון בחינה שטרם חל מועד ההיבחנות בו בידי נבחן, שימוש בטלפון נייד, באוזניות, בשעון חכם, וב"מחשוב לביש"[49] בכלל, וכן בכל אמצעי תקשורת אחר במהלך הבחינה - כל אלה הם בגדר עבירות משמעת על פי חוזר "טוהר הבחינות"[50].

בשנת 2011 פרסם מרכז המחקר של הכנסת דוח בנושא[51], ולפיו את רובן הגדול של העבירות על כללי טוהר הבחינות (90% מהן) לא איתרו המשגיחים הנוכחים בבחינות עצמן, אלא המעריכים של מחברות הבחינה. מאז השיטות לפגיעה בטוהר הבחינות השתנו והתפתחו עם השנים בהתאם להתפתחות הטכנולוגית, וכך הצטרפו לשיטות המוכרות של הדלפת בחינות והעתקה בבחינות גם הפצה לא מורשית של שאלוני הבחינות ופתרונות שלהן באמצעות טלפונים

49 מחשוב לביש - הוא כל אביזר אלקטרוני/ אביזר מחשוב הנישא על הגוף והמספק לנושא אותו מידע, למשל שעון חכם, משקפיים, בגד, מצלמה, טבעת חכמה צמיד חכם ועוד.

50 ראו: חוזר מנכ"ל משרד החינוך "טוהר הבחינות" הוראת קבע מספר 0237 ,בתוקף מיום 3.12.2019.

51 מרכז המחקר והמידע של הכנסת, "שמירה על טוהר בחינות הבגרות", מ-7.3.11.

סלולריים ושימוש ברשתות חברתיות וביישומונים. דרכים אלו מאפשרות להפיץ באנונימיות את הבחינה ואת פתרונה באופן המקשה את ההתחקות אחר המפיץ.

פעולות שנקט משרד החינוך לשמירה על טוהר בחינות הבגרות ביום קיומן

הפצת שאלוני הבחינה ללא רשות עלולה במקרים מסוימים להיחשב עבירה פלילית של "הוצאת מסמך ממשמורת" לפי חוק העונשין, התשל"ז-1977, שדינה שלוש שנות מאסר. נוסף על כך, הפצת שאלוני בחינות הבגרות והתשובות להן לפני הבחינה או בזמן הבחינה עלולה לסייע לחלק מהנבחנים לקבל יתרון בלתי הוגן על פני שאר התלמידים, ואף לקבל במרמה ציונים שלא היו אמורים לקבל, ולכן עשויה לעלות לכדי עבירה פלילית של קבלת דבר במרמה.

ביוני 2015 מינתה מנכ"לית משרד החינוך דאז צוות משרדי לבחינת נושא ההיערכות לבחינות הבגרות חורף 2016 וכן לבחינות העתידיות, בראשות סמנכ"ל בכיר ומנהל המינהל הפדגוגי דאז וסמנכ"ל חירום, בטחון ובטיחות דאז (להלן - הוועדה). בטיוטת דוח הוועדה[52], הומלץ בין השאר, ליווי של גוף חיצוני שיבחן לעומק את תהליכי התפעול של בחינות הבגרות. בשנת 2018 ביצע משרד החינוך באמצעות חברה חיצונית "מיפוי וניתוח תהליכים וסיכונים באגף הבחינות", שכלל השוואה בין-לאומית של תהליכי תפעול הבחינות ובחינת מודלים חלופיים.

שינוי של מודל הפצת הבחינות: בהמשך להמלצות הוועדה שינה משרד החינוך את המודל להפצת השאלונים מהפצה באמצעות דואר ישראל להפצה באמצעות חברות בלדרות; רכישה והתקנה של מאות כספות ברזל "חכמות"[53] בבתי הספר; כתיבת נוהלי עבודה החל בשלב גיבוש השאלונים, עבור דרך שלבי הדפסתם ואריזתם וכלה בשלב הפצתם לבתי הספר; פרסום (במרץ 2021) של מסמך בקשה לקבלת מידע (R.F.I) בנושא הערכת בחינות בגרות בכתב ובעל פה על בסיס מערכת לבינה מלאכותית; ופרסום (ביולי 2021) של מסמך בקשה לקבלת מידע (R.F.I) בנושא ביצוע בחינות בשאלונים לא מודפסים ללא יכולת להפיץ ולקלוט תשובות תוך כדי בחינה.

