דוח מבקר המדינה

סייבר ומערכות מידע

דוח מבקר המדינה

סייבר ומערכות מידע

ירושלים | אייר התשפ"ג | מאי 2023

מס' קטלוגי - 2023-S-003

ISSN 0793-1948

דוח זה מובא גם באתר המרשתת של
משרד מבקר המדינה
www.mevaker.gov.il

עיצוב גרפי: צוות אי.אר דיזיין

תוכן העניינים

פתח דבר 7

المقدمة 13

Foreword 446

ביקורות מערכתיות

התקשרויות בפטור ממכרז בתחום התקשוב 17

הנגשת שירותי ממשל בעידן הדיגיטלי לאנשים עם מוגבלות ולציבור שאינו משתמש במדיה הדיגיטלית 89

משרד הפנים

שימוש במסמכי זיהוי ביומטריים - תעודות זהות ודרכונים 191

המשרד לביטחון לאומי - שירות בתי הסוהר

טכנולוגיות דיגיטליות ואבטחת המידע והסייבר בשירות בתי הסוהר 299

משרד המשפטים - רשות האכיפה והגבייה

הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה 375

המוסד לביטוח לאומי

אסדרת הגנת הסייבר במוסד לביטוח לאומי 405

משרד הבריאות

ביקורת סייבר במרכז הרפואי א' - מבדק חדירה לתשתית ולרשת התקשורת 427

פתח דבר

הדוח המונח על שולחן הכנסת מציג את תוצאות הביקורת בתחומי הגנת הסייבר, טכנולוגיות המידע והגנת הפרטיות.

הקדמה הטכנולוגית הביאה לכך שתחומים רבים יותר ויותר בחיינו מתבססים על מערכות מידע מרכזיות, ובהתאם לכך צפויה עלייה ניכרת בשכיחותם של איומי סייבר ובמידת חומרתם. לצד היתרונות של המרחב המקוון לכלכלה ולחברה, חלה עלייה בהיקף מתקפות הסייבר הדורשת חיזוק של רמת ההגנה והיערכות להתמודדות מיטבית עם תקיפות סייבר.

בעשור האחרון גברו תקיפות הסייבר על ארגונים ועל אנשים פרטיים ברחבי העולם. בשנת 2020 זוהו ברחבי העולם כ-9.5 מיליון ניסיונות למתקפות סייבר שמטרתן הייתה להשבית מערכות מחשוב ולמנוע את היכולת להשתמש בהן - בשנה זו זוהו 18 ניסיונות למתקפה בדקה בממוצע; במחצית הראשונה של שנת 2020 נגנבו או זלגו למרשתת (אינטרנט) לפחות 36 מיליארד נתונים אישיים בעקבות מתקפות סייבר.

עם תחילת כהונתי כמבקר המדינה ונציב תלונות הציבור הגדרתי את תחום הסייבר כאחד מנושאי הליבה שבהם תעסוק ביקורת המדינה. זאת במטרה לבחון את היערכותם ומוכנותם של הגופים המבוקרים להתמודדות עם הסיכונים המשמעותיים במרחב הקיברנטי, עם האיומים האסטרטגיים ועם אתגרי הסייבר העתידיים המונחים לפתחם. דוח זה עוסק כולו בתוצאות ביקורת המדינה בתחום הגנת הסייבר ומערכות המידע. ואלה פרקי הדוח:

א. שימוש במסמכי זיהוי ביומטריים - תעודות זהות ודרכונים

ב. טכנולוגיות דיגיטליות ואבטחת המידע והסייבר בשירות בתי הסוהר

ג. הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה

ד. ביקורת סייבר במרכז הרפואי א' - מבדק חדירה לתשתית ולרשת התקשורת

ה. אסדרת הגנת הסייבר במוסד לביטוח לאומי

ו. הנגשת שירותי ממשל בעידן הדיגיטלי לאנשים עם מוגבלות ולציבור שאינו משתמש במדיה הדיגיטלית

