דוח מבקר המדינה

הגנת המידע הממוחשב בבית הנשיא

▪ סיוון התשפ"ו ▪ יוני 2026

הגנת המידע הממוחשב בבית הנשיא

מבוא

נשיא מדינת ישראל הוא ראש מדינה בלתי מפלגתי המייצג את המדינה כלפי פנים וכלפי חוץ[1]. נשיא מדינת ישראל נבחר בידי הכנסת לתקופת כהונה של שבע שנים, וזאת מכוח חוק יסוד: נשיא המדינה. חלק גדול מסמכויות הנשיא הן סמכויות טקסיות באופיין, כגון חתימה על חוקים ואמנות עם מדינות חוץ, וחלק אחר מסמכויותיו הן ייחודיות, ובהפעלתן נתון לנשיא שיקול דעת, דוגמת הסמכות לחון עבריינים ולהקל בעונשם והסמכות להטיל את הרכבת הממשלה על אחד מחברי הכנסת[2]. נוסף על כך, הנשיא מייצג את מדינת ישראל בפני הקהילה הבין-לאומית ויהדות התפוצות וכן עוסק במיסוד ובהובלה של שותפויות מקומיות ובין-לאומיות בנושאים שונים, דוגמת ההתמודדות עם משבר האקלים[3]. בית הנשיא, בהיותו מוסד של המדינה, הוא גוף מבוקר מכוח סעיף 9(2) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]. לשכת נשיא המדינה נכללת ביחידות שירות המדינה, ועובדיה הם עובדי מדינה[4].

פעילותו התקינה של בית הנשיא מושפעת ותלויה בין השאר ברמת הסודיות, השלמות, הזמינות והשרידות של המידע שברשותו, גם במערכות המחשוב המעבדות ומאכסנות אותו וברכיבי התקשורת של מערכות אלה. במערכות הממוחשבות של בית הנשיא אצור מידע רב, לרבות מידע רפואי, מידע בדבר עבר פלילי, מידע ביומטרי ומידע כלכלי על קרוב ל-100,000 מבקשי חנינה. המידע ומערכות המחשוב בבית הנשיא הם נכס מרכזי וחיוני, ויש להגן עליהם ככל משאב אחר בעל ערך ארגוני. פגיעה בהם עלולה לגרום לנזקים בהיבטים תפעוליים, טכנולוגיים וכספיים, ואף לפגוע בצנעת הפרט ובסמל מרכזי של המדינה ובאופן שבו הוא נתפס בתודעה הלאומית והבין-לאומית. הדבר נכון בשגרה, ועל אחת כמה וכמה בעיתות מלחמה, כשכמות תקיפות הסייבר (סבר) מתגברת.

בית הנשיא מפעיל כמה רשתות תקשורת.

פעולות הביקורת

בחודשים מרץ עד ספטמבר 2025 ביצע משרד מבקר המדינה ביקורת בנושא הגנת המידע הממוחשב בבית הנשיא. הביקורת התמקדה ברשת המרכזית, ונבדקו הנושאים האלה: ניהול העל של הגנת המידע; הזדהות המשתמשים וניהול ההרשאות; עדכניות הגרסאות של מערכות ההפעלה והתוכנה; תשתיות רשת בית הנשיא; אבטחת תחנות קצה; והגנת הפרטיות. בדיקת השלמה נערכה ביחידה להגנת הסייבר בממשלה שבמערך הדיגיטל הלאומי. ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם נתונים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]. חסיון נתונים אלה אינו מונע את הבנת מהות הביקורת.

---

1 מבקר המדינה, **דוח ביקורת מיוחד - מינהל וכספים בבית הנשיא** (2015) עמ' 93; סעיף 1 לחוק יסוד: נשיא המדינה.

2 חוק יסוד: נשיא המדינה; חוק יסוד: הממשלה.

3 אתר בית הנשיא: https://www.president.gov.il/institution.

4 בחוק שירות המדינה (מינויים), התשי"ט-1959, ובחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998, מוגדר בית הנשיא כ"לשכת נשיא המדינה". ראו גם סעיף 41 (א) לחוק המינויים. לגבי עובדי לשכת נשיא המדינה - בידי מנהל הלשכה.

ניהול העל של הגנת המידע בבית הנשיא

בשנת 2015 החליטה הממשלה להטיל על כל אחד מהמנהלים של משרדי הממשלה ויחידות הסמך לפעול לשיפור רמת ההגנה במרחב הסייבר (להלן - החלטה 2443). הנחיית היחידה להגנת הסייבר בממשלה (להלן - יה"ב) קובעת כי הנהלת המשרד מחויבת כלפי המטרות והעקרונות של הגנת הסייבר, וכי אלה מהווים חלק בלתי נפרד מניהולו התקין של המשרד. בין היתר נקבע בהנחיית יה"ב כי יש למנות בכל אחד ממשרדי הממשלה ממונה על הגנת הסייבר ולהקים ועדת היגוי משרדית לנושאי הגנת הסייבר, שתפעל לשיפור רמת הגנת הסייבר של המשרד הממשלתי ותפקח על הפעילות השוטפת המבוצעת בתחום זה. הגם שהחלטה 2443 נוגעת למשרדי הממשלה וליחידות הסמך שלהם, ואינה נוגעת לגופים ציבוריים אחרים כגון בית הנשיא, אפשר להסיק מסקנות מתכלית ההחלטה ומהנחיית יה"ב גם בנוגע לצורך לפעול לשיפור רמת ההגנה בסייבר בבית הנשיא ובנוגע לגורמים האחראים לניהול הגנת הסייבר בו.

האסדרה בתחום הגנת הסייבר בבית הנשיא

המחוקק ומתקין התקנות התייחסו לתחום אבטחת המידע והגנת הסייבר בין היתר בחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), בחוק הגנת הפרטיות, התשמ"א-1981, ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע). כמו כן, ממשלת ישראל קבעה כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר[5] היא יעד ביטחוני לאומי חיוני של המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי[6]. בשנים 2011 ו-2015 התקבלו שלוש החלטות ממשלה[7] בנושאים האלה: קידום היכולת הלאומית במרחב הסייבר, אסדרה לאומית והסדרת האחריות לטיפול בתחום הגנת הסייבר. בהתאם להחלטות הממשלה האלה ולחוק להסדרת הביטחון, הנחיית תחום הגנת הסייבר נחלקת בין כמה גורמים. להלן רשימת גופי האסדרה המנחים בתחום הגנת הסייבר:

מערך הסייבר הלאומי: מערך הסייבר הלאומי הוקם בשנת 2017 מכוח החלטת ממשלה[8]. תפקידי המערך כוללים בין השאר קידום אסדרה לאומית בהגנת הסייבר והנחיית גופים עם תשתיות מחשוב קריטיות[9]. מערך הסייבר מסייע בביצוע מבדקי חדירה ומחקרי תקשורת בגופים המונחים על ידו. כמו כן הוא פרסם מדריך יישומי להגנת הסייבר בארגון, שהוא בגדר המלצה לכל ארגון במשק ומייצג סטנדרטים מקובלים (best practice) בתחום הגנת הסייבר (להלן - תורת ההגנה בסייבר).

יה"ב: היחידה הוקמה מכוח החלטת הממשלה 2443 מפברואר 2015[10]. על פי ההחלטה, ייעוד היחידה הוא לכוון ולהנחות מקצועית את משרדי הממשלה ויחידות הסמך בתחום הגנת הסייבר ולהקים מרכז שליטה ובקרה ממשלתי להתמודדות עם איומי סייבר (SOC ממשלתי). יה"ב גיבשה והפיצה הנחיות מסגרת להגנת הסייבר בממשלה הכוללות הוראות ונהלים המחייבים את משרדי הממשלה ומגדירות מנגנונים ותהליכי עבודה שבאמצעותם ניתן לשפר את רמת ההגנה בסייבר (להלן - הנחיות יה"ב)[11].

---

5 מרחב הסייבר - מרחב המורכב מרובד פיזי - כלל רכיבי המחשוב והתקשורת, מרחב לוגי - הקוד המפעיל את רכיבי המחשוב, ומרחב אנושי - כלל האנשים המשתמשים ברשת. מתוך **דוח מבקר המדינה - יולי 2024**, "הגנה על המידע הממוחשב במשרד ראש הממשלה", עמ' 3.

6 החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15).

7 החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11); החלטה 2443, העוסקת כאמור ב"קידום אסדרה לאומית והובלה ממשלתית בתחום הגנת הסייבר" (15.2.15); והחלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15).

8 החלטת הממשלה 3270 (17.12.17).

9 מבקר המדינה, **דוח מבקר המדינה - מרץ 2022**, "מערכות המידע והגנת הסייבר בבחירות לכנסות ה-21, ה-22 וה-23 - תחום הגנת הסייבר", עמ' 50.

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

11 מתוך אתר מערך הדיגיטל הלאומי: https://www.gov.il/he/pages/yahav_metric.

שירות הביטחון הכללי (להלן - השב"כ): על פי החוק להסדרת הביטחון, השב"כ אמון על הנחיית הגופים הציבוריים המפורטים בחוק, ובהם בית הנשיא, בכל הנוגע לאבטחת מידע מסווג מהבחינה הביטחונית, ובכלל זה מתן הנחיות מקצועיות ופיקוח על קיום הוראות החוק להסדרת הביטחון בגופים ציבוריים.

הרשות להגנת הפרטיות: הרשות מופקדת על הגנת הזכות לפרטיות בישראל, ובכלל זה על האסדרה של אבטחת המידע האישי השמור בכלל מאגרי המידע בישראל, בהתאם להוראות חוק הגנת הפרטיות ותקנות אבטחת מידע. לשם כך הרשות מוסמכת לבצע אכיפה מינהלית ואכיפה פלילית בגופים ציבוריים ובגופים פרטיים[12].

הנחיית בית הנשיא

כאמור, לשכת נשיא המדינה נכללת ביחידות שירות המדינה, ועובדיה הם עובדי מדינה.

1. **אימוץ הוראות החלות על משרדי הממשלה בתחומי ניהול ההון האנושי, הכספים והמשק:** כחלק מעצמאות בית הנשיא, חוק שירות המדינה (מינויים), התשי"ט-1959 מקנה למנכ"ל בית הנשיא סמכויות מסוימות של שר ושל נציב שירות המדינה, ולוועדת הכספים של הכנסת הוא מקנה את סמכויות ועדת שירות המדינה. בית הנשיא מאמץ בפועל את הוראות תקנון שירות המדינה (להלן - התקשי"ר)[13], תוך שמירת הסמכות לבצע בהן שינויים במקרים חריגים כאשר השינוי נדרש ומתחייב; במקרים כאלה, על ועדת הכספים של הכנסת או על מנכ"ל בית הנשיא לקבוע כללים ייחודיים לעובדי בית הנשיא. יצוין כי בית הנשיא אף מאמץ את הוראות תקנון הכספים והמשק של מדינת ישראל (להלן - התכ"ם)[14] לצורך ניהול כספיו ומשקו, בשינויים המחויבים, אף שהוא אינו משרד ממשלתי[15].

   אימוץ הוראות התקשי"ר בידי בית הנשיא, תוך שמירת הסמכות לבצע בהן שינויים במקרים חריגים כאשר השינוי נדרש ומתחייב, מונע אי-ודאות במרקם יחסי העבודה ומאפשר הישענות על גוף מקצועי כנציבות שירות המדינה, האמונה על הטיפול בענייני עובדים, זכויותיהם וחובותיהם. בדומה לכך, אימוץ הוראות התכ"ם בידי בית הנשיא, בשינויים המחויבים, מספק ודאות בנושאים הנוגעים לניהול הכספים והמשק בבית הנשיא.

2. **הוראות החלות על משרדי הממשלה בתחום הגנת הסייבר:** החוק להסדרת הביטחון מבסס את הצורך בהנחיה מקצועית של גופים ציבוריים בתחום הגנת הסייבר בהיבטים מסוימים. נוסף על כך, החלטות הממשלה 3611, 2443 ו-2444 קובעות הנחיות בתחום הגנת סייבר למשרדי הממשלה ויחידות הסמך שלהם, במטרה לשפר את רמת ההגנה בסייבר ולהפחית סיכונים הנשקפים לנכסי המידע של הגופים הכפופים, כל אחד בהתאם להוראותיו. בנוגע לגופי הממשלה - משרדי הממשלה ויחידות הסמך שלהם, יה"ב משמשת גוף מנחה מקצועי, המגבש ומפיץ הוראות ונהלים מחייבים, המגדירים מנגנונים ותהליכי עבודה לשיפור את רמת ההגנה בסייבר וכן נורמות מקובלות בתחום זה. בנוגע למידע מסווג ביטחונית, השב"כ משמש גורם מנחה לגופים הציבוריים שנקבעו בחוק האמור.

בכל הנוגע להגנה על מידע ממוחשב שאינו מסווג, לא נקבע בחוק או בדרך אחרת גורם מנחה לבית הנשיא.

---

12 מבקר המדינה, **דוח מבקר המדינה - מאי 2025**, "מערכות המידע והגנת הסייבר בבחירות לרשויות המקומיות", עמ' 14.

13 תקשי"ר - קובץ הוראות וכללים המסדיר את ניהולו של שירות המדינה בתחום משאבי האנוש והמפרט את זכויותיהם וחובותיהם של עובדי המדינה.

14 תקנון זה מתפרסם על ידי אגף החשב הכללי במשרד האוצר. הוראות התכ"ם כוללות הנחיות אופרטיביות, מקצועיות ועדכניות, המחייבות את משרדי הממשלה ואת יחידות הסמך שלהם. https://takam.mof.gov.il/about.

15 מבקר המדינה, **דוח ביקורת מיוחד - מינהל וכספים בבית הנשיא**.

נמצא כי עד ספטמבר 2024 פעל בית הנשיא ללא גורם מנחה בתחום הגנת הסייבר במערכות המידע שנבדקו בביקורת. משמעות הדבר היא שעד מועד זה לא הוחלו על בית הנשיא הכללים ודרכי הפעולה שהוחלו על משרדי הממשלה, שנועדו לשפר את רמת ההגנה בסייבר, להפחית את הסיכונים הנשקפים לנכסי המידע ולפעול בתחום זה על פי סטנדרטים בין-לאומיים. זאת, בשונה מתחומי ניהול ההון האנושי, הכספים והמשק, שלגביהם אימץ בית הנשיא זה מכבר את הכללים החלים על משרדי הממשלה, בשינויים המחויבים. בספטמבר 2024 פנה בית הנשיא ליה"ב וביקש ממנה להנחות אותו בכל הנוגע להגנת הסייבר ואבטחת המידע הבלתי מסווג.

בהתייחסות יה"ב למצאי הביקורת עלה כי במסגרת הנחיית בית הנשיא, יה"ב מקיימת מאז החלה להנחות את בית הנשיא פגישות חודשיות עם בית הנשיא; לבית הנשיא ניתנו הרשאות גישה לפורטל יה"ב המרכז בין היתר, את ההנחיות והבקרות הנדרשות; הוקם אזור אישי בפורטל עבור דוחות בקרה של יה"ב; ובקרות יה"ב שולבו בתוכנית העבודה של בית הנשיא בתחום הגנת הסייבר לשנת 2025.

לצד עצמאות בית הנשיא, ומבלי לפגוע בעצמאותו, לצורך ניהול תחומי פעולה מקצועיים הכרוך באסדרה של כללים ודרכי פעולה, ולנוכח איום מרכזי שמהווה תחום הגנת המידע והסייבר ברמה הלאומית, היה מקום שבית הנשיא יאמץ כבר לפני שנים מכלול של כללים מקצועיים אשר נקבעו ועודכנו דרך קבע בידי גורמים מקצועיים מומחים בכל אחד מהתחומים, ויפעל לאורם. בית הנשיא בחר לאמץ זה מכבר מכלול של כללים כאלה שקבע שירות המדינה בתחומי ניהול ההון האנושי, הכספים והמשק, ונכון היה לפעול בדרך זו גם בקשר לתחום אבטחת המידע והסייבר. במשך שנים פעל בית הנשיא ללא אימוץ או קביעה עצמאית של כללים מקצועיים בתחום הגנת הסייבר ואבטחת המידע הבלתי מסווג, ובספטמבר 2024 אימץ את הנחיות יה"ב בתחום זה. ממצאי הביקורת שיפורטו להלן עשויים היו לנבוע מהיעדר הנחיה מקצועית של בית הנשיא בתחום זה.

יש לראות בחיוב את פנייתו של בית הנשיא ליה"ב בספטמבר 2024, בבקשה לקבל הנחיה בכל הנוגע להגנת הסייבר ולאבטחת מידע בלתי מסווג, וכן את פעולותיו הראשוניות ליישום ההנחיות. על בית הנשיא לפעול על פי הנחיות יה"ב בתחום הגנת הסייבר ואבטחת המידע הבלתי מסווג.

מטרתו של דוח ביקורת זה היא למפות את הפערים שהיו קיימים לאורך השנים בבית הנשיא בתחום אבטחת המידע והסייבר. לצורך כך נדרשת אבן בוחן של כללים מקצועיים בתחום הגנת הסייבר ואבטחת מידע בלתי מסווג. כיוון שבמהלך השנים ועד ספטמבר 2024 לא פעל בית הנשיא בהתאם לכללים מקצועיים כאמור, נעשה המיפוי למול הכללים המקצועיים החלים על זרועות הממשלה, לרבות הנחיות יה"ב.

