דוח מבקר המדינה

הגנת המידע הממוחשב בבית הנשיא - דוח מיוחד

▪ סיוון התשפ"ו ▪ יוני 2026

הגנת המידע הממוחשב בבית הנשיא - דוח מיוחד

תקציר

רקע

נשיא המדינה הוא ראש מדינה בלתי מפלגתי המייצג את המדינה כלפי פנים וכלפי חוץ. נשיא המדינה 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. נוסף על כך, הנשיא מייצג את מדינת ישראל בפני הקהילה הבין-לאומית ויהדות התפוצות וכן עוסק במיסוד ובהובלה שותפויות מקומיות ובין-לאומיות בנושאים שונים, דוגמת התמודדות עם משבר האקלים. 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.

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 בעל רגישות מיוחדת 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.

נתוני מפתח

כמעט 100,000

מספר מבקשי החנינה שמידע רגיש לגביהם מצוי במאגר מידע של בית הנשיא. מאגר זה נוהל בידי בית הנשיא שלא על פי חלק מהוראות הדין החלות על גופים המחזיקים במאגרי מידע

בחלק

מהחשבונות הקיימים בבית הנשיא, נמצא ליקוי משמעותי מסוים בתחום הזדהות המשתמשים וניהול הרשאות

אין

לבית הנשיא תוכנית להתאוששות מאסון

ניטור

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

חלק

מהמערכות הממוחשבות בבית הנשיא הגיעו לסוף מחזור החיים שלהן

בחלק

מתחנות הקצה בבית הנשיא פעלו גרסאות שפג תוקפן ולכן הן היו חשופות לפגיעויות

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.

תמונת המצב העולה מן הביקורת

עיקרי הליקויים שעלו בביקורת

ניהול העל של הגנת המידע בבית הנשיא

- **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 אימץ בית הנשיא את הנחיות יה"ב[1] בתחום הגנת הסייבר ואבטחת המידע הבלתי מסווג.

- **עד יוני 2025 לא הוקמה בבית הנשיא ועדת היגוי לנושאי הגנת סייבר** - יצוין כי במהלך הביקורת, ביוני 2025, הוקמה לראשונה ועדת היגוי משרדית לנושאי הגנת הסייבר בבית הנשיא בראשות מנכ"ל בית הנשיא, ובתחילת יולי 2025 היא התכנסה לראשונה. נמצא כי משימות מרכזיות לא קודמו בבית הנשיא: הנהלת בית הנשיא לא העריכה נזקים ולא בחנה ואישרה את מפת הסיכונים המשרדית; 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.

- **הנהלת בית הנשיא טרם גיבשה או אישרה מדיניות להגנת הסייבר גם לאחר שאימצה את הנחיות יה"ב המחייבות לעשות כך** - 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.

- **נהלים** - בכל הנוגע לאבטחת המידע 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.

- **הערכה ומיפוי של סיכוני סייבר** - סקר סיכונים הוא מרכיב מרכזי בהגנת המידע והסייבר. 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.

- **ביצוע מבדקי חדירה** - 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.

- **תוכניות עבודה שנתיות** - 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 2025 כללה שתי משימות בלבד הנוגעות להגנת הסייבר. ציון שתי משימות בלבד בתכנית העבודה ל-2025 מעלה חשש כי חסרו בה משימות ליבה חיוניות בתחום הגנת הסייבר. כמו כן גם שתי המשימות שצוינו בתוכנית חסרות ציון של לוחות הזמנים לביצוע וציון הגורם האחראי לכך.

- **תחומי ליבה בתחום טכנולוגיות המידע -** תחומי ליבה של אחריות וסמכות בתחום הגנת הסייבר כפי שהוגדרו בידי נש"ם ויה"ב, 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

[1] יה"ב הוקמה מכוח החלטת ממשלה 2443 מפברואר 2015. 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).

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 והנחיה מקצועית בתחום זה.