ז. התקשרויות בפטור ממכרז בתחום התקשוב

יובהר כי חמשת הפרקים הראשונים עברו תהליך חיסיון, וועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניחם במלואם על שולחן הכנסת אלא לפרסם רק חלקים מהם, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]. להלן סקירה של חלק מפרקי הדוח:

מסמכי זיהוי אמינים משמשים מפתח למגוון רחב של פעולות במגזר הממשלתי והעסקי. כעשור לפני מועד סיום הביקורת, בשנת 2013, החל בישראל מעבר למסמכי זיהוי ביומטריים - תעודות

זהות חכמות ודרכונים ביומטריים - שצפויים להחליף את מסמכי הזיהוי מהסוג הישן, אשר נחשבים קלים לזיוף, ועלולים לשמש גורמי טרור או פשיעה ואף לשמש לצורכי הגירה בלתי חוקית. בפרק בנושא **שימוש במסמכי זיהוי ביומטריים - תעודות זהות ודרכונים** נמצא כי אף שהמעבר לתעודות זהות חכמות החל כבר לפני עשור בקרב תושבים שהביעו רצון בכך, ובאופן מחייב לכלל התושבים ביולי 2017, והושקעו עד כה 430 מיליון ש"ח בהנפקתן, נכון ליולי 2022, מיליוני תושבים מחזיקים בתעודה מהסוג הישן, הקלה לזיוף. עוד העלתה הביקורת ליקויים מהותיים בכמה תחומים עיקריים: עיכוב משמעותי במעבר לתיעוד לאומי ביומטרי והיעדר שימוש בו; ליקויים בשמירה על נתונים ביומטריים במערכות הממוחשבות של רשות האוכלוסין וההגירה; וקושי בהתמודדות עם הגידול בביקוש להנפקת מסמכי זיהוי ביומטריים. נוכח חומרת ממצאי הביקורת, מומלץ כי רשות האוכלוסין וההגירה תפעל לתיקון הליקויים, וכי שר הפנים יוודא שנעשות פעולות לתיקון הליקויים בתחומים האמורים, ובכלל זאת יוודא כי ליקויים בתחום הביטחון וההגנה על המידע יתוקנו בתיאום עם הגורמים המקצועיים האמונים על כך: השב"כ, המשטרה ומערך הסייבר הלאומי. בשנים האחרונות חלו שינויים מרחיקי לכת בהיבטים הנוגעים לפרויקט הלאומי הביומטרי, בכלל זה חל שיפור ניכר ביכולות הטכנולוגיות בתחום הביומטרייה, וגדל במידה רבה היקף השימוש בשירותים מקוונים הדורשים הזדהות בטוחה. השלמת המעבר לתיעוד לאומי ביומטרי, תוך הסרת החסמים המשפטיים והטכנולוגיים המקשים את השימוש בו והתאמת הפרויקט לשינויים שחלו בשנים האחרונות, עשויה למנף את השימוש במסמכי הזיהוי הביומטריים וצפויה להביא לתועלות ניכרות בהיבטי הביטחון, הכלכלה והשירות לציבור.