אגף הבחינות מסר לצוות הביקורת שלאחר הטמעת המעבר להפצה באמצעות חברות בלדרות ולאחר התקנתן של כספות בכלל בתי הספר (בשנת 2017) הופסקה באופן מוחלט תופעת ההדלפה בה הבחינה נחשפת שעות לפני שהיא מתקיימת. עם זאת, להערכת האגף התפתחה תופעה של הפצה לא מורשית של שאלוני הבחינה מרגע הוצאתם מהכספות.

52 משרד החינוך מסר למשרד מבקר המדינה שאין ביכולתו לאתר את הנוסח הסופי של דוח הוועדה, ושלח למשרד מבקר המדינה טיוטת דוח שהגדיר "כאחרונה".

53 כספות ברזל שמאפשרות למשרד החינוך לשלוט מרחוק על שעת פתיחתן, ובהן הוא שומר את שאלוני בחינות הבגרות.

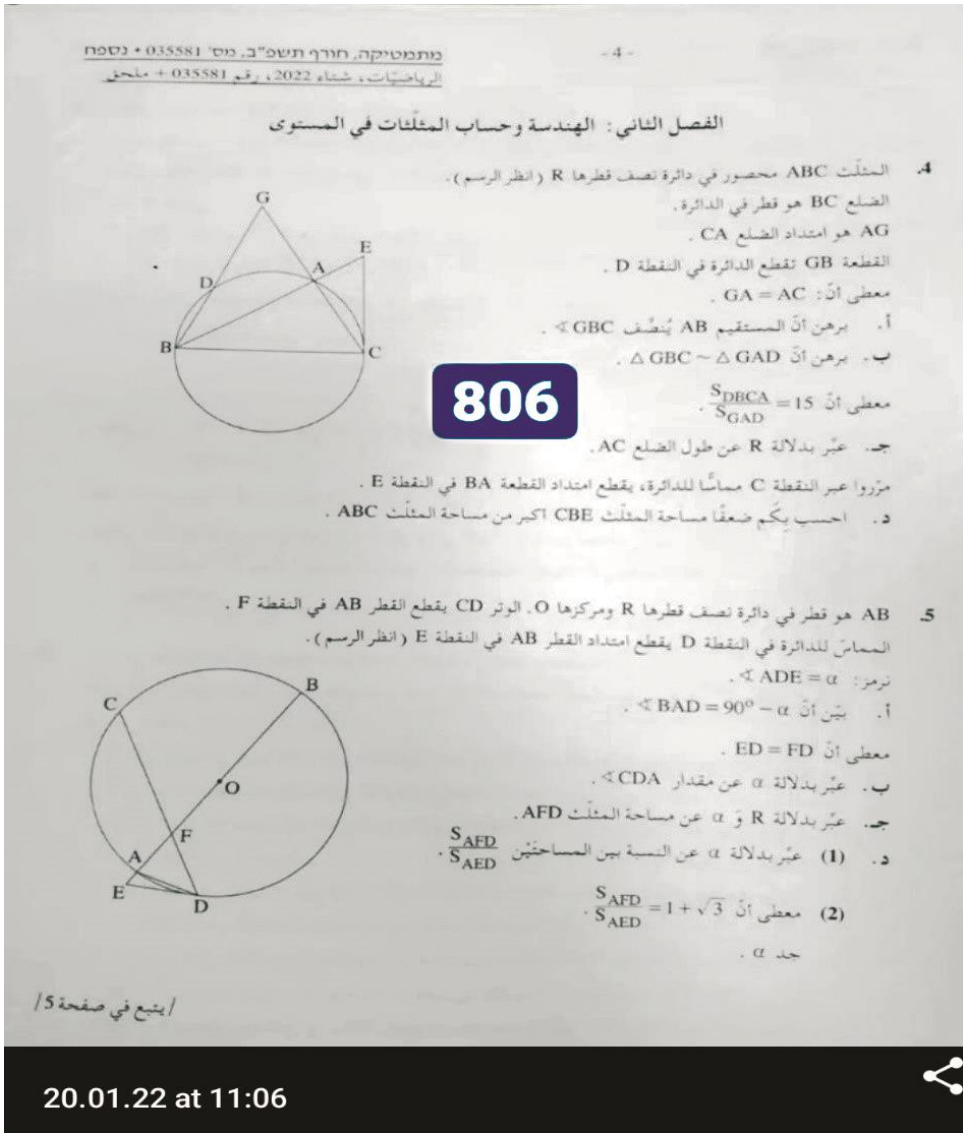
הפצה לא מורשית של בחינות בגרות ביום קיום הבחינה