- **הזדהות משתמשים וניהול הרשאות** - ממצאי הביקורת העלו ליקויים בעלי משקל בנושא הזדהות משתמשים וניהול הרשאות.

- **שימוש בתיבות דוא"ל אישיות** - בית הנשיא לא הקצה תיבות דוא"ל משרדיות לכל עובדי בית הנשיא העושים שימוש בדואר אלקטרוני 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.

- **ניטור מערכות המידע ברשת בית הנשיא** - נמצאו ליקויים המתייחסים לעמידת בית הנשיא בדרישות הנוגעות לניטור מערכות המידע.

- **עדכניות הגרסאות של מערכות ההפעלה והתוכנה** - 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. כמו כן בית הנשיא אינו מקפיד על התקנת כל עדכוני האבטחה המתפרסמים למוצרים השונים. משמעות הדבר היא שחלק מהמערכות הממוחשבות של בית הנשיא חשופות לפגיעויות שונות.

- **תשתיות רשת בית הנשיא ואבטחתה**

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

  - **מערכת הגנה להגבלת הגישה לרשת** - נמצא כי בית הנשיא לא עומד בהנחיות יה"ב שמטרתן הגבלת הגישה לרשת.

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

- **אבטחת תחנות הקצה** - תחנות הקצה בארגון הן יעד נפוץ לתקיפה באמצעות ניצול חולשות במערכת ההפעלה או ביישומים שונים המותקנים עליה. לפיכך מעקב שוטף אחר תחנות קצה חיוני כדי להבטיח שהן מאובטחות כנדרש וכדי לוודא שתחנות שאינן פעילות מנותקות מהרשת ולא משמשות יעד לתקיפה.

  נמצא כי בחלק מתחנות הקצה פעלו גרסאות של מערכות הפעלה שפג תוקפן והן היו חשופות לפגיעויות. ממצאים אלה משקפים היעדר שליטה של בית הנשיא בכל הנוגע לאבטחת תחנות הקצה.

- **ניהול המשכיות תפקודית בעת חירום** - 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.

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

- **הסדרת הטיפול במאגר החנינות באמצעות ספק** - מאגר החנינות של בית הנשיא מכיל מידע רגיש של קרוב ל-100,000 מבקשי חנינה, לרבות נתונים רפואיים, סוציאליים וכלכליים. משנת 2019 קיבל בית הנשיא שירותים מספק חיצוני לצורך אספקת שירותי אפיון, פיתוח, תמיכה ותחזוקה של מאגר החנינות. בית הנשיא לא פעל כנדרש בתקנות אבטחת מידע בכל הנוגע לקבלת שירותים אלה מהספק: (א) הוא לא ביצע בדיקה מקדימה בנוגע לסיכוני אבטחת המידע הכרוכים בהתקשרות עם הספק החל בשנת 2019; (ב) בהסכם ההתקשרות עם הספק לא עוגנו הוראות בדבר המידע שהספק רשאי לעבד והמטרות שלשמן בלבד הוא רשאי להשתמש במידע שעיבד; (ג) בהסכם לא פורטו המערכות שהספק רשאי לגשת אליהן והפעולות שהוא מורשה לבצע; (ד) לא נקבע מנגנון להשבת המידע לבית הנשיא בסיום תקופת ההתקשרות; (ה) לא הוטלה על הספק החובה לדווח לבית הנשיא על עמידתו בהוראות תקנות אבטחת מידע, ואף לא על אירוע אבטחת מידע במאגר, אם התרחש; (ו) 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.

- **העברת מידע ממאגר החנינות לגופים ממשלתיים** - 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. כמו כן 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 מיוחדת. לכן גורם הניגש לתיבת הדוא"ל (כגון מנהל מערכת) נחשף לפרטים אישיים של מבקשי חנינות לאורך שנים רבות, בלי שהיה צורך בשמירתם.

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.

יש לראות בחיוב את פעולות בית הנשיא לביצוע חלקים ראשונים בסקר סיכונים ובמבדק חדירה תשתיתי.