שירות בתי הסוהר (השב"ס) הוא ארגון הכליאה הלאומי, גוף ביטחוני הנכלל במערכת אכיפת החוק ואמון על החזקת אסירים פליליים וביטחוניים במשמורת במטרה להגן על שלום הציבור וביטחונו. היקף האחריות של השב"ס לאלפי אסירים וכן ניהול פריסה רחבה של מתקני כליאה בכל רחבי הארץ מציבים את השב"ס כארגון גדול ומורכב המצריך משאבי אבטחה, ניהול ושליטה טכנולוגיים יעילים. הדבר מקבל משנה תוקף עקב אופיו ורגישותו הביטחונית של הארגון והסיכונים הביטחוניים והפליליים התלויים בתפקודו התקין. משנת 2021 השקיע השב"ס בקידום תוכנית "קברניט" להתאמת הטכנולוגיה בארגון לאתגריו המבצעיים והניהוליים. הפרק בנושא **טכנולוגיות דיגיטליות ואבטחת המידע והסייבר בשירות בתי הסוהר** חושף פערים עמוקים וליקויים משמעותיים של מערך ביטחוני רגיש, היוצרים סיכון של ממש. נמצא פער יסודי בין מהותו של הארגון, אופיו, המידע המוחזק בו והסיכונים הנוגעים לפעילותו לבין התרבות התפקודית הרווחת בו בכל הנוגע לאבטחת מידע וניהול המידע המסווג. הפרק חושף מציאות רבת שנים שלפיה תחומי האחריות והסמכות של השב"ס ושל המאסדרים בתחום אבטחת המידע המסווג והסייבר ובתחום הטכנולוגיות הדיגיטליות ומערכות המידע אינם מיושמים, הלכה למעשה, באופן תקין וכנדרש. נמצאו פערים יסודיים בתוכנית התאוששות מאסון של המערכות הטכנולוגיות בשב"ס. תמונת המצב העולה מפרק זה היא תוצאה של הזנחה רבת שנים, שבמהלכן לא הייתה משילות טכנולוגית שהניחה יעדים, קבעה תהליכים, הקצתה משאבים, וניהלה כראוי את הסיכונים והמתודולוגיות הארגוניות בתחום הטכנולוגי. קיימת אי-ודאות תקציבית מהותית בנוגע למימוש המענה המתוכנן בתוכנית "קברניט" למכלול הפערים הטכנולוגיים והאבטחתיים. מומלץ כי ראש הממשלה, בהתייעצות עם השר לביטחון לאומי, יבחן את סוגיית אבטחת המידע והסייבר בשב"ס בכללותה ובפרט את סוגיית אבטחת המידע המסווג. על השב"ס והמשרד לביטחון לאומי לוודא שהרציפות התפקודית לא תיפגע בקרות אירועי אסון העלולים לסכן את יציבותו ותפקודו של מערך הכליאה הלאומי. המשרד לביטחון לאומי והשר העומד בראשו נושאים באחריות לתפקוד מערך הכליאה בישראל, ובמסגרת זו עליהם להבטיח

כי השב"ס ממלא את תפקידו באמצעות תשתית טכנולוגית מתאימה, וכי בניין הכוח בתחום זה מנוהל בראייה ארוכת טווח ובמתווה תקציבי המבטיח את מימושו.

נכון לנובמבר 2022, במוסד לביטוח לאומי מתבצעות בכל יום כ-2.9 מיליון תקיפות סייבר בממוצע, ומהן כ-66,000 תקיפות שיש בהן פוטנציאל לנזק. בדומה למדינות אחרות, ישראל חשופה לתקיפות סייבר לצורכי כופר וגניבת מידע. מלבד זאת, נוכח האקלים הגיאו-פוליטי המורכב ביטחונית, ישראל משמשת כר מטרות נרחב לתוקף הקיברנטי הפוטנציאלי, המעוניין לפגוע בחוסנה ובביטחון הלאומי שלה. הדוח כולל פרק בנושא **אסדרת הגנת הסייבר במוסד לביטוח לאומי**. גוף כדוגמת בט"ל, מחייב שיגובש עבורו מענה אסדרתי מספק הכולל הנחיה של מערך הסייבר הלאומי, הנחיה של הרשות להגנת הפרטיות ותיאום בין שניהם כדי להבטיח את ההגנה המיטבית. נוכח היקפי המידע השמורים בבט"ל והסיכונים לדליפתו מומלץ כי ועדת ההיגוי העליונה, שתפקידה לבחון אילו גופים מוגדרים חיוניים ולכן זקוקים להגנה קיברנטית, תקדם את הבחינה של בט"ל כגוף תמ"ק (תשתיות מחשוב קריטיות). מומלץ כי עד סיום הבחינה יוסדר ממשק מקצועי בין מערך הסייבר הלאומי לבט"ל לצורך מתן מענה ישיר, העברת דיווחים, בקרה על תיקון הליקויים וכיו"ב. כמו כן מומלץ כי ועדת ההיגוי תבחן אם יש עוד גופים בעלי מאגרי מידע בהיקפים הדומים לבט"ל שיש לבחון את הגדרתם כגופי תמ"ק, ובכך לשפר את ההגנה על התשתיות החיוניות של מדינת ישראל.