צוות הביקורת בדק בחודשים יוני 2021 עד פברואר 2022 הפצה לא מורשית של בחינות בגרות שמתבצעות ביישומון מסוים למסרים מיידיים (להלן - היישומון). בבדיקה נמצאו שבע קבוצות הפעילות במגזר היהודי ובמגזר הערבי, שבהן התבצעה פעילות הפצה לא מורשית של שאלונים ושל הפתרונות לשאלונים - למשל קבוצה ובה מעל 12 אלף חברים. יצוין כי לא נצפה שום מקרה של הדלפת שאלון בחינה לפני המועד המוגדר לפתיחת הכספות, אלא רק הפצה לא מורשית לאחריו, והדבר הוא בגדר עבירת משמעת לפי חוזר טוהר הבחינות, המקנה לנבחן זמן לפתרון שאלון הבחינה ולהפצת התשובות בזמן הבחינה ולעתים אף לפני.

צוות הביקורת מצא עשרות דוגמאות להפצה של שאלוני בחינות בגרות בזמן קיום הבחינה. להלן מובאות כמה דוגמאות לשאלונים ולפתרון בחינה שהופצו בזמן הבחינה:

להלן דוגמה לתצלום של שאלון בחינה במתמטיקה בהיקף 5 יחידות, בערבית, מס' 35581, שעל פי נתוני משרד החינוך היה אמור להתקיים ביום חמישי, 20.1.22 בשעה 11:00 (תשפ"ב); השאלון הופץ בקבוצות היישומון כשש דקות לאחר השעה המיועדת לתחילת הבחינה:

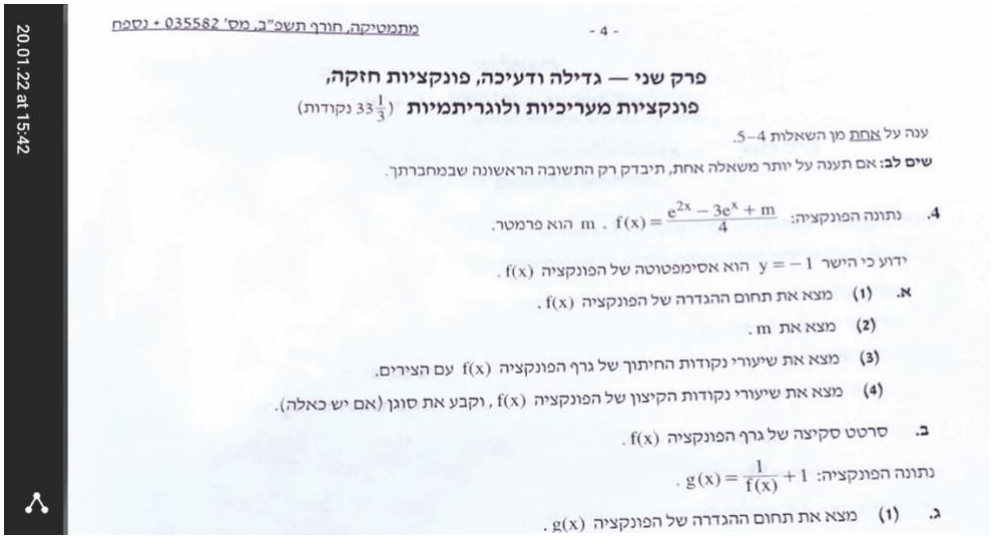
תמונה 1: **תצלום של שאלון מס' 35581 שהופץ ב-20.1.22 בשעה 11:06**



המקור: היישומון.