<u>הקמת ועדת היגוי לנושאי הגנת הסייבר וביצוע תפקידיה</u>

כאמור, בשנת 2015 החליטה הממשלה בהחלטה 2443 להטיל על כל אחד מהמנהלים של משרדי הממשלה ויחידות הסמך לפעול לשיפור רמת ההגנה במרחב הסייבר[16]. בין היתר, הוחלט להקים ועדת היגוי משרדית לנושאי הגנת הסייבר (להלן - ועדת ההיגוי), שתפעל לשיפור רמת הגנת הסייבר של המשרד הממשלתי ותפקח על הפעילות השוטפת המבוצעת בתחום זה.

על פי הנחיות יה"ב, הנהלת משרד ממשלתי ויחידת סמך ממשלתית (להלן - המשרד) מחויבת כלפי המטרות והעקרונות של הגנת הסייבר, המהווה חלק בלתי נפרד מניהולו התקין של המשרד. ועדת ההיגוי היא מסגרת ארגונית ניהולית לקבלת החלטות אסטרטגיות בתחום הגנת הסייבר ולביצוע בקרה ניהולית על אופן יישום הגנת הסייבר במשרד. יו"ר הוועדה והגורם שמופקד על הקמתה הוא

[16] החלטת הממשלה 2443 (15.2.15). מרחב הסייבר - מרחב המורכב מרובד פיזי - כלל רכיבי המחשוב והתקשורת, מרחב לוגי - הקוד המפעיל את רכיבי המחשוב, ומרחב אנושי - כלל האנשים המשתמשים ברשת.

מנכ"ל המשרד. נוסף עליו חברים בוועדת ההיגוי ממונה הגנת הסייבר במשרד, מנהל משאבי אנוש, מנהל מערכות מידע (מנמ"ר), מנהל ביטחון (הגנה פיזית), יועץ משפטי, חשב ונציג יה"ב. על הוועדה להתכנס לכל הפחות פעם בחצי שנה[17].

על פי הנחיות יה"ב, לוועדת ההיגוי 12 תפקידים, כמתואר בתרשים שלהלן.

תרשים 1: **תפקידי ועדת ההיגוי לנושאי הגנת הסייבר**

על פי הנחיות יה"ב, בעיבוד משרד מבקר המדינה.

על פי הנחיית יה"ב, ועדת ההיגוי נדרשת בין השאר ליזום סקרי הנהלה אשר נועדו לבדוק את ישימות הפעילויות המוגדרות למערכת ניהול הגנת הסייבר במשרד ואת ביצוען (להלן - סקרי הנהלה); לגבש מדדים כמותיים לטיב היישום של תשתית הגנת הסייבר במשרד; לבחון את היישום גם על פי היעדים הכמותיים שנקבעו; ולשקול, על בסיס ממצאי הסקרים, הטמעת שינויים רלוונטיים בהגנת הסייבר.

הביקורת העלתה את הממצאים האלה:

1. **ועדת ההיגוי היא המסגרת הארגונית והניהולית לקבלת החלטות אסטרטגיות בתחום הגנת הסייבר ולביצוע בקרה ניהולית על אופן יישום הגנת הסייבר במשרד. אופיים של הסיכונים הכרוכים בשימוש הנרחב במערכות המחשוב במערכת הציבורית היה יכול ללמד על הצורך בהקמתה של הוועדה כבר לפני שנים, גם בבית הנשיא. נמצא כי עד יוני 2025 לא הוקמה בבית הנשיא ועדת היגוי לנושאי הגנת סייבר.**

17 החלטת ממשלה 2443.

יצוין כי במהלך הביקורת, ביוני 2025, הוקמה לראשונה ועדת היגוי בבית הנשיא בראשות מנכ"ל בית הנשיא, ובתחילת יולי 2025 היא התכנסה לראשונה.

2. **משרד מבקר המדינה בחן אם בהיעדר ועדת היגוי בבית הנשיא עד יולי 2025 קודמו משימות מרכזיות בתחום אבטחת המידע והסייבר, המטופלות בדרך כלל בידי ועדת ההיגוי. נמצא כי משימות מרכזיות לא קודמו בבית הנשיא: הנהלת בית הנשיא לא העריכה נזקים ולא בחנה ואישרה את מפת הסיכונים המשרדית. כמו כן הנהלת בית הנשיא לא גיבשה יעדים מדידים לבחינת יישום תשתית הגנת הסייבר, לא ביצעה סקרי הנהלה ולא בדקה את ישימות הפעילויות המוגדרות למערכת ניהול הגנת הסייבר בבית הנשיא ואת ביצוען**.

בהתייחסות מפברואר 2026 מסר בית הנשיא כי ועדת ההיגוי התכנסה פעמיים מאז הקמתה, ביוני 2025. עוד מסר בית הנשיא כי בוצע תהליך של מיפוי הנכסים, וכי המיפוי טרם אושר בידי ועדת ההיגוי.

על מנכ"ל בית הנשיא, העומד בראש הנהלת בית הנשיא והמשמש יו"ר ועדת ההיגוי, לוודא כי הוועדה פועלת כנדרש בהנחיות יה"ב, ובכלל זה מאשרת את מיפוי נכסי המידע של המשרד; מאשרת מפת סיכונים ארגונית על סמך סקר סיכונים; פועלת להעלאת מודעות העובדים לסיכונים בסייבר; מקצה משאבים בהיקף הנדרש להגנה על הסייבר; ומתכנסת בתדירות הנדרשת.

<u>המדיניות ונוהלי העבודה בתחום הגנת הסייבר</u>

על פי הנחיית יה"ב, על בית הנשיא לגבש מערך מסמכים ונהלים בתחום הגנת הסייבר:

1. **המדיניות בתחום הגנת הסייבר:** מגדירה את עקרונות הגנת הסייבר של המשרד ואת המסגרות הארגוניות, לרבות בעלי התפקידים השונים שתפקידם ליישם את המדיניות ולבקר את אופן יישומה.

2. **נוהלי העבודה בתחום הגנת הסייבר:** נכתבים על בסיס מדיניות הגנת הסייבר ומגדירים את העקרונות לביצוע המדיניות ואת תהליכי הביצוע.

המדיניות בתחום הגנת הסייבר

מדיניות הגנת הסייבר היא הבסיס ליישום ולהפעלה של אמצעי אבטחה ולבחינת רמת אבטחת הסייבר הקיימת בארגון. הנחיות יה"ב קובעות כי המשרד אחראי לקבוע מדיניות להגנת הסייבר, הנגזרת בין השאר מחוקים, מתקנות ומתקן ISO 27001, וכן מתורת ההגנה של מערך הסייבר הלאומי; יש לבדוק ולאשרר את מדיניות הגנת הסייבר אחת לשנתיים, או מוקדם יותר אם חלים שינויים ניכרים במערך המחשוב או במערך הארגוני של המשרד. ועדת ההיגוי אחראית לגיבוש עקרונות המדיניות, לאישור, לאשרור ולתיקוף המדיניות ולסקירת אופן יישומה בפועל. ממונה הגנת הסייבר במשרד אחראי לגיבוש מדיניות הגנת הסייבר לצורך דיון והחלטה בעניינה בוועדת ההיגוי.

על פי הנחיית יה"ב, אלה הנושאים שצריכים להופיע במסמך המדיניות להגנת הסייבר:

1. **המבנה הארגוני של המשרד:** באמצעותו יוגדרו המסגרות הארגוניות שיישמו את המדיניות בפועל;

2. **הגנה פיזית:** הגנה על הציוד והמידע מפני גישה פיזית של גורמים לא מורשים;

3. **הגנת רשומות:** הגדרת התהליכים וכלי הטיפול הדרושים להגנה על אמצעים פיזיים ולוגיים נושאי מידע;

4. **הגנה לוגית:** מעגלי הגנה על המידע בתחומי המחשוב והתקשורת;

5. **הגנה על משאבי האנוש:** הגדרת עקרונות הגנת המידע והמערכות התומכות בו בכל הקשור לעובדי המשרד ולעובדים במיקור חוץ;

6. **ניהול וסיווג של הנכסים:** סיווג נכסי המידע וניהולם וכן קביעת הגורם האחראי לכל נכס מידע;

7. **הגנה על שרשרת האספקה:** צמצום הסיכון הנובע מחשיפה של ספקים חיצוניים למערכות ולמידע השמור בהן;

8. **טיפול באירועי הגנת הסייבר:** קביעת עקרונות דיווח וטיפול באירועי הגנת הסייבר כך שניתן יהיה לצמצם נזקים, לתקן ליקויים, לטפל משמעתית בגורמים הרלוונטיים ולהפיק לקחים;

9. **פיתוח ורכש:** שילוב הגנת הסייבר בתהליכי הפיתוח והרכש;

10. **שמירה על המשכיות תפקודית:** הגדרת עקרונות שיאפשרו את המשך פעילות המחשוב החיונית בעת חירום;

11. **תוכנית עבודה ותקציב:** גיבוש תוכנית עבודה ותקציב בתחומי הגנת הסייבר כדי לעמוד ביעדים הממשלתיים ולנתב את המשאבים הנדרשים;

12. **התאמה (compliance):** להבטיח עמידה של הארגון בדרישות החוק והתקנות הישראליות בתחום הגנת הסייבר.

נמצא כי הנהלת בית הנשיא טרם גיבשה או אישרה מדיניות להגנת הסייבר, גם לאחר שאימצה את הנחיות יה"ב המחייבות לעשות כן. לפיכך, בית הנשיא פועל בתחום הגנת הסייבר ללא מסמך מדיניות מאושר, שנועד בין היתר להבהיר מהן המסגרות הארגוניות המיישמות את הגנת הסייבר במשרד, להגדיר את העקרונות שיאפשרו גיבוש נהלים ויתמכו בהמשכיות התפקודית ולהבטיח עמידה בהוראות הדין הנוגעות להגנת הסייבר.

על ועדת ההיגוי של בית הנשיא לקבוע מדיניות להגנת הסייבר, בהתאם לנדרש בהנחיות יה"ב, ולתקפה בתדירות הנדרשת.

בהתייחסות מפברואר 2026 מסר בית הנשיא כי הוא התקשר עם חברה שעתידה לספק לבית הנשיא, עד סוף הרבעון הראשון של שנת 2026, מסמך מדיניות שיובא לדיון בוועדת ההיגוי ויאושר בידי ההנהלה.

נוהלי העבודה בתחום הגנת הסייבר

על פי הנחיות יה"ב, יש להסדיר את הפעילויות להגנת הסייבר בנהלים מאושרים בידי ממונה הגנת הסייבר. כך למשל, אפשר להסדיר בנהלים את הפעולות הנדרשות להפחתת החשיפה לאיומים ואת הסיכונים הנשקפים לארגון מהתממשות אירוע סייבר.

נהלים לאבטחת מידע נדרשים לצורך הפחתת החשיפה לאיומים ולסיכונים הנשקפים לארגון מהתממשות אירוע סייבר. אשר לנהלים בתחום הגנת הסייבר שהומצאו על ידי בית הנשיא -

מדובר ב-17 נהלים שלגביהם הועלה כלהלן: בבית הנשיא אין ממונה על הגנת הסייבר (ראו להלן), וממילא הנהלים לא אושרו בידי גורם זה, כנדרש בהנחיות יה"ב. יצוין כי כלל הנהלים לא נבחנו ולא אושרו בידי הנהלת בית הנשיא או בידי ועדת ההיגוי. שלושה נהלים גובשו בידי מנהל מערכות המידע בתקופת הביקורת ועסקו בנושאים האלה: מדיניות עבודה מרחוק; ניהול מדיה נתיקה; וגיבוי המערכת. על פי המידע שמסר ממונה אבטחת המידע בבית הנשיא, 14 נהלים נוספים, שבית הנשיא המציא, נכתבו עם כניסתו לתפקיד בנובמבר 2022 ו"אושרו במשך הזמן" בידי ראש אגף הביטחון בבית הנשיא.

נמצא אפוא כי בכל הנוגע לאבטחת מידע ברשת שנבדקה, בית הנשיא גיבש נהלים העוסקים רק בחלק מהנושאים הרלוונטיים, ואינם עוסקים בנושאי ליבה בתחום הגנת הסייבר, כגון במשתמשים ובהרשאות; בכללים לניטור של אירועים, חריגות ואיומים; במחזור חיי תוכנה; ובעדכוני מערכות הפעלה. הנהלים שגובשו לא אושרו כנדרש בהנחיות יה"ב. ליקוי זה של חסר בנהלים בבית הנשיא יוצר סיכון.

על בית הנשיא להשלים את החסר בנהלים מרכזיים ולגבש נהלים נוספים בתחום הגנת הסייבר, כנדרש.

בית הנשיא מסר בהתייחסותו לממצאי הביקורת כי במסגרת ההתקשרות עם חברה כאמור, החברה עתידה לספק לבית הנשיא, עד סוף הרבעון הראשון של שנת 2026, ערכת נהלים להגנת הסייבר, שתובא לדיון בוועדת ההיגוי ותובא לאישור ההנהלה.

<u>הערכה ומיפוי של סיכוני סייבר - סקר הערכת סיכונים</u>

סקר הערכת סיכונים (להלן - סקר סיכונים) הוא תהליך שיטתי שמטרתו לזהות נכסים ותהליכי מידע ואת האיומים הנשקפים להם, להעריך את הסיכון הנובע מאיומים אלה ולזהות את הבקרות הנדרשות לצמצום הסיכונים, תוך התחשבות בסבירות התממשותם ובנזק הפוטנציאלי הכרוך בהם. הסיכון הנבחן במסגרת סקר סיכונים מוגדר כאפשרות לחשיפה של מידע ולפגיעה במערכות המחשוב המעבדות ומאחסנות אותו וברכיבי התקשורת של הארגון, עקב ניצול פגיעויות או חולשות הקיימות בהם. סקר סיכונים משמש בסיס לקביעת תוכנית עבודה שנתית, במטרה להבטיח שמשאבי בית הנשיא יושקעו בהגנת הסייבר, בהלימה לסיכונים הנשקפים לו.

סקר סיכונים מבוצע בהתאם לתורת ההגנה בסייבר שפרסם מערך הסייבר הלאומי, ולפיה יש לבצע אותו אחת ל-36 חודשים ולתקף את ממצאיו בכל 18 חודשים. האחריות לייזום הסקר מוטלת על מנהל מערכות המידע של הארגון. על פי הנחיית יה"ב, דוח מסכם של סקר הסיכונים ישמש בסיס לתוכנית העבודה השנתית. בתרשים שלהלן מוצגים השלבים הכלולים בתהליך סקר סיכונים.

תרשים 2: **השלבים בביצוע סקר סיכונים**

על פי הנחיות יה"ב, בעיבוד משרד מבקר המדינה.

סקר סיכונים הוא מרכיב מרכזי בהגנת המידע והסייבר, והדבר עולה מתורת ההגנה בסייבר ומהנחיות יה"ב. ביולי 2025 - במהלך הביקורת וכעשרה חודשים לאחר שבית הנשיא אימץ את הנחיות יה"ב, בית הנשיא עדכן כי הוא החל לראשונה בביצוע סקר סיכונים תשתיתי, ובמסגרתו מבוצע מבדק חדירה.

יש לראות בחיוב את פעולות בית הנשיא לביצוע סקר סיכונים. על בית הנשיא להשלים את הסקר ואת הטיפול בממצאיו, להשלים את סקרי הסיכונים במערכות המידע ולטפל בממצאיהם ולבצע סקרי סיכונים בתדירות הנדרשת על פי הנחיות יה"ב.

<u>הערכה ומיפוי של סיכוני סייבר - ביצוע מבדק חדירה</u>

מבדק חדירה הוא מתקפה מתוכננת ומבוקרת על מערכת ממוחשבת שנעשית על ידי בודק ("האקר") במטרה למצוא חולשות אבטחה, את פוטנציאל הגישה לחולשות אלו ואת השימושיות שניתן להפיק מהגישה אליהן ואל המידע שהן מאחסנות. תורת ההגנה בסייבר והנחיות יה"ב קובעות כי יש לבצע מבדקי חדירה על בסיס תקופתי.

נמצא כי בית הנשיא ביצע מבדק חדירה תשתיתי חלקי בלבד.

עוד נמצא כי בית הנשיא לא ביצע מבדק חדירה ליישומים המותקנים על גבי מערכות המחשוב שלו.

בהתייחסותו לממצאי הביקורת פירט בית הנשיא פעולות נוספות שביצע לאחר הביקורת, ובכלל זאת פעולות לתיקון ליקויים שעלו בבדיקות שערך.

יש לראות בחיוב את פעולות בית הנשיא לביצוע פעולות במסגרת מבדק חדירה תשתיתי. על בית הנשיא להשלים את מבדק החדירה התשתיתי, לבצע מבדקי חדירה יישומיים ולבצע מבדקי חדירה למערכות על בסיס תקופתי, כנדרש בהנחיות יה"ב.

<u>תוכניות עבודה שנתיות</u>

על תכלית קיומה של תוכנית עבודה שנתית אפשר ללמוד מהמדריך לתכנון עבודה שנתי בגופי הממשלה (להלן - מדריך התכנון הממשלתי). תיעדוף פעילויות של משרדי הממשלה נעשה, ככלל, באמצעות קביעת תוכנית עבודה שנתית המשקפת את הפעולות שהמשרד מתכנן לבצע בתקופה נתונה, כדי לעבור מהמצב הקיים למצב עתידי רצוי שאליו הוא שואף. תכנון נכון, על פי מדריך התכנון הממשלתי, טעון פירוט של המשימות לביצוע, הגורמים האחראים לביצוען, לוחות הזמנים לביצוע, המשאבים הנדרשים והמדדים שבאמצעותם ניתן לבחון את התקדמות המשימות.