תקציב בית הנשיא להגנת הסייבר - בית הנשיא הקצה לתחום הגנת הסייבר כ-15% מתקציב תחום טכנולוגיית המידע הכולל שלו בשנת 2023; כ-5.8% בשנת 2024; ובשנת 2025 כ-11%. יש לראות בחיוב את הקצאת התקציב להגנת הסייבר בידי בית הנשיא בשנים 2023 ו-2025. עם זאת, בית הנשיא לא ניהל רישום נפרד של התקציבים המופנים באופן ייעודי לתחום הגנת הסייבר, כדי שניתן יהיה לבחון אם הוא עומד בהנחיית יה"ב.

עיקרי המלצות הביקורת

- על בית הנשיא לפעול על פי הנחיות יה"ב בתחום הגנת הסייבר ואבטחת המידע הבלתי מסווג.
- 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. על ועדת ההיגוי של בית הנשיא לקבוע מדיניות להגנת הסייבר, בהתאם לנדרש בהנחיות יה"ב, ולתקפה בתדירות הנדרשת.
- על בית הנשיא להשלים את סקר הסיכונים ואת הטיפול בממצאיו, להשלים את סקרי הסיכונים במערכות המידע ולטפל בממצאיהם ולבצע סקרי סיכונים בתדירות הנדרשת על פי הנחיות יה"ב. כמו כן על בית הנשיא להשלים את מבדק החדירה התשתיתי, לבצע מבדקי חדירה יישומיים ולבצע מבדקי חדירה למערכות על בסיס תקופתי, כנדרש בהנחיות יה"ב.
- 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. כמו כן על בית הנשיא להשלים את החסר בנהלים מרכזיים ולגבש נהלים נוספים בתחום הגנת הסייבר, כנדרש.
- כדי להבטיח שבית הנשיא מקצה די משאבים להגנת הסייבר, עליו לנהל רישום נפרד של התקציבים המופנים לתחום זה. כמו כן, מומלץ לבית הנשיא להשלים הטלת תחומי האחריות והסמכות על בעלי תפקידים מתאימים בתחום הגנת הסייבר.
- על בית הנשיא לתקן את הליקויים ולעמוד במלוא הנחיות שנקבעו בעניין הזדהות משתמשים וניהול הרשאות.
- 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.
- על בית הנשיא לפעול לשיפור מערך הניטור על מערכות המידע שלו.
- 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.
- על בית הנשיא להתאים את מבנה הרשת לנדרש על פי הנחיות יה"ב ובקרות תורת ההגנה בסייבר ולהתקין את מלוא מערכות ההגנה הנדרשות.
- על בית הנשיא לוודא כי הוא מנהל את כל תחנות הקצה בארגון, כנדרש בהנחיות יה"ב.
- 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 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 לבחינת מערך השיקום וההתאוששות שלו בתדירות הנדרשת בהנחיית יה"ב. כן מומלץ כי הנהלת בית הנשיא תשתתף בניסויים אלו.

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 בבית הנשיא למאגרי המידע ולמערכותיהם, כמו כן, עליו לערוך ביקורת על עמידה בהוראות תקנות אבטחת מידע על ידי גורם שאינו ממונה על אבטחת המידע בבית הנשיא, זאת לכל הפחות אחת ל-24 חודשים.

על בית הנשיא להיערך לביצוע הפעולות הנדרשות מגוף המחזיק במאגר מידע הטעון רמת אבטחה גבוהה בכל הנוגע למאגר החנינות; מאגר זה צפוי להכיל מידע על 100,000 אנשים ומעלה בתוך זמן קצר. כמו כן 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.

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.

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 לשם ניהול תחומי העשייה העיקריים של בית הנשיא, העלתה הליקויים בתחומים האלה:

1. **ההיבט הניהולי:** 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. **ההיבט האבטחתי:** 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. **היבט ההגנה על הפרטיות:** 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.