להלן דוגמה להפצת תצלום של שאלון בחינה במתמטיקה בהיקף 5 יחידות, בערבית, מס' 35582, שעל פי נתוני משרד החינוך היה אמור להתקיים ביום חמישי, 20.1.22 בשעה 15:30 (תשפ"ב) ושהופץ בקבוצות היישומון, כ-12 דקות לאחר השעה המיועדת לתחילת הבחינה:

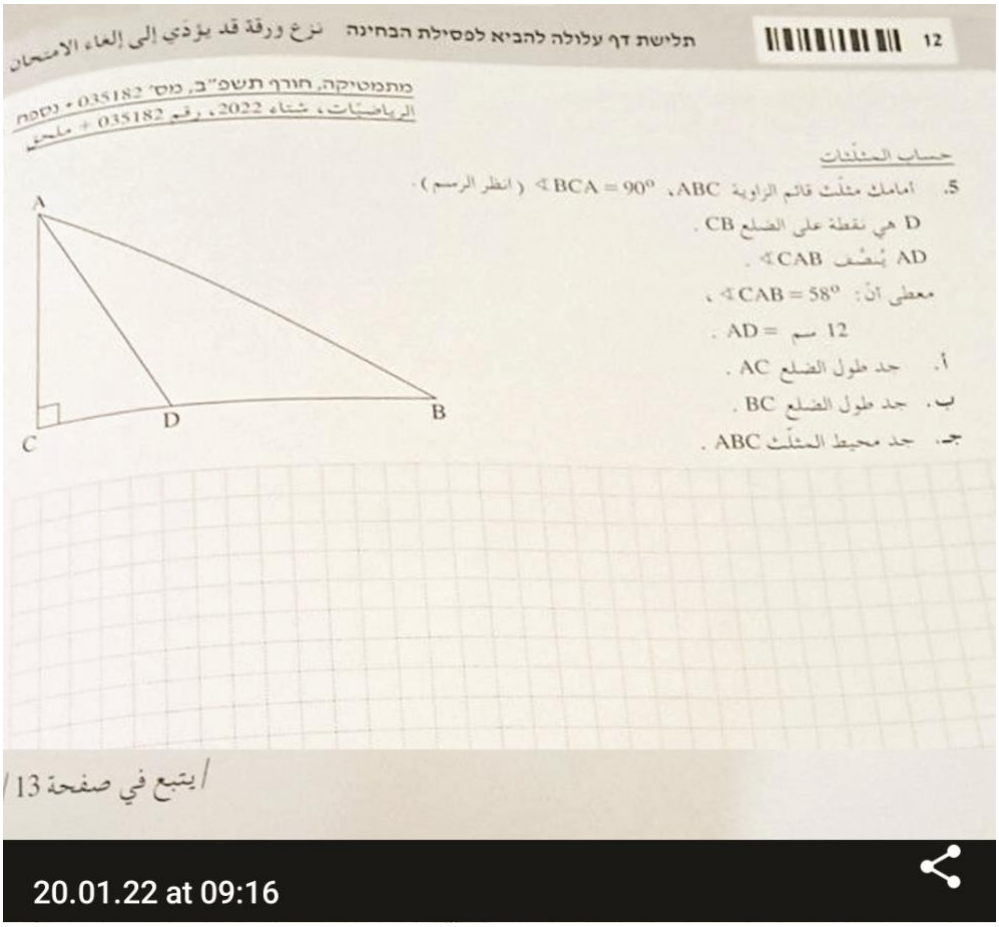
תמונה 2: **תצלום של שאלון מס' 35585 שהופץ ב-20.1.22 בשעה 15:42**