תורת ההגנה בסייבר, הכוללת המלצות לגופים במשק ומשקפת סטנדרטים מקובלים, ממליצה לבנות תוכנית עבודה להפחתת הסיכונים שאיתר הארגון בסקר הסיכונים שערך, לצורך שיפור החוסן הארגוני ויכולתו של הארגון להתגונן מפני מתקפות סייבר. תוכנית העבודה יכולה לכלול, למשל, הטמעת תהליכים ורכש פתרונות, כגון בדיקה תקופתית של הגיבויים בארגון; התקנת תוכנות הגנה על תחנות קצה; והדרכת עובדים. מהנחיות יה"ב עולה כי על ממונה הגנת הסייבר לגבש תוכנית עבודה להגנת הסייבר בהתאם למדיניות להגנת הסייבר ולהביאה לפני ועדת ההיגוי לבחינתה ואישורה.

נמצא כי הנהלת בית הנשיא לא ניהלה במהלך השנים את פעילותה בתחום הגנת הסייבר בהתאם לתוכניות עבודה ייעודיות לתחום הגנת הסייבר. עם זאת, תוכניות העבודה הכלליות של בית הנשיא כללו גם משימות הנוגעות להגנת הסייבר: תוכנית העבודה לשנת 2023 כללה שש משימות הנוגעות להגנת הסייבר, עם לוח זמנים לביצוע וציון הגורם האחראי לביצוע, ולדברי בית הנשיא ארבע מהן בוצעו ושתיים הנוספות לא בוצעו; תוכנית העבודה לשנת 2024 כללה ארבע משימות הנוגעות להגנת הסייבר, עם לוח זמנים לביצוע וללא ציון הגורם האחראי לכך, אחת מהן

עסקה בהקמת ועדת היגוי להגנת הסייבר עד פברואר 2024[18], עם זאת משימה זו בוצעה כאמור ביוני 2025.

עוד נמצא כי תוכנית העבודה לשנת 2025 כללה שתי משימות בלבד הנוגעות להגנת הסייבר, ללא לוח זמנים לביצוע וללא ציון הגורם האחראי לכך. ציון שתי משימות בלבד בתכנית העבודה ל-2025 מעלה חשש כי חסרו בה משימות ליבה חיוניות בתחום הגנת הסייבר. יוצא אפוא כי בכל הנוגע לשנת 2025, תוכנית העבודה של בית הנשיא הייתה חסרה ולא עמדה בדרישות הבסיסיות של תכנון העבודה - פירוט כלל המשימות לביצוע, קביעת לוח זמנים לביצוען וציון האחראים לכך.

כדי לשפר את החוסן הארגוני ואת יכולתו של בית הנשיא להתגונן מפני תקיפות סייבר, וכן להבטיח שמשאבי בית הנשיא יושקעו בהגנת הסייבר בהלימה לסיכונים הנשקפים לו, על בית הנשיא לבנות תוכניות עבודה שנתיות המתמקדות בתחום הגנת הסייבר, כנדרש בהנחיות יה"ב. כדי להבטיח את אפקטיביות תוכניות העבודה, יש לפרט בהן את לוחות הזמנים לביצוע ואת הגורמים האחראים לביצוע המשימות השונות ולעקוב אחר מימושן.

תקציב בית הנשיא להגנת הסייבר

כדי להבטיח שהמשרד מקצה די משאבים להגנת הסייבר, נקבע בהנחיית יה"ב כי עליו להקצות לכל הפחות 8% מתקציב תחום טכנולוגיית המידע שלו באופן ייעודי לתחום הגנת הסייבר. עוד על פי הנחיית יה"ב, ועדת ההיגוי אחראית להקצאת התקציב הייעודי להגנת הסייבר. כדי שניתן יהיה לבחון אם המשרד אכן מיישם את ההנחיות הללו, הוא נדרש לרכז נתונים על התקציבים של תחום טכנולוגיית המידע ולנהל רישום נפרד של התקציבים המופנים באופן ייעודי לתחום הגנת הסייבר[19].

נמצא כי בית הנשיא לא ניהל רישום נפרד של התקציבים המופנים באופן ייעודי לתחום הגנת הסייבר, וכדי שניתן יהיה לבדוק אם הוא מפנה את התקציבים הנדרשים לתחום הגנת הסייבר כנדרש בהנחיות יה"ב, יש לסקור את הוצאותיו בפועל לתחום זה אל מול סך הוצאותיו בתחום טכנולוגיות המידע.

סקירת ההוצאות בפועל העלתה שבית הנשיא הקצה לתחום הגנת הסייבר כ-15% מתקציב תחום טכנולוגיית המידע הכולל שלו בשנת 2023; כ-5.8% בשנת 2024[20]; ובשנת 2025 כ-11%. יש לראות בחיוב את הקצאת התקציב להגנת הסייבר בידי בית הנשיא בשנים 2023 ו-2025.

כדי להבטיח שבית הנשיא מקצה די משאבים להגנת הסייבר, עליו לנהל רישום נפרד של התקציבים המופנים לתחום זה.

משרות ליבה בתחום טכנולוגיות המידע

כאמור, בית הנשיא מאמץ בפועל את הוראות התקשי"ר, תוך שמירת הסמכות לבצע בהן שינויים במקרים חריגים כאשר השינוי נדרש ומתחייב. החל בשנת 2011 נקבעו בידי נש"ם ובהנחיית יה"ב כללים למינוי שבעה בעלי תפקידים לביצוע משימות ליבה ניהוליות בתחום ניהול מערכות המידע ואבטחת המידע.

1. **חוזר נש"ם:** במסגרת תהליך בחינת מערך המחשוב בשירות המדינה קבעה נש"ם בחוזר מיוני 2011 אשר עוגן בתקשי"ר (להלן - חוזר נש"ם) כי על משרדי הממשלה ויחידות הסמך

---

18 ביצוע תדריכי אבטחת מידע; תרגיל אבטחת מידע והדרכות בתחום הלוגי, הפיזי והאזנה; כשירות ממונה אבטחת מידע; הקמת ועדת היגוי.

19 מבקר המדינה, **דוח מבקר המדינה - יולי 2024**, "הגנה על המידע הממוחשב במשרד ראש הממשלה", עמ' 11.

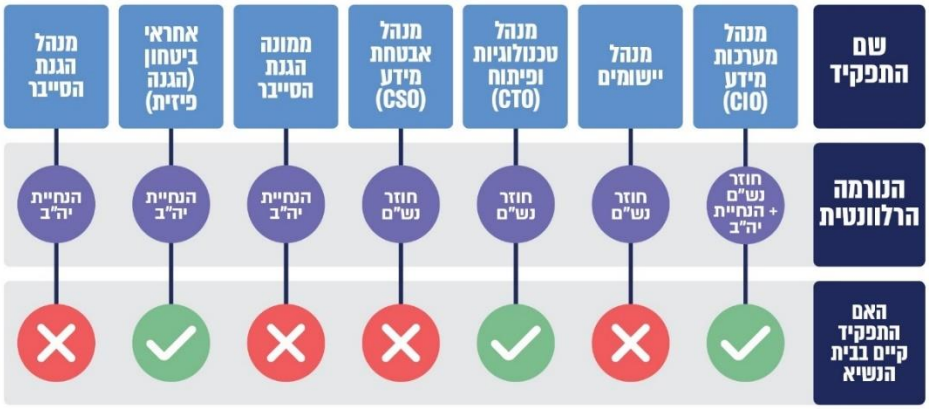
20 בית הנשיא ציין בהתייחסותו כי היקף תקציב 2024 מוסבר במגבלות התקציביות של הממשלה בשנת מלחמה.

לאייש ארבעה תפקידי ליבה טכנולוגיים: (א) **מנהל מערכות מידע** (מנמ"ר - CIO): אחראי על מכלול שירותי טכנולוגיות המידע והמחשוב של המשרד, ותפקידיו בין היתר ליזום תוכניות עבודה וליישמן, לנהל את תקציב טכנולוגיות המידע של המשרד וליזום רכש ופיתוח של חומרה ותוכנה; (ב) **מנהל יישומים**: מופקד על ניהול היישומים באגף מערכות המידע של המשרד, לרבות פיתוח, יישום והטמעה של פרויקטים ממוחשבים במשרד; (ג) **מנהל טכנולוגיות ופיתוח** (CTO): אחראי לתכנון, לתפעול ולתחזוקה של הטכנולוגיות במערכות המשרד, לרבות בחינת טכנולוגיות חדשות ואחריות לשרידות המערכות; (ד) **מנהל אבטחת מידע** (CSO): מופקד על יישום מדיניות אבטחת המידע במערכות המידע, ובין תפקידיו ליווי פרויקטים בתחום המחשוב בכל הנוגע לאבטחת מידע, הכנת תוכנית עבודה שנתית בתחום אבטחת מידע ובקרה על פעילויות ממוחשבות לשם מניעת פרצות במערכות המחשוב. בחוזר נש"ם ובתקשי"ר נקבע כי את ארבעת התפקידים יאיישו עובדי מדינה בלבד[21].

2. **הנחיית יה"ב:** הנחיית יה"ב קובעת ארבעה בעלי תפקידים בתחום הגנת הסייבר שיש למנות במשרדי הממשלה ויחידות הסמך, זאת כחלק מהמסגרות הארגוניות דוגמת ועדת ההיגוי המשרדית, שנועדו ליישם את מדיניות הגנת הסייבר במשרד. ואלה בעלי התפקידים וסמכויותיהם: (א) **ממונה הגנת הסייבר**: ימונה על ידי מנכ"ל המשרד ויהיה אחראי על התכנון, הניהול והבקרה של מכלול היבטי הגנת הסייבר בארגון, ובכלל זה גיבוש מדיניות להגנת הסייבר של המשרד, גיבוש תוכנית עבודה להגנת הסייבר בהתאם למדיניות, ניתוח והערכה שוטפים של תוכנית הגנת הסייבר בהתאם לצרכים, לאיומים ולמענים, הכנת תוכנית תקציבית לטיפול בהגנת הסייבר, ובקרה על היישום והניהול של תחום הגנת הסייבר; (ב) **מנהל מערכות מידע** (מנמ"ר - CIO): כנדרש כאמור, גם על פי חוזר נש"ם; (ג) **אחראי ביטחון** (הגנת פיזית): אחראי לתכנון, לניהול ולבקרה של מכלול היבטי ההגנה הפיזית על המידע הארגוני; (ד) **מנהל הגנת הסייבר**: אחראי בין היתר ליישום מדיניות הגנת הסייבר, בהתאם להנחיות ממונה הגנת הסייבר, לניהול ולהנחיה מקצועית בתחום הגנת הסייבר, ליישום החלטות ועדת ההיגוי המשרדית ולמעורבות בפרויקטים וברכש של מוצרים ושירותים בתחום הגנת הסייבר.

עולה כי כפועל יוצא מהתקשי"ר, מחוזר נש"ם ומהנחיית יה"ב, על בית הנשיא למנות[22] גורמים אחראים לביצוע משימות של שבעה בעלי תפקידים בתחום טכנולוגיות המידע והגנת הסייבר (להלן - תפקידי הליבה). משרד מבקר המדינה בדק האם בתקן כוח האדם של בית הנשיא מצויות משרות המופקדות על משימות של תפקידי הליבה:

תרשים 3: **תפקידי הליבה בתחום טכנולוגיות המידע ובתחום הגנת הסייבר בבית הנשיא, 2022 - 2025**



על פי נתוני בית הנשיא, בעיבוד משרד מבקר המדינה.

---

21 חוזר נש"ם, "שינויים במערך הארגוני של אגפי מערכות מידע במשרדי הממשלה וביחידות הסמך", 21.6.11, סעיף 3.3.4; חוזר נש"ם, "שינויים במערך הארגוני של אגפי מערכות מידע במשרדי הממשלה וביחידות הסמך", 21.6.11.

22 הן בחוזר נש"ם והן בהנחיית יה"ב נקבע כי יש למנות מנהל מערכות מידע (מנמ"ר), כך שעל פי שתי הנחיות אלה יש למנות שבעה בעלי תפקידים בסך הכול.

מהתרשים עולה כי בתקן כוח האדם של בית הנשיא מצויים שלושה מתפקידי הליבה: מנהל מערכות מידע (מכהן בתפקידו משנת 2009); מנהל טכנולוגיות ופיתוח (מכהן בתפקידו משנת 2020); ואחראי ביטחון (הגנה פיזית) (מכהן בתפקידו משנת 2007). יצוין כי שלושת בעלי התפקידים האלה הם עובדי מדינה.

נכון לנובמבר 2025, בתקן כוח האדם של בית הנשיא אין משרות של בעלי התפקידים הבאים: מנהל יישומים, מנהל אבטחת מידע, ממונה הגנת הסייבר ומנהל הגנת הסייבר. הלוח שלהלן מציג את תחומי האחריות והסמכות של ארבעת תפקידי הליבה שאינם קיימים בבית הנשיא.

לוח 1: **תחומי האחריות והסמכות של תפקידי הליבה שאינם קיימים בבית הנשיא**

שם התפקיד	מנהל יישומים	מנהל אבטחת מידע (CSO)	ממונה הגנת הסייבר	מנהל הגנת הסייבר
הנורמה הרלוונטית	חוזר נש"ם	חוזר נש"ם	הנחיית יה"ב	הנחיית יה"ב
תחומי האחריות והסמכות	ניהול היישומים, לרבות פיתוח, היישום והטמעה של פרויקטים ממוחשבים	יישום מדיניות אבטחת המידע במערכות המידע, לרבות ליווי פרויקטים בתחום המחשוב בכל הנוגע לאבטחת מידע, הכנת תוכנית עבודה שנתית בתחום אבטחת מידע ובקרה על פעילויות ממוחשבות לשם מניעת פרצות במערכות המחשוב	תכנון, ניהול ובקרה של מכלול היבטי הגנת הסייבר בארגון, ובכלל זה גיבוש מדיניות להגנת הסייבר; גיבוש תוכנית עבודה להגנת הסייבר; ניתוח והערכה שוטפים של תוכנית הגנת הסייבר בהתאם לצרכים, לאיומים ולמענים; הכנת תוכנית תקציבית לטיפול בהגנת הסייבר; ובקרה על היישום והניהול של תחום הגנת הסייבר	יישום מדיניות הגנת הסייבר; ניהול והנחיה מקצועית בתחום הגנת הסייבר; יישום החלטות ועדת ההיגוי ומעורבות בפרויקטים וברכש של מוצרים ושירותים בתחום הגנת הסייבר

עולה אפוא כי נכון לנובמבר 2025, בתקן כוח האדם של בית הנשיא אין ארבע משרות של בעלי התפקידים שהוגדרו בידי נש"ם ויה"ב כתפקידי ליבה: מנהל יישומים, מנהל אבטחת מידע, ממונה הגנת הסייבר ומנהל הגנת הסייבר. משכך בדק משרד מבקר המדינה, על סמך ניתוח תיאורי התפקיד, אם תחומי האחריות והסמכות של ארבעת בעלי התפקידים הללו מולאו על ידי בעלי תפקידים אחרים בבית הנשיא.

הבדיקה העלתה כי תחומי האחריות של תפקיד מנהל יישומים, אשר לדברי בית הנשיא הם באחריות מנהל מערכות מידע ונרכשים "ברכש שירותים", אינם מצויים בתיאור התפקיד של מנהל מערכות מידע; תחומי האחריות של תפקיד מנהל אבטחת מידע, אשר לדברי בית הנשיא הם באחריות ראש אגף בכיר ביטחון, חירום, מידע וסייבר ומבוצעים בפועל על ידי ממונה אבטחת מידע, אינם מצויים בהגדרות התפקיד שלהם; תחומי האחריות של תפקיד מנהל הגנת הסייבר, אשר לדברי בית הנשיא הם באחריות ראש אגף בכיר ביטחון, חירום, מידע וסייבר בתיאום עם מנהל מערכות מידע ובסיוע של שירותים חיצוניים, אינם מצויים בתיאורי התפקיד של שני בעלי תפקידים אלה.

יוצא אפוא כי תחומי ליבה של אחריות וסמכות בתחום הגנת הסייבר לא הוטלו רשמית על ממלאי תפקידים בבית הנשיא, ובכלל זה התכנון, הניהול והבקרה של מכלול היבטי הגנת הסייבר; גיבוש מדיניות הגנת הסייבר ותוכניות העבודה; ניתוח והערכה שוטפים של תוכנית הגנת הסייבר בהתאם לצרכים, לאיומים ולמענים; הכנת תוכנית תקציבית לטיפול בהגנת הסייבר ובקרה על היישום והניהול של תחום הגנת הסייבר; יישום מדיניות אבטחת המידע במערכות המידע לרבות בקרה על פעילויות ממוחשבות לשם מניעת פרצות במערכות המחשוב; וכן ניהול תחום הגנת הסייבר ומתן הנחיה מקצועית בתחום זה.

בהתייחסות לממצאי הביקורת מסר בית הנשיא כי בית הנשיא הוא גוף קטן שצרכיו אינם זהים בהכרח לצרכים של משרדי ממשלה גדולים יותר. נוכח האמור, חלק מהתפקידים בוצעו בפועל באמצעות ספקי שירותים. בית הנשיא ציין עוד כי באוקטובר 2025 פורסם מכרז למשרה חדשה של ראש אגף לתכנון, בקרה וחדשנות. לפי תיאור התפקיד שהמציא בית הנשיא, ראש האגף יופקד בין היתר על ניהול אגף המחשוב ומערכות מידע ויהיה חבר בוועדת ההיגוי לנושא הגנת הסייבר. בית הנשיא ציין כי במידה ויידרש תיקון בתיאורי שאר התפקידים, הוא יבוצע לאחר איוש המשרה החדשה והשלמת שינוי המבנה הארגוני באגף מערכות מידע, בהתייעצות עם יה"ב ובמידת הצורך עם נש"ם.

עוד ציין בית הנשיא בהתייחסותו כי תפקיד מנהל היישומים מבוצע באמצעות רכש שירותים; המשימות המוטלות על ממלא תפקיד מנהל אבטחת מידע, בוצעו בידי עובד אגף הביטחון, בשל מחסור במשרות בבית הנשיא, ומשימות אלה יוטלו בעתיד על מנהל האגף החדש לתכנון, בקרה וחדשנות.

בית הנשיא מאמץ בפועל את הוראות התקשי"ר ואת הנחיות יה"ב. לפיכך, מומלץ לבית הנשיא להשלים הטלת תחומי האחריות והסמכות על בעלי תפקידים מתאימים בתחום הגנת הסייבר.

☆

פעילותו התקינה של בית הנשיא מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות והשרידות של המידע שברשותו וכן של מערכות המחשוב המעבדות ומאחסנות אותו. לשם שמירה על המידע ועל מערכות המחשוב נדרש בית הנשיא לפעול על פי הנחיות יה"ב או לאמץ כללים מחמירים אחרים של גוף מקצועי חלופי.

הביקורת העלתה כי עד ספטמבר 2024 פעל בית הנשיא ללא גורם מקצועי מנחה בתחום הגנת הסייבר ואבטחת המידע הבלתי מסווג, ובכלל זה שלא בהתאם להוראות המנחות את הגופים הממשלתיים. בחינת תפקודו של בית הנשיא למול אבן הבוחן של ההוראות המחייבות גופים ממשלתיים העלתה פערים מהותיים. עוד העלתה הביקורת כי עד יולי 2025 בית הנשיא פעל ללא ועדת היגוי המופקדת על קבלת החלטות אסטרטגיות בתחום הגנת הסייבר ולביצוע בקרה ניהולית על אופן יישום הגנת הסייבר במשרד; הוא לא גיבש ולא אישר מדיניות להגנת הסייבר; הוא לא גיבש יעדים מדידים לבחינת יישום תשתית הגנת הסייבר ולא ביצע סקרי הנהלה באמצעות ועדת ההיגוי או פורום הנהלה חלופי.

הליקויים שהעלתה הביקורת בהיבטי ניהול העל בבית הנשיא, לצד אי-הטלת האחריות על בעלי תפקידים בתחומי הליבה של הגנת הסייבר, עלולים לגרום נזק ניכר בהיבטים תפעוליים, טכנולוגיים וכספיים ואף לפגוע בצנעת הפרט של אנשים הפונים לבית הנשיא. כמו כן הם עלולים לפגוע בסמל מרכזי של המדינה ובאופן שבו הוא נתפס בתודעה הלאומית והבין-לאומית. הדבר נכון בשגרה, ועל אחת כמה וכמה בעיתות מלחמה, כשכמות תקיפות הסייבר מתגברת. מהתייחסות בית הנשיא לממצאי הביקורת עולה שבכוונתו להמשיך ולפעול לתיקון ליקויים שעלו בביקורת.

בית הנשיא מאמץ בפועל את הוראות התקשי"ר ואת הנחיות יה"ב. לפיכך, על בית הנשיא לנהל את הגנת הסייבר בהתאם להנחיות יה"ב ולתקשי"ר.

הזדהות משתמשים וניהול הרשאות

ההגנה הלוגית[23] על המידע האגור במערכות המידע והתקשורת של הארגון נועדה בין היתר לקבוע את המגבלות הארגוניות על הנגישות למידע הארגוני ולהגדיר את השימוש המותר לכל אחד מהמשתמשים במערכות הארגון. כאשר ההגנה הלוגית אינה מוגדרת כהלכה או אינה מיושמת במלואה, תשתיות המחשוב של הארגון וכן המידע והתהליכים הנסמכים עליהן חשופים לסיכונים, כגון דליפת מידע רגיש או מסווג לגורמים שאינם מורשים לקבלו, שיבוש המידע או פגיעה בזמינותו.

קביעת מדיניות לגבי מערך הזדהות[24] אפקטיבי של המשתמשים בעת הכניסה לרשת הארגונית ויישומה בפועל וכן קביעת מדיניות לגבי מערך ההרשאות של הארגון וניהולו באופן סדור הם נדבכים מרכזיים בהגנה הלוגית[25].

בביקורת נמצאו ליקויים בעלי משקל בנושא הזדהות משתמשים וניהול הרשאות. נמצא ליקוי משמעותי מסוים בנוגע לחלק מהחשבונות הקיימים בבית הנשיא.

על בית הנשיא לתקן את הליקויים ולעמוד במלוא ההנחיות שנקבעו בעניין זה.

מתשובת בית הנשיא עולה כי החל לפעול לתיקון הליקויים.

שימוש בתיבות דוא"ל אישיות

בהנחיות יה"ב נקבע כי חל איסור להשתמש בתיבת דוא"ל פרטית לצורכי עבודה.

שימוש בתיבת דוא"ל פרטית[26] לצורכי עבודה עלול לגרום לפגיעה במידע ולתקלות מסוגים שונים: בנוגע לאבטחת מידע, שימוש כאמור עלול להגדיל את הסיכון לחשיפת המידע שהועבר בדוא"ל, בין היתר בשל הצפנה שאינה עומדת בסטנדרטים הנדרשים ובשל העובדה שתיבות דוא"ל פרטיות מקושרות לעיתים לרשתות חברתיות ולאפליקציות נוספות; המידע המתקבל בדוא"ל בענייני עבודה עלול לכלול מידע רגיש על אנשים, וחשיפתו עלולה לפגוע גם בפרטיותם; שימוש בתיבת דוא"ל פרטית עלול להוביל לאובדן מידע ארגוני ולהקשות על הארגון לבצע בקרה על תיבת הדוא"ל. היות שתיבות דוא"ל הן כלי עבודה בסיסי ונפוץ ביותר בעולם העבודה כיום, יש חשש שעובד שלא הוקצתה לו תיבת דוא"ל משרדית ישתמש בתיבת הדוא"ל הפרטית שלו גם לצורכי עבודה. משרד מבקר המדינה בחן אם הוקצתה תיבת דוא"ל לכל עובד בבית הנשיא שתפקידו מחייב, או עשוי לחייב, שימוש בדוא"ל במסגרת עבודתו השוטפת.

נמצא כי בית הנשיא לא הקצה כתובות דוא"ל משרדיות לכל עובדי בית הנשיא העושים שימוש בדוא"ל במסגרת עבודתם השוטפת וכי יש עובדים, בכמה יחידות ארגוניות בבית הנשיא, שלא הוקצתה להם כתובת דוא"ל משרדית אף שלעמיתיהם המשמשים בתפקיד זהה הוקצתה כתובת כאמור (נכון לספטמבר 2025).

מבירור שנעשה עם בית הנשיא עלה כי חלק מהעובדים שלהם לא הוקצתה תיבת דוא"ל משתמשים במחשב במהלך עבודתם. עוד על פי בית הנשיא, יש עובדים אחרים שאינם משתמשים במחשב במהלך עבודתם, ולפיכך פוחת הצורך להתקשר עימם באמצעות דוא"ל ארגוני.

---

23 הגנה המשתמשת בתוכנות ובנתונים כדי להגן על הזמינות, השלמות והסודיות של הנתונים והתהליכים הממוחשבים.

24 הזדהות היא נתון המאפשר לזהות את המשתמש, הרכיב או השירות באופן חד-ערכי.

25 אימות זהות המשתמש נעשה באמצעות נתון מיוחד הנוגע לאדם המזדהה, למשל באמצעות השוואת הסיסמה שהוא הזין לסיסמתו במאגר הסיסמאות של הארגון.

26 לרוב - של חברה מסחרית (דוגמת Gmail), להבדיל מכתובת הדוא"ל הארגונית שהנפיק לו הארגון שבו הוא עובד.

בית הנשיא לא הקצה תיבות דוא"ל משרדיות לכל עובדי בית הנשיא העושים שימוש בדוא"ל במסגרת עבודתם השוטפת, ובכך למעשה יצר פתח לשימוש לא תקין בדוא"ל - שימוש של עובדים בתיבת דוא"ל פרטית לצורכי עבודה, דבר העלול לגרום לדלף מידע ולאובדן מידע וכן לפגוע ביכולתו של בית הנשיא לבצע בקרה על השימוש בתיבות הדוא"ל.

על בית הנשיא להקצות תיבות דוא"ל משרדיות לכל העובדים העושים שימוש בדוא"ל בשגרת עבודתם ולוודא כי לצורכי עבודה ייעשה שימוש אך ורק בתיבות דוא"ל משרדיות.

בתשובתו מסר בית הנשיא כי יערוך בדיקה מקיפה לאיתור מקרים שבהם נעשה שימוש בחשבונות דוא"ל פרטיים לצרכי עבודה, ויפעל להפסיק לאלתר שימוש כזה, ככל שיימצא. כן נמסר בתשובה כי ביחס לעובדים שככלל אינם נדרשים לשימוש בדוא"ל במהלך עבודתם - יתייעץ בית הנשיא עם הגוף המנחה ויפעל על פי הוראותיו.

ניטור מערכות המידע ברשת בית הנשיא

ניטור מערכות מידע מאפשר לחשוף ניסיונות לביצוע פעולות לא מורשות במערכות, לזהות מתקפות על המערכות ולסייע בתהליך ההתאוששות מהן. על פי הנחיות יה"ב, יש לנטר מערכות מידע לרבות תשתיות מחשוב ואחסון, מערכי תקשורת והתקני קצה. הניטור מתבצע באמצעות איסוף וניתוח של מידע על פעולות הנעשות במערכות הממוחשבות ועל אירועים שמתחוללים בהן. ניטור מערכות מידע יכול שיתבצע בזמן אמת, באמצעות כלים ממוחשבים לאיתור פעולות ואירועים חריגים, או בדיעבד באמצעות ניתוח פעולות שנעשו ואירועים שקרו.

תנאי מקדים לניתוח הפעולות הוא איסוף המידע הרלוונטי. על פי הנחיות יה"ב, יש לאסוף באופן שיטתי את המידע על הפעולות המתבצעות במערכת הממוחשבת, לסננו בהתאם לכללים שנקבעו ולגבש תובנות מעשיות כבסיס לתגובה ולתיקון. התהליך אמור להתבצע באמצעות איסוף קובצי ה-Log (לוג) מרכיביה השונים של המערכת וניתוחם במרכז הגנת מידע (Security - SOC Operation Center) על פי חוקים והגדרות שנקבעו. ה-SOC אמור לזהות התרחשות של אירועים חריגים בהתאם לחוקים שהוגדרו, גם בהתחשב בצרכים העסקיים של הארגון, ולהתריע עליהם. למשל, ניתן לזהות באמצעות הניטור ניסיון של גורם זר לחדור למערכת או ניסיון להוציא מידע אל מחוץ למערכת. ארגון בגודלו של בית הנשיא, אשר כל מערכותיו מנוטרות כנדרש, צפוי לקבל עשרות עד מאות התראות בחודש, בין השאר בהתאם לאופי הפעילות ולרמת הניטור.

ניטור נדרש גם באפליקציות השונות הפועלות בארגון, בין היתר כדי לזהות פעולות חריגות המתבצעות בידי גורמים בתוך המערכת אשר עלולות להעיד על שימוש לא ראוי במערכות, כגון עובד המדפיס כמות גדולה של חומר רגיש באופן שאינו עולה בקנה אחד עם תפקידו או ניסיון של עובד לצפות במידע שאינו מוסמך לצפות בו או עובד המבקש לערוך שינויים במידע שהוא אינו מוסמך לערוך.

על פי בקרות תורת ההגנה בסייבר, כל ארגון מחויב לגבש מתודולוגיה סדורה, הנתמכת על ידי נוהל תיעוד וניטור. בנוהל יפורטו בין היתר: יעדי ההגנה שיש לנטרם; מדרג הסיכון של יעדי ההגנה; רשימת האירועים שיתועדו על ידי המערכת וישמשו מקור לשליחת התראות; קביעת הרשומות שאיסופן נדרש לצורך חקירת התראות ואירועי סייבר; ומשך שמירת הנתונים.

יצוין כי להבדיל מביצוע פעולות הניטור שיכולות להתבצע בידי גוף חיצוני בהתאם להנחיות ולהגדרות של בית הנשיא, גיבוש המתודולוגיה והגדרת סוג האירועים שינוטרו וכללי הניטור ייעשו בידי הגוף עצמו, המכיר את מערכותיו ואת יעדי ההגנה שיש לנטרם.

בנובמבר 2023 החל בית הנשיא לפעול מול ה-SOC הממשלתי (G-SOC)[27] ולחבר אליו חלק ממערכותיו. מינואר 2024 עד אוגוסט 2025 ניפק ה-SOC ארבעה דוחות חציוניים לבית הנשיא.

מדוחות שניפק ה-SOC הממשלתי עולה כי יש להבחין בין מערכות בסיסיות של משרדי ממשלה - המצויות ככלל בכל משרד (כגון FW[28] ו-NAC) ובין מערכות ייחודיות למשרד, כגון מערכת שעוסקת בתחום החנינות בבית הנשיא. כאמור, הצורך בניטור חל על כלל המערכות. יצוין כי על פי מערך הדיגיטל הלאומי, הרוב הגדול של המערכות הבסיסיות בכלל משרדי הממשלה היה מחובר ל-SOC הממשלתי.

נמצאו ליקויים המתייחסים לעמידת בית הנשיא בדרישות הנוגעות לניטור מערכות מידע.

על בית הנשיא לפעול לשיפור מערך הניטור על מערכות המידע שלו.

עדכניות הגרסאות של מערכות ההפעלה והתוכנה

חולשה (vulnerability) היא נקודת תורפה בנכס דיגיטלי או בתוכנה אשר ניתן לנצלה כדי לחולל תקיפת סייבר[29]. רכיבי מערכות המידע עלולים להיות חשופים לחולשות (להלן גם - פגיעויות). זאת, מסיבות שונות, לרבות פיתוח שגוי או לא עקבי של מוצר, דרישות אבטחה לא מספקות בשלב הפיתוח וגילוי חולשות במערכות מידע בתקופת השימוש בהן[30]. חולשות אלו עלולות לחשוף את מערכות המידע בארגון לפעילות עוינת מצד תוקף (פנימי או חיצוני).

מרשם הפגיעויות הלאומי של ארצות הברית (NVD - National Vulnerabilities Database) של המוסד הלאומי לתקינה וטכנולוגיה בארצות הברית (NIST - National Institute of Standards and Technology) מרכז מידע על פגיעויות המתגלות ברכיבי מערכות מידע ומתעד כל פגיעות באמצעות מספר סידורי חד-ערכי (CVE ID[31]). הפגיעויות המתגלות מתועדות ונרשמות. היות שהשפעתן של הפגיעויות על רכיבי מערכות המידע אינה זהה, קובע ה-NVD לכל פגיעות דירוג (CVSS - Common Vulnerabilities Scoring System) המתאר את דרגת החומרה האיכותנית של הפגיעות בסולם של 1 - 10; דירוג CVSS 7.0 - 8.9 משקף דרגת חומרה גבוהה ודירוג של 9.0 - 10.0 משקף דרגת חומרה קריטית[32]. ככלל, עם גילויה של חולשה חדשה פועל היצרן לפיתוח עדכון לתוכנה ("טלאי") שהתקנתו במערכת נועדה להתמודד עם החולשה שהתגלתה ולאיינה. יצרנים מפרסמים עדכונים כאמור מפעם לפעם, על פי הצורך או על פי מדיניות שנקבעה, כל עוד המערכת הרלוונטית מצויה בתוך תקופת התמיכה שאותה הגדיר היצרן. עם סיום תקופת התמיכה חדל היצרן מלפרסם מענה לפגיעויות המתגלות ברכיבים.

פרסום העדכון כשלעצמו אינו מבטיח את חסינותן של המערכות מפני החולשה שהתגלתה. כדי להבטיח את חסינות המערכת נדרש הלקוח המחזיק במוצר הרלוונטי להתקין את עדכון האבטחה במערכת.

---

27 בהחלטת ממשלה משנת 2015 שעסקה בקידום האסדרה הלאומית בתחום הגנת הסייבר נקבע, בין היתר, כי יוקם מרכז שליטה ובקרה ממשלתי לשם התמודדות עם איומי סייבר, גיבוש תמונת מצב ממשלתית שוטפת בהיבטי הגנת הסייבר ומתן מענה לאירועי סייבר. בהחלטה נקבע כי על משרדי הממשלה להעביר ל-SOC הממשלתי באופן שוטף דיווחים הקשורים בהגנת הסייבר, לרבות אירועי סייבר, איומים, חולשות, פוגענים ונוזקות.

28 Firewall.

29 אתר מערך הסייבר הלאומי, מילון מונחי סייבר.

30 פגיעות בעיצוב, בהטמעה, בתפעול או בבקרות הפנימיות של מערכת.

31 Common Vulnerabilities and Exposures - אתר חברת IBM; ולגבי ה-ID באתר NIST.

32 אתר NIST תחת הכותרת "Vulnerabilities Metrics".

לפיכך, שימוש במערכות המצויות לאחר תום תקופת התמיכה בהן, או שימוש במערכות המצויות בתקופת התמיכה שלהן בלי לוודא שעדכוני האבטחה שפורסמו הותקנו במערכת כנדרש ובסמוך לאחר פרסומם, חושף את רכיבי מערכות המידע שלא עודכנו לפגיעויות בדרגת חומרה קריטית, לרבות פגיעויות שנעשה בהן שימוש מוכח בידי תוקפי סייבר ברחבי העולם.