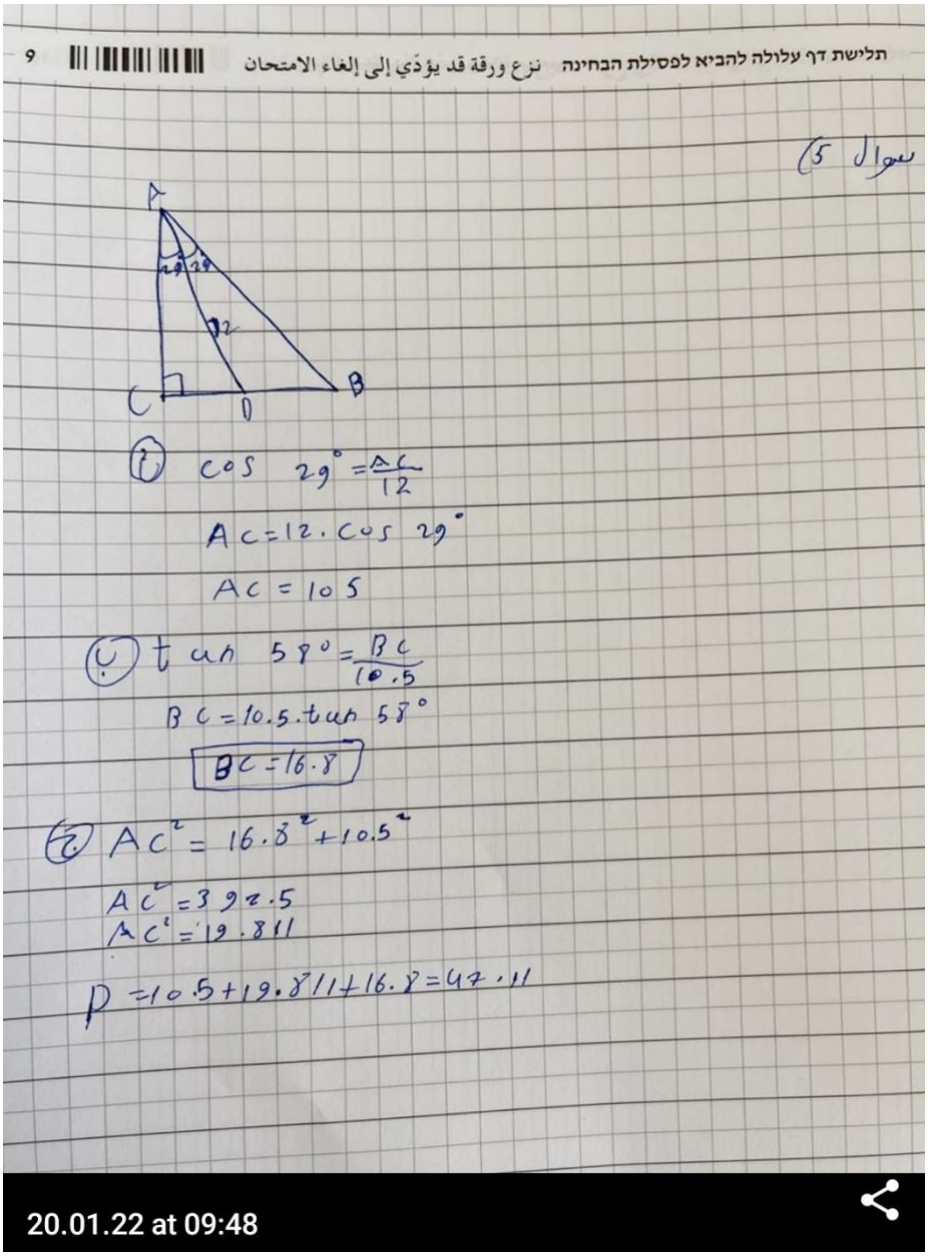
המקור: היישומון.

להלן דוגמה לתצלום שאלון בחינה במתמטיקה בהיקף 3 יחידות, בערבית, מס' 35182, שעל פי נתוני משרד החינוך היה אמור להתקיים ביום שלישי, 18.1.22 בשעה 09:00 (תשפ"ב) ושהופץ בקבוצות היישומון כ-16 דקות לאחר השעה המיועדת לתחילת הבחינה, וכן תצלום של פתרון הבחינה באותה קבוצה כחצי שעה לאחר מכן:

תמונה 3: **תצלום של שאלון מס' 35182 שהופץ ב-20.1.22 בשעה 9:16 וכן של הפתרון משעה 9:48**



המקור: היישומון.



המקור: היישומון.

משרד החינוך מסר לצוות הביקורת כי הוא נמצא בקבוצות היישומון שמהן הובאו הדוגמאות שלעיל. בפועל, כאשר עולות בקבוצות הודעות הכוללות פתרונות לשאלוני הבחינה, הם מועברים למעריכים אשר מתודרכים בדבר הפעולות שעליהם לנקוט אם עולה חשש לאי

תקינות. המשרד הוסיף כי הוא החמיר את אמצעי הענישה וכך, תלמיד שנמצא שהשתמש בפתרונות שהועברו ביישומון מעוכב מהיבחנות למשך שנה שלמה.