בתקנות אבטחת מידע, בהנחיות יה"ב ובבקרות תורת ההגנה בסייבר[33] נקבעו הוראות בדבר הצורך לשמור על עדכניות מערכות הארגון וכן הוראות האוסרות להשתמש בגרסאות מערכת שהגיעו לסוף תקופת התמיכה שלהן (בסעיף 13(ג) לתקנות אבטחת מידע נקבע כאמור - "לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם ניתן מענה אבטחתי מתאים"). בדיקת עדכניות רכיבי המערכת מחייבת אפוא את שני אלה: ראשית, לוודא כי הארגון אינו משתמש במערכות לאחר סוף תקופת התמיכה בהן; שנית, לוודא כי הארגון דואג להתקין, בתוך פרק הזמן הנדרש, את עדכוני האבטחה המתפרסמים לגבי המערכות שברשותו.

עדכניות רכיבי מערכות המידע בבית הנשיא

סביבות מחשוב כוללות מערכות מסוגים שונים, כגון שרתים, תחנות עבודה, מתגים[34], נתבים, "חומות אש" (Firewall, להלן גם - FW[35]), ומדפסות. הבדיקה בפרק זה התמקדה בעדכניות שרתים ורכיבי תקשורת הפועלים ברשת בית הנשיא.

מערכות ההפעלה של שרתים

מחזור החיים של מערכות ההפעלה של שרתים, כמתואר בתרשים שלהלן, כולל תקופת התמיכה העיקרית שבה, ככלל, היצרן מפרסם עדכונים למערכות ההפעלה של השרת, לרבות עדכוני אבטחה בדרגות חומרה שונות, ומאפשר שינויים והתאמות במוצר על פי הדרוש לארגון; תקופת תמיכה מוארכת שבה הארגון מקבל מהיצרן עדכוני אבטחת מידע עם אפשרות לתמיכה בתשלום; והתקופה שלאחר סוף התמיכה במוצר (להלן - סוף תקופת התמיכה או סוף מחזור החיים) שבה חדל היצרן לפתח עדכוני אבטחה למוצר, אינו מספק לו עוד תמיכה וממליץ על מעבר למוצר חלופי או לגרסה עדכנית של אותו המוצר. כאמור, שימוש בגרסת מערכת הפעלה לאחר מועד סוף התמיכה הרלוונטי לגביה עלול לחשוף את המערכת לחולשות שיפורסמו מאותו מועד ואילך וכן למצב שבו תתרחש תקלה משמעותית במערכת שלא תיתמך עוד על ידי היצרן. היות שתהליך הרכישה, ההתקנה וההטמעה של מוצרים חדשים או של גרסאות חדשות למוצרים קיימים נמשך בדרך כלל כמה שבועות לכל הפחות, יש חשיבות להיערכות מוקדמת ולתכנון מראש של לוח הזמנים לעדכון המוצרים.

תרשים 4: **תהליך מחזור החיים של מערכות ההפעלה**

על פי אתר האינטרנט של היצרן, בעיבוד משרד מבקר המדינה.

---

33 תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017, סעיף 13(ג); בקרות תורת ההגנה בסייבר, 2.0, גרסה 1.3, בקרה 6.11 (עמודה K).

34 רכיבי חומרה ברשתות מחשבים המחברים בין התקנים שונים ברשת מבטיחים מעבר יעיל של המידע ביניהם ומאפשרים לנהל את העברת המידע.

35 Firewall - אמצעי הגנה המשמש לסינון תעבורה, הצפנה וחלוקה בין מקטעי רשת על פי חלוקה מוגדרת מראש.

מצאי שרתים: בתקופת הביקורת פעלו ברשת בית הנשיא שרתים במספר גרסאות של מערכות הפעלה.

נמצא כי חלק ממערכות ההפעלה בבית הנשיא אינן נתמכות על ידי היצרן ולכן חשופות לפגיעויות.

מתשובת בית הנשיא עולה כי במהלך תקופת הביקורת החל בית הנשיא בתהליך להחלפת חלק מהשרתים שמערכת ההפעלה שלהם הייתה מצויה לאחר סוף מחזור החיים.

על בית הנשיא לוודא כי הוא אינו משתמש בשרתים הפועלים בגרסאות המצויות לאחר סוף מחזור החיים שלהן.

התקנת עדכוני אבטחה במערכות ההפעלה של שרתים

במהלך חיי המוצר, וכל עוד לא הגיע לסוף מחזור החיים שלו, מפרסם היצרן, מפעם לפעם, עדכוני אבטחה לרכיבי המערכת. עדכונים אלה נועדו להתמודד עם פגיעויות שהתגלו במערכת מאז פורסם עדכון האבטחה הקודם ולאיינן. על הארגון שמשתמש במוצר להקפיד להתקין את העדכונים במערכותיו כדי להבטיח שלא יהיה חשוף לפגיעויות אלה. כלומר, אין די בכך שהארגון מקפיד להשתמש רק במוצרים שטרם הגיעו לסוף מחזור החיים שלהם, עליו גם להקפיד להתקין במערכותיו את עדכוני האבטחה שהיצרן מפרסם מדי פעם. הימנעות מהתקנת עדכוני האבטחה חושפת את המוצרים שלא עודכנו לפגיעויות בדרגת חומרה קריטית, לרבות פגיעויות שנעשה בהן שימוש מוכח בידי תוקפי סייבר ברחבי העולם.

בהנחיות יה"ב ובתורת ההגנה בסייבר נקבע כי יש לעדכן את מערכות האבטחה הלוגיות בעדכוני האבטחה העדכניים ביותר. עדכוני האבטחה מדורגים על פי חומרת הפרצה שהם נועדו לגדור: נמוך, בינוני, גבוה וקריטי. ככלל, כאשר עדכון האבטחה מוגדר על ידי היצרן "קריטי", יש להתקינו עם פרסומו בתוך פרק זמן קצר שנקבע בהנחיות.

במהלך השנים האחרונות פרסם היצרן של מערכות ההפעלה של שרתים המצויות בבית הנשיא עדכוני אבטחה לכל אחת מגרסאות מערכות ההפעלה שבהן נעשה שימוש בבית הנשיא, ובהם גם עדכוני אבטחה קריטיים. בסך הכול פורסמו בתקופה זו עשרות עדכוני אבטחה.

עדכונים אלו כללו תיקונים שנועדו להתמודד עם פגיעויות המאפשרות הפעלת קוד עוין מרחוק על השרת הנתקף או השגת הרשאות עודפות ברשת בידי התוקף. בין העדכונים הללו נכללו גם עדכונים שנועדו להתמודד עם פגיעויות שנעשה בהן שימוש בפועל בידי תוקפי סייבר ברחבי העולם ושהן נכללו ב"קטלוג הפגיעויות המנוצלות" של הסוכנות לאבטחת סייבר ותשתיות של ארצות הברית (CISA).

נמצא כי בית הנשיא לא התקין את כל עדכוני אבטחת המידע הדרושים בחלק ממערכות ההפעלה של השרתים הפועלים אצלו, והם חשופים לפגיעויות שפורסמו.

על בית הנשיא להתקין עדכונים על גבי כל הרכיבים הפועלים ברשתות שלו, בהתאם לעדכוני האבטחה שמפרסמים היצרנים ובהתאם לאמור בהנחיות יה"ב. כמו כן מומלץ שבית הנשיא יפעל באמצעות מנגנון סדור שנועד להבטיח את עדכון המערכות.

רכיבי תקשורת

רכיבי התקשורת אחראים על ניהול תעבורת הנתונים בארגון ושולטים בזרימת הנתונים ברשתות הפנימיות ובינן ובין הרשתות החיצוניות. רכיבים אלה ממלאים תפקיד קריטי בשמירה על השלמות והאבטחה של תשתית הרשת הארגונית. כמערכות התומכות בכל תעבורת הנתונים ברשת, רכיבים אלה מהווים יעד מרכזי לגורמים זדוניים המבקשים לשבש פעולות חיוניות, להשיג גישה לא-מורשית או להוציא מידע רגיש. פגיעה ברכיבים אלה עלולה להוביל לביצוע מתקפות

MITM אשר עלולות לפגוע בסודיות, בשלמות ובזמינות של הנתונים ולגרום שיבושים תפעוליים משמעותיים[36].

בדיקת עדכניות הרכיבים בבית הנשיא התייחסה לרכיבי תקשורת - הן בנוגע לחומרה עצמה והן בנוגע לגרסאות התוכנה המותקנת עליהם. במסגרת הבדיקה נבחנו חמישה רכיבי תקשורת, שלגביהם סיפק בית הנשיא נתונים לבקשת משרד מבקר המדינה.

נמצא כי חלק מרכיבי התקשורת בבית הנשיא הגיעו לסוף מחזור החיים שלהם לפני מספר שנים.

ממצא דומה נמצא גם לגבי גרסאות התוכנה של רכיבים אלה.

בתשובתו ציין בית הנשיא כי בשנת 2024 לא הוחלפו רכיבי תקשורת מסוימים בשל שיקולי תקציב הקשורים לתקופת המלחמה.

על בית הנשיא להקפיד שלא להשתמש ברכיבי תקשורת שהגיעו לסוף מחזור החיים שלהם ולוודא שגרסאות התוכנה המותקנות ברכיבים אלו עדכניות.

אפליקציית מסד נתונים

מסדי הנתונים מופעלים באמצעות מערכת לניהול בסיסי נתונים המאפשרת לנהל כמויות גדולות של מידע, לטפל בו ולהנגיש נתונים מתוך מסד נתונים רחב. חולשות המתגלות במערכות הניהול עלולות לאפשר לתוקפים, בין היתר, השגת הרשאות גבוהות והשתלטות על השרת והנתונים המצויים בו וכך לפגוע בסודיות, באמינות ובזמינות של המידע בארגון.

לגרסאות השונות של מערכת ניהול מסדי הנתונים קובע היצרן תאריך לסיום חיי המוצר, שלאחריו אינו מספק עוד שירותי תמיכה או עדכוני אבטחה לחולשות המתגלות במוצר[37]. שימוש במוצר לאחר מועד זה חושף את המערכת לחולשות שהתגלו בו, ללא אפשרות להגן על המערכת מפניהן.

גם במהלך מחזור החיים של המוצר מפרסם היצרן מדי פעם חבילות שירות (Service Pack או SP) שהתקנתן נדרשת כדי לאפשר את המשך התקנתם של עדכוני האבטחה התקופתיים שהיצרן מפרסם. לכל חבילת שירות נקבע תאריך סיום משלה, ולאחריו לא ניתן להתקין עדכוני אבטחה חדשים ללא התקנת חבילת שירות עדכנית.

מוצר מרכזי בשרת מסדי הנתונים בבית הנשיא יגיע לסוף מחזור החיים שלו במהלך שנת 2026.

בית הנשיא לא פעל כנדרש כדי להבטיח שמסדי הנתונים שברשותו יהיו מוגנים מפגיעויות.

על בית הנשיא לפעול לתיקון הליקוי.

אפליקציה לניהול ושיתוף תוכן ומסמכים

בבית הנשיא פועלת אפליקציה המאפשרת לארגונים לנהל ולשתף תוכן ומסמכים המצויים בידי הארגון באופן יעיל ומסייעת לשפר את שיתוף הפעולה והתקשורת בין העובדים והצוותים בארגון (להלן - אפליקציית השיתוף או שרת השיתוף).

השתלטות של תוקף פנימי או חיצוני על שרת השיתוף של הארגון עלולה לחשוף את המידע האצור בו לפגיעה - ובכלל זה דליפת המידע מחוץ לארגון או צמצום זמינותו לארגון.

---

36 מתקפת "האיש שבתווך" - A man-in-the-middle attack (או בקיצור MITM) היא מתקפה שבה התוקף מכניס ציוד רשת זדוני לתעבורת הרשת באופן שגורם לציוד הרשת לחשב באופן שגוי את נתיב התעבורה וכך הוא פוגע בהזרמת המידע ברשת.

37 יצוין כי לעיתים ניתן להתקין חבילות המאפשרות המשך קבלת עדכונים, אך זאת בתשלום נוסף ולפרק זמן מוגבל בלבד.

נמצא כי אפליקציית השיתוף הפועלת בבית הנשיא אינה נתמכת עוד בידי היצרן וחלק מעדכוני האבטחה הנדרשים לא הותקנו בה ולפיכך היא חשופה לפגיעויות.

על בית הנשיא לוודא כי לא יעשה שימוש באפליקציית שיתוף המצויה לאחר תום מחזור החיים שלה, וכי יותקנו על המערכת החדשה כל עדכוני האבטחה המפורסמים על ידי היצרן בהתאם לאמור בהנחיות יה"ב.

☆

פגיעויות המתגלות במוצרי חומרה ותוכנה שבהם נעשה שימוש ברשת הארגון עלולות לחשוף את מערכות המידע בארגון לפעילות עוינת מצד תוקף פנימי או חיצוני, לרבות שימוש לא מורשה במידע בתוך הארגון, דליפת מידע אל מחוץ לארגון או חדירה של גורם עוין שעלולה לחבל במידע הארגוני או לפגוע בזמינותו. פגיעויות כאלה מתגלות חדשות לבקרים, וההתמודדות איתן מחייבת ניהול מדוקדק ומעקב אחר מחזור החיים של כלל המוצרים בארגון כדי לוודא שלא נעשה שימוש במוצרים שהגיעו לסוף מחזור החיים שלהם ואינם נתמכים עוד בידי היצרן ושכל עדכוני האבטחה שמפרסמים יצרני המוצרים מותקנים במערכות הארגון.

נמצא כי בבית הנשיא מצויות מערכות שאינן נתמכות עוד בידי היצרן, וכי בית הנשיא אינו מקפיד על התקנת כל עדכוני האבטחה המתפרסמים למוצרים השונים לרבות שרתים ורכיבי תקשורת שנבדקו. משמעות הדבר היא שחלק מהמערכות הממוחשבות של בית הנשיא חשופות לפגיעויות שונות.

על בית הנשיא לגבש מנגנון יעיל העוקב באופן שיטתי ולאורך זמן אחר מחזור החיים של המוצרים הפועלים במערכותיו ואחר פרסום עדכוני האבטחה הנוגעים להם, לוודא כי לא ייעשה שימוש במוצרים שהגיעו לסוף מחזור החיים שלהם ולהתקין בהם עדכוני אבטחה בהתאם להנחיות יה"ב ולתקנות אבטחת מידע, כדי להבטיח את הגנת המידע האצור במערכותיהם.

תשתיות רשת בית הנשיא ואבטחתה

<u>ארכיטקטורת הרשת וניטורה</u>

רשת התקשורת בארגון מהווה את עמוד השדרה, המחבר בין כלל משאבי המחשוב בארגון, הן בינם לבין עצמם והן בינם לרשת האינטרנט ולארגונים אחרים. ככלל, תשתית התקשורת היא קריטית לפעילותו היום-יומית של הארגון, והשבתתה או פגיעה בה עלולות להשפיע מהותית על הארגון. רשת התקשורת היא גם ערוץ גישה שדרכו ניתן להגיע למידע האצור במערכות הארגון. על כן נדרש לתכנן את הרשת באופן המאפשר עמידות בסיסית להתמודדות עם איומים חיצוניים ופנימיים, החל מפעילות של תוקף פנימי המנסה להגיע למשאבי רשת שאין הוא מורשה לגשת אליהם, עבור דרך כלים אוטומטיים המנסים להתבסס ברשת ולגרום בה נזק רוחבי, וכלה בתוקף ייעודי העושה שימוש בנקודת חולשה מסוימת כדי לחדור לרשת ולגנוב מידע או לגרום נזק משמעותי.

ארכיטקטורת רשת מאובטחת כוללת, בין היתר, הפרדות פונקציונליות, טכנולוגיות, תהליכיות ונוהליות בין חלקי הרשת השונים, קיום יכולות בקרה וניטור של מעבר מידע, בקרה על רכיבי הרשת ועל שינויים מבניים בה וכן סינון וחסימה של מידע חשוד. חשיבות רבה ניתנת לבקרות שנועדו להגן על חיבור הרשתות הארגוניות בינן לבין עצמן, על צומתי התקשורת בתוך הרשתות הארגוניות ועל החיבור בין הרשתות הארגוניות ובין רשת האינטרנט.

אחת מהיכולות הבסיסיות הנדרשות לאבטחת מבנה הרשת היא פילוח הרשת (Network Segmentation), להלן גם - סגמנטציה), קרי - חלוקת הרשת למקטעים או לתת-רשתות קטנות יותר ומבודדות שכל אחד מהם משרת מטרות שונות, סוגים שונים של נתונים ושירותים, סוגי משתמשים או חלוקה המבוססת על מיקום פיזי.

לצד מטרות ניהוליות, כגון שיפור יכולות השליטה והניהול, הבטחת אמינות הרשת, טיפול יעיל בתקלות, אכיפת מדיניות ושיפור ביצועים, הסגמנטציה חיונית גם לשיפור יכולות האבטחה ברשת. למשל, אם תוכנה זדונית חודרת למקטע מפולח מסוים, הנזק הנגרם מוגבל בדרך כלל לאותו מקטע ואינו מתפשט לחלקים נוספים של הרשת. כמו כן, פילוח הרשת מאפשר פריסה ממוקדת ויעילה יותר של אמצעי אבטחה, המותאמת לכל מקטע רשת, וכן זיהוי מהיר של איומים הדורשים טיפול.

סגמנטציה דורשת חלוקה של הרשת למרחבים וירטואליים בהתאם לשימושים השונים וקביעת כללים למעבר בין אזורים שונים ברשת. יישום כללים אלה מתבצע באמצעות חומות אש (FW). רכיב ה-FW משמש קו הגנה ראשון, המגביל ומאבטח את התעבורה הנכנסת לרשת הארגונית ואת התעבורה בין המקטעים בתוכה. מסיבה זו גורמים המבקשים לתקוף את הארגון מתמקדים לעיתים קרובות בפרצות בחוקי ה-FW, במטרה להשיג גישה לחלקים שונים של הרשת. בהיעדר יישום, ניהול ותחזוקה נאותים של רכיב ה-FW, נחשף הארגון לסיכונים קריטיים לאבטחת הרשת שלו, כגון החדרת תוכנות זדוניות ותנועתן בין מרכיבי הרשת, הוצאה לא-מורשית של מידע וכן קושי בניטור פעילות חריגה במעבר בין האזורים השונים ברשת (בשילוב עם כלים נוספים) ובביצוע ניתוח לאחר מעשה של פעולות תקשורת שבוצעו בה[38].

הנחיות יה"ב ובקרות תורת ההגנה בסייבר מחייבות מידור בין החלקים השונים של רשת התקשורת באמצעות חלוקת הרשת לסגמנטים, תוך הבחנה בין סגמנטים בעלי רמות רגישות שונות ותוך הגבלת התעבורה ביניהם באמצעות FW. זאת, במטרה לצמצם את מרחב התקיפה הפוטנציאלי של רשתות הארגון.

נמצא כי האופן שבו בנויה רשת בית הנשיא, אינו תואם את הנדרש על פי הנחיות יה"ב ובקרות תורת ההגנה בסייבר, ויוצר סיכון.

על בית הנשיא להתאים את מבנה הרשת לנדרש על פי הנחיות יה"ב ובקרות תורת ההגנה בסייבר.

מתשובת בית הנשיא עולה כי החל לפעול לתיקון הליקויים במבנה הרשת.

מערכת הגנה להגבלת הגישה לרשת

רשת התקשורת מהווה את ערוץ הגישה לכלל נכסי המחשוב בארגון. כתוצאה מכך, רכיב (כגון מחשב נייד) המחובר לערוץ גישה זה מחזיק בגישה פוטנציאלית לנכסי המחשוב הקיימים ברשת. חיבור רכיב שאינו מאובטח ונגוע בתוכנה זדונית עלול לאפשר לתוקף גישה לרשת הארגון. כדי להגביל את הגישה לרשת לרכיבי מחשוב מוכרים ומאושרים בלבד, נדרשים אמצעי הגנה.

נמצא כי בית הנשיא לא עומד בהנחיות יה"ב שמטרתן הגבלת הגישה לרשת.

על בית הנשיא לעמוד בהנחיות יה"ב שמטרתן הגבלת הגישה לרשת, בהקדם האפשרי.

מניעת דליפת מידע

הנחיות יה"ב והוראות תורת ההגנה בסייבר מחייבות לוודא כי הארגון הטמיע מנגנונים טכנולוגיים ואחרים להתמודדות עם דליפת מידע מרשת הארגון לגורמים זרים ולגורמים בלתי מורשים[39].

---

38 ראו מדריך אבטחת FW של מערך הדיגיטל הלאומי; מאמר באתר חברת TUFIN (פתרונות לניהול אבטחת מידע ברשת), "What is a Firewall Log Review and Why is it Significant?".

39 בקרות תורת ההגנה בסייבר.

נמצא כי בית הנשיא לא עומד במלוא ההנחיות שנקבעו בהנחיות יה"ב ובתורת ההגנה בסייבר לצורך מניעת דליפת נתונים.

על בית הנשיא לעמוד בהוראות הגופים המנחים בעניין זה.

אבטחת תחנות הקצה

תחנות קצה הן מכשירים פיזיים המתחברים לרשת הארגונית ומחליפים איתה מידע. המחשבים האישיים - נייחים וניידים - המשמשים את עובדי הארגון לצורך ביצוע עבודתם השוטפת הם, לרוב, תחנות קצה.

תחנות הקצה בארגון משמשות "דלת הכניסה" לנתונים שלו, ולכן הן יעד נפוץ לתקיפות באמצעות ניצול חולשות במערכת ההפעלה או ביישומים שונים המותקנים עליה. מעקב שוטף אחר תחנות הקצה חיוני כדי להבטיח שהן מאובטחות כנדרש וכדי לוודא שתחנות שאינן פעילות מנותקות מהרשת ולא משמשות יעד לתקיפות.

בדומה לשרתים, גם בתחנות הקצה פועלות מערכות הפעלה ואפליקציות, שבהן מתגלות חולשות מדי פעם, ולכן יש לעדכנן באופן שוטף על פי הוראות היצרן.

על פי הנחיות יה"ב, כדי שניתן יהיה לעקוב כנדרש אחר רמת האבטחה במחשבי הארגון, יש צורך בניהול מרכזי של תחנות הקצה וביצירת "תהליך ייעודי מובנה וסדור" להתקנת עדכוני אבטחה ובביצוע "סריקה עיתית באמצעות אמצעי ניטור רציף והולם". ניהול מרכזי כאמור מאפשר למנהל הגנת הסייבר לקבל מידע בדבר מצבן של תחנות הקצה בארגון ולדעת אם מותקנים בהן עדכוני האבטחה הנדרשים. תחנה שלא מעודכנת באופן שוטף בעדכוני האבטחה של היצרן עלולה להפוך לפרצת אבטחה המסכנת את המידע הארגוני. הסיכון לפרצה דרך תחנת קצה גובר כאשר הארגון מאפשר לעובדיו להתחבר לרשת המשרדית באמצעות מחשבים ניידים.

בספטמבר 2025 היו בבית הנשיא תחנות קצה ששימשו כתחנות עבודה: תחנות מחשב נייחות ותחנות מחשב ניידות המאפשרות להתחבר לרשת הארגונית מרחוק.

נמצא כי תחנות הקצה הנייחות בבית הנשיא לא נוהלו כנדרש בהנחיות יה"ב.

על בית הנשיא לוודא כי הוא מנהל את כל תחנות הקצה בארגון, כנדרש בהנחיות יה"ב.

<u>עדכניות גרסאות מערכת ההפעלה של תחנות הקצה</u>

1. בהנחיות יה"ב ובהוראות תורת ההגנה בסייבר נקבע כי חל איסור להשתמש במוצרים שהגיעו לסוף מחזור החיים שלהם, כאשר היצרן אינו תומך עוד במוצר. שימוש בגרסת מערכת ההפעלה לאחר סוף מחזור החיים עלול כאמור לחשוף את המערכת לחולשות וכן למצב שבו תתרחש תקלה משמעותית במערכת שלא תיתמך עוד על ידי היצרן. היות שתהליך הרכישה, ההתקנה וההטמעה של מוצרים חדשים נמשך בדרך כלל כמה שבועות לכל הפחות, יש חשיבות להיערכות מוקדמת לעדכון המוצרים.
נמצא כי בית הנשיא עשה שימוש בתחנות קצה במערכת הפעלה שאינה נתמכת עוד בידי היצרן, ולכן חשופה לפגיעויות.

2. במהלך מחזור החיים של המוצר מפרסם היצרן מדי פעם גרסאות עדכון למוצר שהתקנתן נדרשת כדי לאפשר את המשך התקנתם של עדכוני האבטחה התקופתיים שהיצרן מפרסם. לכל גרסת עדכון תאריך סיום משלה, ולאחריו לא ניתן להתקין עדכוני אבטחה חדשים ללא התקנת הגרסה העדכנית.

נמצא כי בחלק מתחנות הקצה פעלו גרסאות שפג תוקפן והן היו חשופות לפגיעויות.

3. על פי הנחיות יה"ב והוראות תורת ההגנה בסייבר יש לעדכן באופן שוטף מערכות המצויות בתוך מחזור החיים שלהן באמצעות התקנת עדכוני אבטחה שמפרסם היצרן. עדכונים אלו נועדו להתמודד עם פגיעויות המתגלות במערכת מדי פעם.

במערכת ההפעלה הרלוונטית התגלו במהלך השנים פגיעויות רבות ומשמעותיות.

4. נמצא כי בידי בית הנשיא לא היו נתונים על עדכון מערכות ההפעלה בתחנות קצה מסוימות, במועד כלשהו. הדבר מעלה חשש כי מערכות ההפעלה בתחנות אלה אינן מעודכנות כנדרש.

תחנות הקצה בארגון הן יעד נפוץ לתקיפות באמצעות ניצול חולשות במערכת ההפעלה או ביישומים שונים המותקנים עליה. לפיכך, מעקב שוטף אחר תחנות הקצה חיוני כדי להבטיח שהן מאובטחות כנדרש וכדי לוודא שתחנות שאינן פעילות מנותקות מהרשת ולא משמשות יעד לתקיפה. הביקורת העלתה כי בית הנשיא לא פעל כנדרש בנושא זה. ממצאים אלה משקפים היעדר שליטה של בית הנשיא בכל הנוגע לאבטחת תחנות הקצה ויוצרים סיכון.

על בית הנשיא לוודא כי הוא פועל כנדרש בכל הנוגע לניהול ואבטחת תחנות הקצה בארגון, נייחות וניידות.

מתשובת בית הנשיא עולה כי במהלך תקופת הביקורת (מאי 2025) הותקן בבית הנשיא רכיב מסוים, המהווה אמצעי לתיקון הליקויים האמורים בעתיד.

ניהול המשכיות תפקודית בעת חירום

השבתה מלאה או חלקית של מערך המחשוב עלולה להסב נזק של ממש לתחום העסקי, לתחום הכלכלי ולתדמית הארגון. תוכנית להמשכיות עסקית ותפקודית (BCP - business continuity program) היא תוכנית מקיפה המתייחסת לפעילות שארגון נדרש לבצע כדי להבטיח שבעת חירום, עקב שיבוש תהליכים עסקיים קריטיים, פונקציות עסקיות יהיו זמינות ללקוחות, לספקים ולגופים אחרים[40].

לצורך הבטחת ההמשכיות התפקודית של מערכות התקשוב החיוניות של הארגון בעת חירום, קובעות הנחיות יה"ב כי יש לגבש תוכנית להמשכיות עסקית ותפקודית, הכוללת גם תוכנית להתאוששות מאסון. תוכנית זו תתבסס על הערכת סיכונים ותפרט את האמצעים שיש לנקוט בעקבות אירוע חירום המסכן את פעילות המשרד. כמו כן התוכנית תכלול התייחסות לארבעה שלבים בעת חירום: שלב התגובה; שלב ההתאוששות; שלב השיקום; ושלב התחקור. התוכנית להמשכיות עסקית ותפקודית תובא לאישור ועדת ההיגוי לנושאי הגנת הסייבר. עקרונות התוכנית להמשכיות עסקית ותפקודית יובאו לאישור ועדת ההיגוי לנושאי הגנת הסייבר.

על פי הנחיית יה"ב, יש לבצע ניסוי הבוחן את מערך השיקום וההתאוששות של הארגון, כפי שנקבע בתוכנית ההמשכיות העסקית והתפקודית, זאת לפחות אחת לחמש שנים.

נמצא כי לבית הנשיא אין תוכנית המשכיות עסקית ותפקודית ואין ברשותו תוכנית להתאוששות מאסון המבוססת על הערכת סיכונים. כמו כן בית הנשיא לא ביצע ניסוי (תרגיל) לבחינת מערך ההתאוששות שלו, כנדרש בהנחיות יה"ב. יוצא אפוא כי בית הנשיא לא נקט מבעוד מועד את הפעולות הנדרשות כדי להבטיח שבעת חירום, עקב שיבוש תהליכים עסקיים קריטיים, פונקציות עסקיות יהיו זמינות, וכך יצומצם הנזק התפקודי והתדמיתי שעלול להיגרם לארגון.

על בית הנשיא לגבש תוכנית עסקית ותפקודית, הכוללת גם תוכנית להתאוששות מאסון, המבוססת על הערכת סיכונים ומפרטת את האמצעים שיש לנקוט בעקבות אירוע חירום המסכן

[40] הנחיות מערך הדיגיטל הלאומי, היערכות להמשכיות עסקית ותפקודית במצב חירום, 1.12.24.

את פעילות המשרד. תוכנית זו תכלול התייחסות לארבעה שלבים: שלב התגובה; שלב ההתאוששות; שלב השיקום; ושלב התחקור, ותובא לדיון והחלטה בידי ועדת ההיגוי לנושאי הגנת הסייבר. כמו כן, על בית הנשיא לבצע ניסויים (תרגילים) לבחינת מערך השיקום וההתאוששות שלו בתדירות הנדרשת בהנחיית יה"ב. כן מומלץ כי הנהלת בית הנשיא תשתתף בניסויים אלו.

בעקבות הביקורת הודיע בית הנשיא למשרד מבקר המדינה ביולי 2025 כי הוא פועל לגיבוש תוכנית המשכיות עסקית. כמו כן, בהתייחסותו לממצאי הביקורת מסר בית הנשיא כי הוא בוחן אפשרות להתקשר עם חברה המספקת מענה להתאוששות מאסון ולהמשכיות עסקית. עוד מסר בית הנשיא כי הוא נמצא בתהליך מתקדם לביצוע הערכת סיכונים שיחל, ככל הנראה, ברבעון הראשון של שנת 2026.

הגנת הפרטיות בבית הנשיא

הזכות לפרטיות הוכרה על ידי המחוקק כזכות יסוד עם חקיקתו של חוק יסוד: כבוד האדם וחירותו בשנת 1992. קודם לכן, בשנת 1981, נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), מתוך הכרה בסכנה לפגיעה בפרטיות, בין היתר נוכח ההתפתחות הטכנולוגית ונוכח הגידול בהיקף איסוף המידע וריכוזו בידי גורמים ציבוריים ופרטיים. נוסף על חוק היסוד ועל חוק הגנת הפרטיות, בשנת 2017 הותקנו תקנות אבטחת מידע, והן נכנסו לתוקף בשנת 2018.

באוגוסט 2025 נכנס לתוקף תיקון מס' 13 לחוק הגנת הפרטיות. תיקון זה הוא עדכון מקיף של חוק הגנת הפרטיות, והוא כולל שורה של הסדרים חדשים בדיני הגנת הפרטיות. ואלה התיקונים העיקריים שנעשו בו: עיגון מעמדה של הרשות להגנת הפרטיות בחוק, הבטחת עצמאותה והסדרת תפקידיה; עדכון ההגדרות בחוק והתאמתן להתפתחויות הטכנולוגיות והמשקיות; צמצום חובתם של מרבית הגופים במגזר הפרטי לרשום את מאגרי המידע שברשותם וקביעת חובת הודעה לרשות להגנת הפרטיות על מאגרי מידע גדולים המכילים מידע בעל רגישות מיוחדת; קביעת סנקציות כספיות בסכומים משמעותיים בשל הפרת החוק והתקנות; קביעת עבירות פליליות חדשות; והרחבת סמכות בית המשפט לפסוק פיצויים ללא הוכחת נזק. מאחר שתיקון מס' 13 נכנס כאמור לתוקף באוגוסט 2025, והביקורת החלה קודם לכן - במרץ 2025 - והסתיימה בספטמבר 2025, בדק משרד מבקר המדינה את עמידת בית הנשיא בדרישות חוק הגנת הפרטיות לפני כניסת התיקון לתוקף וללא ההסדרים החדשים שנקבעו בו.

<u>עמידה בדרישות החוק והתקנות</u>

מאגר מידע הוא אוסף של פרטי מידע אישי המעובד באמצעי דיגיטלי[41]. הן רשויות השלטון והן גופים פרטיים מקימים ומנהלים מאגרי מידע לצרכים שונים. בעידן הדיגיטלי נכלל מידע רב במאגרים אלה, ובמקרים רבים אין לאדם ברירה אלא לספק מידע אישי אם ברצונו לקבל מוצר או שירות. היקף המידע האגור במאגרי המידע השונים והעובדה שמדובר במידע דיגיטלי הופכים את הסכנה לפגיעה בפרטיות לחמורה יותר[42].

כדי להתמודד עם האתגרים והסכנות הנוגעים לפגיעה בפרטיות נקבע בחוק הגנת הפרטיות, לפני תיקון החוק ושינוי המצב המשפטי, כי בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע אחראי לאבטחת המידע שבמאגר המידע[43]. כמו כן, נקבעו בחוק הגנת הפרטיות ובתקנות אבטחת מידע כללים בכל הנוגע להחזקת מידע השמור במאגר ולאופן השימוש בו, ובהם הכללים האלה:

---

41 סעיף 3 לחוק הגנת הפרטיות, התשמ"א-1981. לפני תיקון מס' 13 לחוק הגנת הפרטיות הוגדר מאגר מידע "כאוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב".

42 ראו למשל עת"מ 24867-02-11 **איי.די.איי חברה לביטוח בע"מ נ' משרד המשפטים הרשות למשפט טכנולוגיה ומידע - רשם מאגרי המידע** (פורסם במאגר ממוחשב, 1.8.12), עמ' 18.

43 סעיף 17 לחוק הגנת הפרטיות, התשמ"א-1981, בנוסחו בעבר. בתיקון 13 לחוק, הוחלף המונח "בעל מאגר" במונח "בעל שליטה במאגר מידע". כמו כן, אחריות מנהל מאגר המידע הושמטה במסגרת תיקון 13 לחוק.

1. **מינוי ממונה אבטחת מידע:** על בעל מאגר מידע למנות אדם בעל הכשרה מתאימה לתפקיד ממונה אבטחת מידע. הממונה אחראי לאבטחת המידע במאגרים, ובכלל זה הוא אמון על גיבוש נוהל אבטחת מידע וכן על ההכנה והביצוע של תוכנית בקרה שוטפת לבחינת עמידת המשרד בדרישות תקנות אבטחת מידע.