בחוזר טוהר הבחינות, מפורטים הצעדים המשמעתיים בהן ניתן לנקוט בגין כל הפרה של טוהר הבחינות, לרבות פירוט של העונשים הצפויים. עוד נקבע בחוזר טוהר הבחינות כי בהתאם לנסיבות ולחומרת העניין, תיתכן הגשת תלונה למשטרה לצורך פתיחה בחקירה פלילית נגד המעורבים.

עלה כי בשנים 2018 - 2020 הגיש משרד החינוך ארבע תלונות בלבד במשטרת ישראל (להלן - המשטרה) בגין עבירת "קבלת דבר במרמה" בעקבות הפצה לא מורשית של שאלונים או של תשובות של בחינות הבגרות, יצוין באשר לכך כי בשנת 2020 פסל המשרד למעלה מ- 16,000 מחברות בחינה בשל חשד להפרת טוהר הבחינות. בדצמבר 2019 פנה משרד החינוך למשטרה בכתב בבקשה לפתוח בחקירה בנושא ההונאות במסגרת קיום בחינות הבגרות.

בנובמבר 2021 דיווחה המשטרה לצוות הביקורת כי שניים מהתיקים נסגרו בעילה של "עבריין לא נודע", תיק אחד נסגר בעילה של "היעדר עבירה פלילית", ותיק אחד עדיין נמצא בחקירה.

בתגובת המשטרה לממצאי הביקורת מאוגוסט 2022 (להלן - תשובת המשטרה) היא מסרה, כי היא רואה את סוגיית ההונאה בבחינות הבגרות ושמירה על טוהר הבחינות כנושא חשוב מאוד. כי בחלק מהתלונות נמסרה תלונה כללית הכוללת אינפורמציה חלקית וחסרה ללא שום פרטים קונקרטיים. משכך, תיקים אלו נגנזו בעילה של עבריין לא נודע. מנגד, בתיקים בהם נמסרה תלונה סדורה המכילה את כלל הפרטים, בוצעו פעולות חקירה רבות והן מצויות בחקירה.

עוד עלה בביקורת כי במאי 2021 פנה מנהל אגף הבחינות ללשכת הייעוץ המשפטי במשרד החינוך כדי לאשר לו לקבל את פרטי התלמידים שמספרי הטלפון שלהם נכללו באותן קבוצות לעיל, הרשומים במערכות המידע של המשרד. מנהל אגף הבחינות מסר ביולי 2021 למשרד מבקר המדינה כי לשכת הייעוץ המשפטי לא אישרה את בקשתו מטעמי הגנת הפרטיות.

בחוזר שנתי - "בחינות הבגרות לשנה"ל תשפ"ב (2022)" שפרסם משרד החינוך, נקבע איסור על כניסת תלמידים לכיתת הבחינה לאחר שהבחינה התחילה, וכי בבחינות "עתירות הסיכון כגון, אנגלית מתמטיקה, שפה..." יפתחו כספות הבחינות עם תחילת הבחינה כאשר התלמידים "נמצאים תחת השגחה".

בתשובתו הוסיף המשרד כי בשאלונים עתירי סיכון הוא מפיץ כמה גרסאות לכל בחינה, על מנת לאתר את המעתיקים שמתבססים על הרשתות החברתיות.

משרד מבקר המדינה ממליץ כי משרד החינוך ומשטרת ישראל יבחנו כלים להתמודדות עם תופעת ההדלפות וההפצה הלא מורשית של בחינות הבגרות וכן הפצת פתרונות להם טרם שהם הסתיימו; דגש יש לתת לצורך במענה הולם ומתקדם בהתאם להתפתחויות הטכנולוגיות והשימוש המואץ שנעשה באמצעי תקשורת שונים, שמגבירים תופעות אלו - רשתות החברתיות, יישומונים, מחשוב לביש וכיוצ"ב.

בתשובת המשטרה היא מסרה כי נקבעה פגישה בין נציגיה לבין נציגי משרד החינוך, במטרה להסדיר ולטייב את תהליך העבודה כשמוגשות תלונות על הונאות ופגיעה בטוהר בחינות הבגרות, בין היתר, המטרה לקבוע את המסמכים שעל המשרד לצרף לתלונה ואת הגורם מטעם המשטרה שיטפל בה.

סיכום

בחינות הבגרות הן נקודת הסיום של לימודי התלמיד בחטיבה העליונה ומשמשות כרטיס הכניסה שלו למוסדות להשכלה גבוהה. משרד החינוך אוסף, שומר ומנהל מידע רב הנוגע לבחינות הבגרות. מדובר במידע רגיש הנדרש לרמת אבטחה גבוהה ביותר ובכלל זה על המשרד מוטלת החובה לשמור על המידע, להבטיח את אמינותו, זמינותו ומהימנותו ולוודא שהוא משמש אך ורק למטרות שלשמן הוא נמסר או לצורכי מילוי חובותיו של המשרד על פי החוק. עליו לוודא כי המידע והנתונים לא ישונו או יימחקו, וכי הם ייחשפו למי שמורשה לגשת אליהם בלבד, מתוקף תפקידו או מתוקף היותו הגורם שהמידע נוגע לו כגון התלמידים או הוריהם, או למוסדות השכלה גבוהה ולגורמים אחרים הנדרשים לתעודת הבגרות ולציוני התלמידים. היבט נוסף המחייב נקיטה של אמצעים כדי למנוע פגיעה במאגרי מידע הוא תקיפות סייבר ששכיחותן הולכת וגדלה הגורמות לנזקים משמעותיים ורחבי היקף.

בביקורת הועלו כמה ליקויים בתחום אבטחת המידע - הן מתחום קיום ממשל אבטחת מידע תקין במשרד החינוך ובגופים חיצוניים שמבצעים עבורו חלק מהפעילות במיקור חוץ, והן מהתחומים הטכניים של יישום כלים, מערכות ומנגנוני אבטחת המידע והגנת הסייבר על פי הכללים שחלים עליו מתוקפן של תקנות הגנת הפרטיות והנחיות יה"ב.

בשורש הממצאים שהועלו בדוח כמה בעיות עיקריות: בכל שלבי תהליך הניהול והתפעול של בחינות הבגרות משתתפים גורמים, מערכות וממשקים רבים. אף שמשרד החינוך הוא האחראי לביצוע התהליך בכללותו, עלה כי חלק משלבי התהליך מבוצעים על ידי כמה גורמים פנימיים במשרד החינוך וכן על ידי גורמים חיצוניים רבים (זכיינים). ריבוי בעלי המידע, המערכות והממשקים גורם לחוסר אחידות, בהיבט האבטחה, בין המערכות השונות ובמסגרת התהליך בכללותו. זאת משום ששלבים שונים בתהליך הניהול והתפעול של בחינות הבגרות מבוצעים באמצעות מערכות מידע שמנוהלות בסביבות שונות ונפרדות, שחלקן אינו בשליטת משרד החינוך, ומשרד החינוך לא מקיים בקרה שוטפת על מערכות אלו כנדרש.

נוסף על כך נדרש המשרד להקפיד הקפדה יתרה על טוהר בחינות הבגרות, כדי להבטיח את עקרונות השוויוניות בין הנבחנים, ההגינות כלפיהם ומתן ביטוי נאות לרמת הידע שלהם. אחריות משרד החינוך בכלל ואגף הבחינות בפרט לניהול מערך הבגרויות ולשמירה על טוהר הבחינות באה לידי ביטוי הן לפני קיום הבחינה, הן ביום הבחינה והן לאחריה. בביקורת נמצאו מקרים המעלים חשש להפצה לא מורשית של שאלוני הבחינות והפתרונות להם, זמן קצר מאד לאחר שהבחינה החלה.

ממצאי הדוח עלולים לסכן את שלמותם, זמינותם, סודיותם ואמינותם של ציוני בחינות הבגרות וכן עולה מהם חשש לפגיעה בעקרונות טוהר הבחינות. על משרד החינוך לפעול לתיקון הליקויים שהועלו בדוח, בכלל זה לעמוד בלוחות הזמנים שנקבעו בתוכניות העבודה בתחום אבטחת המידע והגנת הסייבר, לשפר ולהעלות את רמת אבטחת המידע והגנת הסייבר בכלל מערכותיו ותשתיותיו. מומלץ גם שבמערכת החדשה לניהול ציוני הבגרות, שלדברי המשרד הוא מפתח, יינתן מענה על הממצאים שהועלו בדוח זה בנוגע לאבטחת המידע של בחינות הבגרות וציוני הבגרות.