2. **רישום מאגר מידע:** על פי חוק הגנת הפרטיות, על בית הנשיא לרשום את מאגרי המידע שבבעלותו במרשם מאגרי המידע המנוהל בידי הרשות להגנת הפרטיות.

3. **מסמך הגדרות המאגר:** על פי תקנות אבטחת מידע, על בעל מאגר מידע לכתוב מסמך הגדרות מאגר, שיכלול בין היתר את תיאור פעולות האיסוף והשימוש במידע; את מטרות השימוש במידע; את סוגי המידע הכלולים במאגר; את הסיכונים הנשקפים למאגר ואת אופן ההתמודדות איתם.

4. **מיפוי המאגר:** על פי תקנות אבטחת מידע, יש לגבש מסמך מעודכן של מבנה המאגר וכן רשימת מצאי מעודכנת של מערכות המאגר, לרבות מערכות חומרה, רכיבי תקשורת, מערכות תוכנה ותרשים הרשת שעליה פועל המאגר.

5. **נוהל אבטחה:** על פי תקנות אבטחת מידע, חובה לגבש נוהל שיכלול בין היתר הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר; הרשאות הגישה; תיאור אמצעי ההגנה על המאגר ואופן הפעלתם; תיאור הסיכונים הנשקפים למאגר; אמצעי הזיהוי והגישה למאגר; והוראות בנוגע לגיבוי נתוני המאגר.

6. **גישה ובקרה על הגישה למאגר המידע:** על פי תקנות אבטחת מידע, על בעל המאגר לקבוע את הרשאות הגישה למאגר המידע ולמערכותיו, בהתאם להגדרות התפקיד של בעל הרשאת הגישה למאגר ובמידה הנדרשת לביצוע התפקיד בלבד. כמו כן יש לנהל רישום מעודכן של התפקידים והרשאות הגישה שניתנו להם, וכן לתעד את בעלי ההרשאות שממלאים את התפקידים הללו בפועל.

מאחר שבית הנשיא הוא גוף ציבורי כהגדרתו בחוק הגנת הפרטיות, חלה על מאגרי המידע שלו רמת אבטחה בינונית לפחות[44]. על מאגר מידע המחויב ברמת אבטחה בינונית חלות חובות נוספות ומוגברות בכל הנוגע לניהול המאגר, ובהן בין היתר: **גיבוש נוהל אבטחה ייעודי**[45] למאגר, המתייחס לאמצעי הזיהוי והאימות לצורך גישה למאגר; **ועריכת ביקורת על עמידה בהוראות תקנות אבטחת מידע** בידי גורם שאינו ממונה אבטחת המידע במשרד, לכל הפחות אחת ל-24 חודשים. כמו כן, על הגוף לנהל **מנגנון תיעוד אוטומטי** שבאמצעותו ניתן יהיה לבצע בקרה על הגישה למערכות המאגר, לרבות זהות המשתמש; מועד ניסיון הגישה (התאריך והשעה); סוג הגישה; היקפה; והאם הגישה אושרה או נדחתה[46].

יצוין כי על כל מאגר מידע, לרבות מאגר מידע של גוף ציבורי, המכיל מידע על 100,000 אנשים ומעלה, ושבו כלולים פרטים רגישים כגון מידע רפואי, עבר פלילי, מידע ביומטרי ומידע כלכלי, חלה רמת אבטחה גבוהה (מעבר לרמת אבטחה בינונית)[47], המחייבת את בעל המאגר לנקוט פעולות נוספות. בין היתר עליו לערוך סקר לאיתור סיכוני אבטחת מידע (סקר סיכונים) לפחות אחת ל-18 חודשים וכן לבצע מבדק חדירה למערכות המאגר לשם בחינת עמידותן בפני סיכונים פנימיים וחיצוניים לפחות אחת ל-18 חודשים.

---

44 סעיף 1(2) לתוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

45 סעיף 4 (ד) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

46 סעיפים 10 ו-16 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

47 סעיף 1 לתוספת השנייה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

לבית הנשיא יש שבעה מאגרי מידע. להלן פרטי המאגרים:

1. **מאגר החנינות:** לנשיא המדינה נתונה סמכות לחון עבריינים ולהקל בעונשם[48]. כל אדם רשאי לפנות בבקשת חנינה לנשיא המדינה בעצמו, באמצעות בא כוחו או באמצעות בני משפחה מדרגה ראשונה. ניתן להגיש את הבקשה באופן מקוון, בדוא"ל, בפקס או באמצעות דואר רגיל. הבקשה תכלול פרטים אישיים (שם, כתובת, מספר תעודת זהות ודרכי התקשרות); את מהות הבקשה; את פרטי העבירה והחלטות בית המשפט בעניינה; את מועד תחילת ריצוי העונש שלגביו מבוקשת החנינה; את נימוקי הבקשה כגון נסיבות ביצוע העבירה, נסיבות אישיות ומשפחתיות וכן נימוקים רפואיים, סוציאליים, כלכליים ושיקומיים (המידע והפרטים האלה יכונו להלן - מאגר החנינות)[49]. מאגר החנינות מכיל אפוא גם מידע בעל רגישות מיוחדת, כהגדרתו בחוק הגנת הפרטיות, על מבקשי החנינה, לרבות עברם הפלילי ומצבם הרפואי והכלכלי. נכון למועד סיום הביקורת מאגר החנינות מכיל מידע על 99,709 אנשים. בשנים 2023 עד 2024 נפתחו בבית הנשיא 1,568 ו-1,928 בקשות חנינה, בהתאמה. בהתאם לקצב פתיחת תיקי החנינה בשנים אלה, מאגר החנינות צפוי להכיל מידע על 100,000 אנשים ומעלה בתוך זמן קצר.

2. **מאגר פרטי עובדים:** המאגר מכיל מידע אישי על עובדי בית הנשיא, המתועד במערכת קליטה דיגיטלית - "מרכב"ה". נכון למועד סיום הביקורת הכיל מאגר פרטי עובדים מידע על כ-180 עובדים.

3. **מאגר התאמה ביטחונית:** המאגר מכיל מידע בעל רגישות מיוחדת על עובדי בית הנשיא (בהווה ובעבר) בדבר ההתאמה הביטחונית שלהם לתפקיד המחייב רמת סיווג ביטחוני מוגברת. ובכלל זה שם העובד, המען שלו, אמצעי זיהוי לרבות דרכון, מידע על השירות הצבאי או הלאומי, המספר האישי הצבאי, דרכי התקשרות, תאריך הלידה, תאריך העלייה, הדת, הלאום, החשבונות ברשתות החברתיות, המעמד האזרחי, ההשכלה, העבר התעסוקתי, היסטוריית ביקורים בחו"ל, מידע על בני המשפחה, מידע כלכלי, מידע פלילי, מידע רפואי ופעילות חברתית. נכון למועד סיום הביקורת הכיל מאגר התאמה ביטחונית מידע על כ-800 עובדים.

4. **מאגר פניות הציבור:** פניות הציבור הן ערוץ קשר בין ציבור הפונים ובין נשיא המדינה. מאגר זה מכיל את שם הפונה, המען שלו, אמצעי זיהוי, דרכי ההתקשרות ותוכן הפנייה[50]. נכון למועד סיום הביקורת הכיל מאגר פניות הציבור מידע על 65,987 אנשים.

5. **מאגר מערכת מבקרים:** במאגר זה נשמרים פרטי המבקרים בבית הנשיא, והוא מכיל את שם המבקר, המען שלו, אמצעי זיהוי, דרכי ההתקשרות, תאריך הלידה, תפקיד המבקר, השייכות הארגונית ומספר רישיון הרכב. נכון למועד סיום הביקורת הכיל מאגר מערכת מבקרים מידע על 120,876 אנשים.

6. **מאגר ספקים:** המאגר מכיל מידע על הספקים החיצוניים בבית הנשיא, ובכלל זה המספר המזהה של החברה (ח"פ), אמצעי הזיהוי ודרכי ההתקשרות. נכון למועד סיום הביקורת הכיל מאגר ספקים מידע על כ-17,873 ספקים.

7. **מאגר מצלמות אבטחה:** המאגר מכיל מידע חזותי המתועד באמצעות מצלמות האבטחה בבית הנשיא.

---

48 סעיף 11(ב) לחוק יסוד: נשיא המדינה.

49 אתר בית הנשיא, נכון ליום 16.11.25.

50 אתר בית הנשיא:
https://govforms.gov.il/mw/forms/ContactUs@president.gov.il?gbxid=0#!herAddress

כמות המידע האגור במאגרי מידע דיגיטליים יוצרת סכנה חמורה לפרטיות. משום כך עוגנו בחוק ובתקנות דרישות שנועדו להבטיח את פרטיות האנשים שמידע אישי עליהם מופיע במאגרים אלו. בית הנשיא, כגוף ציבורי, נדרש לעמוד בדרישות מחמירות בכל הנוגע לאבטחת המידע והגנת הפרטיות במאגרים שברשותו. דרישות אלו חלות בין היתר על מאגר החנינות, שבו מצוי מידע רגיש על קרוב ל-100,000 מבקשי חנינה, ועל מאגר התאמה הביטחונית, שבו מצוי מידע רגיש על מאות עובדי בית הנשיא בהווה ובעבר.

בביקורת נמצא כי בית הנשיא לא קיים חלק מהוראות הדין החלות על כלל הגופים המחזיקים במאגרי מידע: לא מונה ממונה אבטחת מידע האמון על אבטחת המידע במאגרים; לא גובש מסמך הגדרות מאגר; לא מופו מאגרי המידע, ולא הוכנה רשימת מצאי של מערכות המאגרים; לא גובש נוהל אבטחה הכולל הוראות בדבר האבטחה הפיזית והסביבתית של אתרי המאגר והרשאות הגישה אליהם; לא נקבעו הרשאות גישה של עובדים למאגרים ולמערכותיהם; ולא נוהל רישום מעודכן של התפקידים והרשאות הגישה שניתנו לעובדים. כמו כן, נמצא כי בבית הנשיא אין מנגנון תיעוד אוטומטי המאפשר ביצוע בקרה על הגישה למערכות המאגרים, כנדרש בתקנות אבטחת מידע.

בית הנשיא מסר למשרד מבקר המדינה במהלך הביקורת ולאחר שהועברו אליו שאלות הביקורת, כי לאור תיקון החקיקה בתחומי הגנת הפרטיות שנכנס לתוקף באוגוסט 2025[51], פנה בית הנשיא ליועץ המשפטי של הרשות להגנת הפרטיות כדי ללמוד את התיקון; כי הוא מיפה את מאגרי המידע שברשותו, כחלק מההיערכות לרישומם; וכי הוא פועל למינוי ממונה אבטחת מידע. יצוין כי עד מועד סיום הביקורת לא מונה בבית הנשיא ממונה אבטחת מידע למאגרים.

על בית הנשיא לפעול על פי הוראות חוק הגנת הפרטיות ותקנות אבטחת מידע, ובכלל זה עליו למנות ממונה אבטחת מידע למאגרי המידע; לגבש מסמך הגדרות למאגרי המידע; למפות את מאגרי המידע; לגבש נוהל אבטחה לכל אחד ממאגרי המידע; ולקבוע את הרשאות הגישה שיקבל כל עובד למאגרי המידע ולמערכותיהם, זאת בהתאם להגדרות תפקידו ובמידה הנדרשת לביצוע התפקיד בלבד.

כמו כן, על בית הנשיא לערוך ביקורת על עמידה בהוראות תקנות אבטחת מידע על ידי גורם שאינו ממונה על אבטחת המידע בבית הנשיא לצורך ביצוע ביקורת על העמידה בהוראות תקנות אבטחת מידע, וזאת לכל הפחות אחת ל-24 חודשים.

מאחר שמאגר החנינות צפוי להכיל, בתוך זמן קצר, מידע על 100,000 אנשים ומעלה, על בית הנשיא להיערך לביצוע הפעולות הנדרשות מגוף המחזיק במאגר מידע הטעון רמת אבטחה גבוהה, ובהן עריכת סקר לאיתור סיכוני אבטחת מידע (סקר סיכונים) לפחות אחת ל-18 חודשים וביצוע מבדק חדירה למערכות המאגר לשם בחינת עמידותן בפני סיכונים פנימיים וחיצוניים אחת ל-18 חודשים לפחות[52].

<u>מיקור חוץ במאגר מידע</u>

ארגונים רבים, גם במגזר הציבורי, מסתייעים בנותני שירותים חיצוניים באמצעות מיקור חוץ. ככלל, נותני שירותים חיצוניים אינם חלק מהמערך הארגוני של המשרד, ובמקרים רבים הם מספקים שירות למגוון ארגונים בו-זמנית. מאפיינים אלה של נותני שירותים חיצוניים טומנים בחובם סיכוני סייבר ואבטחת מידע. תקנות אבטחת מידע קובעות כללים מחייבים בכל הנוגע להתקשרות עם ספק חיצוני בהסכם לאספקת שירותים הכרוך במתן גישה למאגר מידע של הארגון.

על פי תקנות אבטחת מידע, אשר נכנסו לתוקף כאמור ב-2018, על בעל המאגר לבחון, לפני ביצוע ההתקשרות עם ספק נותן שירותים, את סיכוני אבטחת המידע הכרוכים בהתקשרות עימו.

---

51 תיקון 13 לחוק הגנת הפרטיות, בתוקף מ-14.8.25.

52 סעיף 5 (ג), (ד) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

עוד נקבע בתקנות כי לאחר שהארגון בחן כאמור את סיכוני אבטחת המידע הכרוכים בהתקשרות עם נותן שירותים חיצוני, ולפני ביצוע ההתקשרות, עליו לעגן בהסכם ההתקשרות בין היתר את הנושאים האלה: המידע שהספק רשאי לעבד ומטרות השימוש המותרות במידע זה; המערכות שהספק רשאי לגשת אליהן והפעולות שהוא מורשה לבצע בהן; אופן השבת המידע למשרד בסיום ההתקשרות; אופן יישום החובות שנקבעו בתקנות אבטחת מידע במסגרת אספקת השירותים למשרד; חיוב הספק לדווח למזמין השירותים על עמידתו בהוראות תקנות אבטחת מידע ועל כל אירוע אבטחת מידע אם התקיים[53].

בשנים 2019 עד 2022 התקשר בית הנשיא בהסכם עם נותן שירותים חיצוני לצורך אספקת שירותי אפיון, פיתוח, תמיכה ותחזוקה של מאגר החנינות. על פי ההסכם, הספק נדרש לפתח את מאגר החנינות בהתאם לדרישות בית הנשיא, לרבות ביצוע שינויים ושיפורים במאגר, וכן להעניק שירותי תמיכה טכנית, הטמעה, הדרכה, תיקון תקלות, ייעוץ וליווי.

בהתייחסות מפברואר 2026 מסר בית הנשיא כי לפני ההתקשרות עם ספק השירותים בשנת 2019 בוצעה בדיקה ביטחונית ביחס לספק; הספק עבר תהליך סיווג ביטחוני; הספק עבר הדרכה מתאימה; ההתקשרות עם הספק בוצעה לאחר אישור גורם מנחה. בית הנשיא ציין עוד כי ההתקשרות עם ספק השירותים השני החל בשנת 2022, לא חייבה חתימה על הסכם התקשרות בשל ההיקף הכספי הקטן, וכי הספק עבר בדיקה ביטחונית, הוא בעל סיווג ביטחוני מתאים ועבר תשאול ייעודי. הספק שנתן שירותים לבית הנשיא בשנים 2019-2022 ציין בהתייחסותו כי הסיווג הביטחוני שלו נבדק; כי הוקנתה לו גישה למערכת חנינות בלבד; כי הפעילות נעשתה במחשבים פיזיים של בית הנשיא, ללא התחברות מרחוק וכי המידע לא יצא מחוץ לבית הנשיא.

מאגר החנינות של בית הנשיא מכיל כאמור מידע רגיש ואישי של קרוב ל-100,000 מבקשי חנינה, לרבות נתונים רפואיים, סוציאליים וכלכליים. משנת 2019 קיבל בית הנשיא שירותים מספק חיצוני לצורך הטיפול במאגר זה. אף על פי כן, נמצא כי בית הנשיא לא פעל כנדרש בתקנות אבטחת מידע בכל הנוגע לקבלת שירותים אלה מהספק: הוא לא ביצע בדיקה מקדימה בנוגע לסיכוני אבטחת המידע הכרוכים בהתקשרות עם הספק החל בשנת 2019; בהסכם ההתקשרות עם הספק לא עוגנו הוראות בדבר המידע שהספק רשאי לעבד והמטרות שלשמן בלבד הוא רשאי להשתמש במידע שעיבד; לא פורטו המערכות שהספק רשאי לגשת אליהן והפעולות שהוא מורשה לבצע; לא נקבע מנגנון להשבת המידע לבית הנשיא בסיום תקופת ההתקשרות; ולא הוטלה על הספק החובה לדווח לבית הנשיא על עמידתו בהוראות תקנות אבטחת מידע, ואף לא על אירוע אבטחת מידע במאגר, אם התרחש.

לצד האמור יצוין כי על פי התייחסויות בית הנשיא והספק לממצאי הביקורת, הסיווג הביטחוני שלו נבדק ופעילותו נעשתה במשרדי בית הנשיא. הספק ציין עוד כי הוקנתה לו גישה למערכת חנינות בלבד; הפעילות נעשתה במחשבים פיזיים של בית הנשיא, ללא התחברות מרחוק; והמידע לא יצא מחוץ לבית הנשיא.

כמו כן נמצא כי החל בשנת 2022 מקבל בית הנשיא שירותי תמיכה למאגר החנינות מספק שירותים חיצוני ללא הסכם תקף. לפיכך לא עוגנו בהסכם מחייב ההוראות הנדרשות להסדרת אופן ההתקשרות עם ספק חיצוני, שנועדו להתמודד עם האתגרים והסכנות הנוגעים לפגיעה בפרטיות וכרוכים בהתקשרות כאמור.

על בית הנשיא לפעול על פי תקנות אבטחת מידע בכל הנוגע לקבלת שירותים מספק חיצוני המורשה לגשת למאגר מידע של בית הנשיא. כמו כן, עליו לעגן בהסכם ההתקשרות עם הספק את ההתניות והכללים הנדרשים על פי תקנות אבטחת מידע.

---

[53] סעיף 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

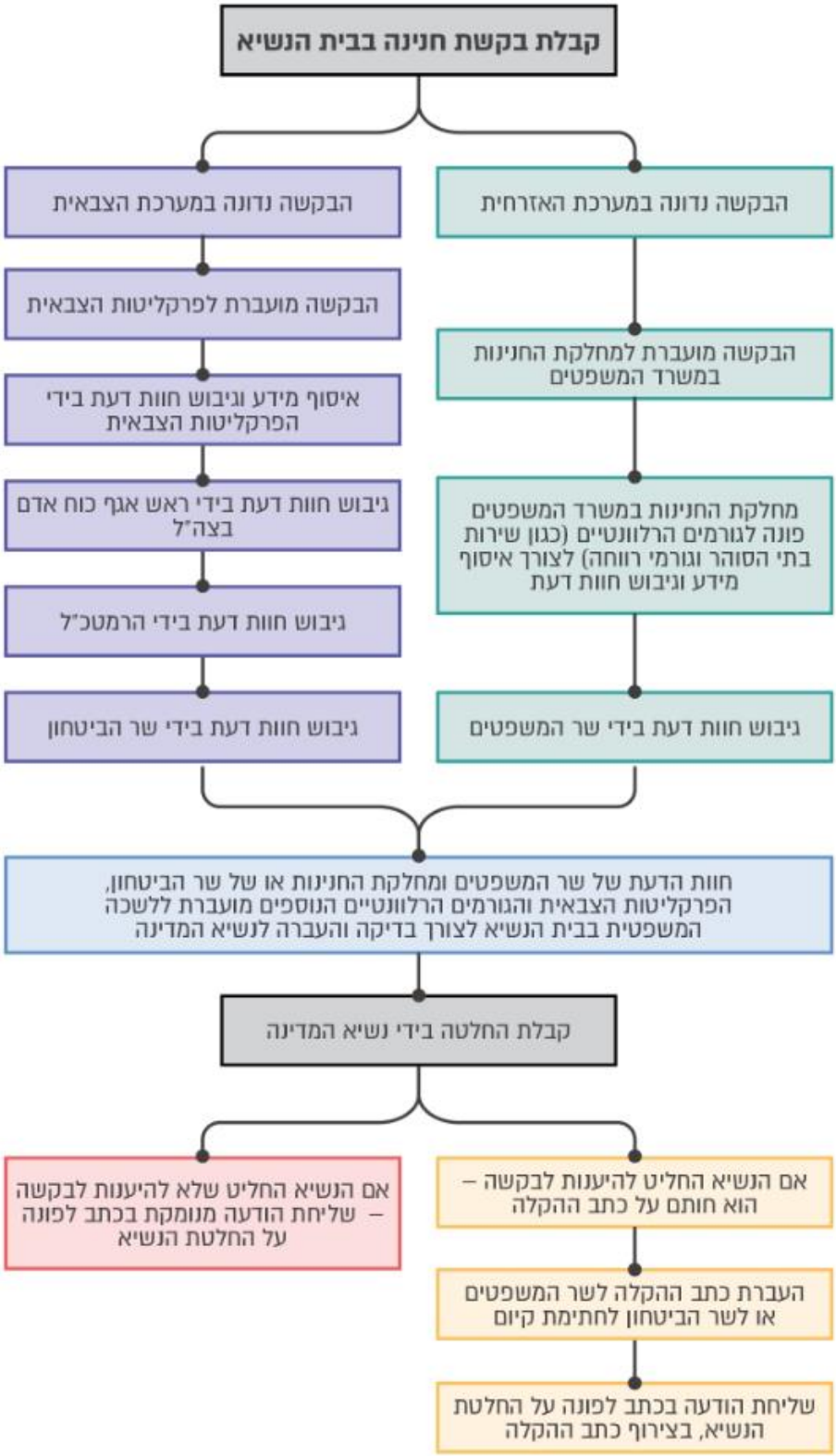
בהתייחסותו מפברואר 2026 בית הנשיא מסר כי בעקבות הביקורת הוא יקיים בחינה של ההתקשרויות בתחום מערכות המידע, כדי לזהות התקשרויות המצריכות קיום הסכם ובדיקה מקדמית.

העברת מידע ממאגר החנינות לגופים ממשלתיים

מאגר החנינות כולל מידע בעל רגישות מיוחדת, כהגדרתו בחוק הגנת הפרטיות[54], כגון פרטים אישיים (השם, הכתובת, מספר תעודת הזהות ודרכי ההתקשרות), נסיבות אישיות ומשפחתיות וכן נימוקים רפואיים, סוציאליים, כלכליים ושיקומיים. תהליך הטיפול בבקשת חנינה המוגשת לבית הנשיא מתואר בתרשים שלהלן:

[54] "מידע בעל רגישות מיוחדת" - לרבות: (א) מידע אישי על צנעת חיי המשפחה של אדם, על צנעת אישותו ועל נטייתו המינית; (ב) מידע אישי המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי כהגדרתו בחוק זכויות החולה, התשנ"ו-1996; (ג) מידע אישי שהוא מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000; (ד) מידע אישי שהוא מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב; (ה) מידע אישי על מוצאו של אדם; (ו) מידע אישי על אודות עברו הפלילי של אדם; (ז) מידע אישי שהוא הערכת אישיות שנערכה מטעם גורם מקצועי שכדרך עיסוק מחווה דעתו על אישיותו של אדם, או שנערכה באמצעי שמיועד לביצוע הערכה של מאפייני אישיות מהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים; (ט) מידע אישי על נתוני שכר של אדם ועל פעילותו הפיננסית.

תרשים 5 : **תהליך הטיפול בבקשת חנינה המוגשת לבית הנשיא**



המקור : אתר בית הנשיא, בעיבוד משרד מבקר המדינה.

מהתרשים וממידע נוסף עולה כי בית הנשיא מקבל בקשות לחנינה, והטיפול בבקשות הללו נדון במסלול אזרחי או צבאי[55]. כאשר הבקשה נדונה במסלול האזרחי, בית הנשיא מעבירה למחלקת החנינות במשרד המשפטים. מחלקת החנינות במשרד המשפטים פונה לגורמים הרלוונטיים, כגון שירות בתי הסוהר, משטרת ישראל וגורמי רווחה או רפואה, לצורך איסוף מידע וגיבוש חוות דעת. חוות הדעת של מחלקת החנינות מועברת לשר המשפטים, המגבש חוות דעת מטעמו ומעבירה יחד עם חוות דעת מחלקת חנינות במשרד המשפטים ללשכה המשפטית בבית הנשיא לצורך גיבוש חוות דעת מטעמה ולצורך קבלת החלטה בידי הנשיא. כאשר הבקשה נדונה במסלול הצבאי, בית הנשיא מעבירה לפרקליטות הצבאית. הפרקליטות הצבאית פונה לגורמים הרלוונטיים לצורך איסוף מידע וגיבוש חוות דעת, ולאחר מכן מגובשות חוות דעת גם בידי אגף כוח אדם בצה"ל והרמטכ"ל והן מועברות לשר הביטחון המגבש חוות דעת מטעמו. חוות הדעת של שר הביטחון יחד עם חוות דעת הפרקליטות הצבאית והגורמים הרלוונטיים הנוספים מועברות ללשכה המשפטית בבית הנשיא לצורך גיבוש חוות דעת ולצורך קבלת החלטה בידי הנשיא.

1. בתקנות אבטחת מידע נקבע כי "העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות"[56]. דוגמה לשיטות הצפנה מקובלות היא שימוש בתיבות דוא"ל מוצפנות ("כספות") וכן העברת קבצים המוגנים על ידי סיסמה ומנגנון הצפנה ייעודי במערכת דוא"ל רגילה. הנחיה זו נקבעה גם בתורת הגנת הסייבר, ולפיה כל ארגון נדרש לקבוע מנגנוני הצפנה למידע רגיש המועבר בין מערכות הארגון ובין משתמש קצה של ארגון אחר על גבי תווך תקשורת ציבורי, כגון רשת האינטרנט. לפי יה"ב, העברת מידע ממאגר מידע בדוא"ל מתאפשרת כל עוד הדוא"ל מוצפן ומפתח ההצפנה או הסיסמה מועברים בנפרד. לפי יה"ב, העברת מידע מיטבית תבוצע באמצעות מנגנון כספות או מערכת ייעודית שזו מטרתה.

נמצא כי בית הנשיא מעביר למשרד המשפטים ולפרקליטות הצבאית בקשות חנינה המכילות מידע ממאגר החנינות, באמצעות דוא"ל, דהיינו דרך רשת האינטרנט - ללא הצפנה. בדרך הזו מועברים גם פריטי מידע בעל רגישות מיוחדת, כגון פרטים אישיים, נסיבות אישיות ומשפחתיות וכן נימוקים רפואיים, סוציאליים, כלכליים ושיקומיים. בכך פועל בית הנשיא שלא כנדרש בתקנות אבטחת מידע ותורת ההגנה בסייבר.

בית הנשיא הודיע כי בעקבות הביקורת הוא פועל ליצירת דרך פעולה אחרת להעברת מידע כאמור.

2. הוראות הדין מחייבות להימנע משמירת "מידע עודף" על אדם - דהיינו פרטי מידע שאינם רלוונטיים ואינם הכרחיים להשגת המטרה שלשמה המידע נאסף מלכתחילה או להשגת מטרות המאגר שבו המידע שמור וכן פרטי מידע שכבר אינם דרושים למטרות אלה[57]. על פי ההוראות, יש לאסוף ולשמור רק את המידע המזערי הנדרש וההכרחי, וזאת מבחינת היקף המידע הנשמר, סוג המידע, משך שמירתו וכדו'. נוסף על כך, על בעל מאגר מידע לבחון אחת לשנה אם המידע הנשמר במאגר חורג מן הנדרש למטרות המאגר. כמו כן מקבל מידע שקיבל נתונים על פי תקנות אבטחת מידע יפריד מיד עם קבלת הנתונים את המידע העודף וימחק אותו לאלתר.

נמצא כי בית הנשיא שומר בקשות חנינה שהועברו למשרד המשפטים ולפרקליטות הצבאית בתיבת דוא"ל של הלשכה המשפטית בבית הנשיא לפרק זמן לא מוגבל. תיבת הדוא"ל אינה מתרוקנת באופן קבוע, ונשמרים בה פרטי בקשות חנינה ישנות, הכוללות מידע בעל רגישות

---

55 כאשר מדובר בבקשה של חייל בשירות חובה וקבע או חייל משוחרר שטרם חלפו שישה חודשים ממועד שחרורו.

56 סעיף 14(ב) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

57 תקנה 2(ג). לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 - הקובעת כי בעל מאגר מידע יבחן אחת לשנה אם המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר ; סעיף 6 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 - "מקבל מידע שקיבל מידע לפי תקנות אלה יפריד מיד עם קבלת הנתונים את המידע העודף וימחק אותו מיד". הוראות הרשות להגנת הפרטיות, **צמצום מידע** (Minimization Data) - מסמך מדיניות (25.3.21).

מיוחדת. לכן גורם הניגש לתיבת הדוא"ל (כגון מנהל מערכת) נחשף לפרטים אישיים של מבקשי חנינות לאורך שנים רבות, בלי שהיה צורך בשמירתם.

על בית הנשיא לפעול על פי תקנות אבטחת מידע: להעביר בקשות חנינה לגורם חיצוני, כגון משרד המשפטים, תוך שימוש בשיטות הצפנה מקובלות; וכן לצמצם את המידע הנשמר בידיו, לרבות בתיבת הדוא"ל, למינימום הנדרש בהתאם לתקנות ולהוראות הרשות להגנת הפרטיות.

בהתייחסות מפברואר 2026 מסר בית הנשיא כי בעקבות הביקורת ניתנה הנחיה לפיה בקשות החנינה יישמרו לתקופה של שנה בלבד וכי שאר החומר הקיים בתיבת הדוא"ל יימחק באופן מיידי.

סיכום

פעילותו התקינה של בית הנשיא מושפעת ותלויה בין השאר ברמת הסודיות, השלמות, הזמינות והשרידות של המידע המצוי ברשותו, ובכלל זה במערכות המחשוב שלו. פגיעה במידע עלולה להוביל לנזקים בהיבטים תפעוליים, טכנולוגיים וכספיים, ואף לפגוע בצנעת הפרט ובשם הטוב ובתדמית של בית הנשיא ושל העומד בראש המדינה.

הביקורת על הניהול וההפעלה של רשת התקשורת המרכזית של בית הנשיא, המשמשת את כלל עובדיו לניהול תחומי העשייה העיקריים של בית הנשיא, העלתה ליקויים בתחומים הבאים:

1. **ה ה י ב ט ה נ י ה ו ל י : עד אמצע שנת 2025 פעל בית הנשיא ללא ועדת היגוי להגנת הסייבר; וללא מדיניות מאושרת ויעדים מדידים בתחום הגנת הסייבר. החסר המהותי בהיבטי ניהול-העל בבית הנשיא ואי-הטלת האחריות לתחומי ליבה על ממלאי תפקידים בבית הנשיא מובילים למסקנה כי תחומי הגנת הסייבר בבית הנשיא נזנחו במידה מסוימת ולא טופלו באופן ההולם את הסיכונים הנשקפים לגוף של המדינה.**

2. **ה ה י ב ט ה א ב ט ח ת י : הועלו ליקויים בעלי משקל בניהול אמצעי ההזדהות והחשבונות של המשתמשים ברשת; בית הנשיא לא הקצה תיבות דוא"ל משרדיות לכל עובדי הארגון העושים שימוש בדוא"ל במסגרת עבודתם השוטפת, ובכך יצר למעשה פתח לשימוש לא תקין בדוא"ל; נמצאו ליקויים המתייחסים לעמידת בית הנשיא בדרישות הנוגעות לניטור מערכות מידע; בבית הנשיא פועלות מערכות שאינן נתמכות עוד בידי היצרן, והוא אינו מקפיד על התקנת כל עדכוני האבטחה הנדרשים במערכותיו, ולכן חלק מהן חשופות לפגיעויות שונות; האופן שבו בנויה רשת בית הנשיא אינו תואם את ההנחיות ויוצר סיכון; בית הנשיא לא התקין חלק ממערכות ההגנה הנדרשות; בית הנשיא לא פעל כנדרש להבטחת שליטה באבטחת תחנות הקצה של הרשת; והוא לא נקט מבעוד מועד את הפעולות הנדרשות להבטחת זמינות פונקציות עסקיות בעת חירום, עקב שיבוש תהליכים עסקיים קריטיים, באופן שהיה מצמצם את הנזק התפקודי והתדמיתי שנגרם לארגון.**

3. **ה י ב ט ה ה ג נ ה ע ל ה פ ר ט י ו ת : בית הנשיא לא קיים חלק מהוראות הדין החלות עליו בכל הנוגע לאבטחת הפרטיות במאגרים שברשותו: לא מונה ממונה אבטחת מידע האמון על אבטחת המידע במאגרים; לא מופו מאגרי המידע, ולא הוכנה רשימת מצאי של מערכות המאגרים; לא גובש נוהל אבטחה, ולא נקבעו הרשאות גישה למאגרים; ואין מנגנון תיעוד אוטומטי של הגישה למערכות המאגר. ממצאים אלה עלו גם בנוגע למאגר החנינות של בית הנשיא, המכיל מידע רגיש על קרוב ל-100,000 מבקשי חנינה, לרבות נתונים רפואיים, סוציאליים וכלכליים. נוסף על כך, בית הנשיא קיבל שירותים מספק חיצוני לצורך הטיפול במאגר זה, אך לא נקט את הפעולות הנדרשות על פי תקנות אבטחת מידע; בית הנשיא מעביר למשרד המשפטים ולפרקליטות הצבאית בקשות חנינה המכילות מידע המוגדר מידע בעל רגישות מיוחדת באמצעות דוא"ל וללא הצפנה, בניגוד לדרישות הדין; בית הנשיא שומר**

בקשות חנינה שהועברו לגופים אלה בתיבת דוא"ל לפרק זמן לא מוגבל, ואינו מצמצם את המידע הנשמר בידיו למינימום הנדרש.

יש לראות בחיוב את פנייתו של בית הנשיא ליה"ב בספטמבר 2024 בבקשה לקבל הנחיה בכל הנוגע להגנת הסייבר ואבטחת המידע הבלתי מסווג, את פעולותיו ליישום ההנחיות, את הקצאת התקציבים להגנת הסייבר וכן את כוונתו להמשיך ליישם את הנחיות יה"ב ולתקן ליקויים שעלו בביקורת.

על בית הנשיא כגוף ציבורי בעל חשיבות לאומית מהמעלה הראשונה, להמשיך לפעול לתיקון הליקויים שעלו בביקורת, במטרה להבטיח את הסודיות, השלמות, הזמינות והשרידות של המידע המצוי ברשותו, למנוע פגיעה בצנעת הפרט של תושבי המדינה ולמנוע פגיעה בשם הטוב ובתדמית של בית הנשיא.