הפרק בנושא **הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה** מעלה ליקויים בתחום הגנת הפרטיות ואבטחת המידע במערכות המידע במרכז לגביית קנסות (המג"ק) שברשות האכיפה והגבייה, אף שהמערכת התפעולית של המג"ק מוגדרת כמאגר שמחייב רמת אבטחה גבוהה. בין הליקויים שעלו: היעדר תיעוד של הגישה של משתמשי המערכת התפעולית של המג"ק למידע המצוי במערכת וכפועל יוצא מכך היעדר בקרה על אותה גישה; אי-ביצוע מעקב הולם אחר אירועים חריגים המתרחשים במערכת; ניהול לקוי של תהליך מתן ההרשאות למערכת התפעולית של המג"ק ושל הפיקוח והבקרה עליהן; היקף גישה בלתי מוגבל של משתמשי המערכת למידע המצוי בה; ניהול לקוי של הרשאות עובדי מוקד המידע הטלפוני למערכת; וכן סיכון לחדירת תוקפים חיצוניים למערכות המג"ק. על רשות האכיפה והגבייה והמג"ק לפעול בהקדם על פי הנחיות הגופים הרלוונטיים למניעת דליפת מידע מהארגון ולשמירה על שלמותו. מאגר המידע של המג"ק הוא רחב היקף וכולל מידע רגיש בנוגע לכ-3 מיליון חייבים. סכומי החוב שבטיפול המג"ק מסתכמים נכון למועד הביקורת בכ-6.8 מיליארד ש"ח. מכאן נובע הצורך בשמירה על מערכות המידע, שנועדה למנוע פגיעה בשלמות המידע וברציפות התפקודית של המג"ק במתן שירותים, למנוע דליפה של נתונים ומידע ממאגר המידע ולמנוע את חשיפתם לגורמים שאינם מורשים לכך.

בשנים האחרונות גברו גם איומי הסייבר על מערכת הבריאות, ובכלל זה על מרכזים רפואיים. כן דווח כי מגזר הבריאות היה אחד מעשרת המגזרים המותקפים ביותר בישראל בשנת 2021. אחת הדרכים להיערכות לאיומי סייבר היא לבצע מבדקי חדירה לארגון, כדי לזהות חולשות במעטפת ההגנה שלו ולפעול למזער אותן, ובמקרים שבהם לא ניתן לטפל בחולשות שעלו - להביא לידיעת הנהלת הארגון את הסיכונים האפשריים ולנהל אותם באופן שוטף. דוח זה כולל פרק בנושא **ביקורת סייבר במרכז הרפואי א' - מבדק חדירה לתשתית ולרשת התקשורת.** במבדק החדירה זוהו 13 ממצאים משמעותיים בחמישה תחומים: סגמנטציה ובקרת זרימה; בקרת גישה לרשת; הגנת עמדות ושרתים; תוכנה לא עדכנית; וגישה לא מאובטחת. עשרה מהממצאים היו בדרגת חומרה גבוהה ושלושה בדרגת חומרה בינונית. בעקבות מבדק החדירה תיקנה הנהלת המרכז הרפואי א' כמה ליקויים, ובפרט עדכנה את רמת האבטחה של מערכות מסוימות.

להערכת הנהלת המרכז הרפואי, העלות הכוללת לתיקון הליקויים יכולה להסתכם ביותר מ-10 מיליון ש"ח לשנה באופן שוטף. מומלץ כי ההנהלה תגבש תוכנית עבודה רוחבית למיגור הסיכונים או למזעורם במקרים שבהם לא ניתן לתקן את הליקויים שעלו. כמו כן מומלץ לבצע מבדקי חדירה בהתאם לתוכנית סדורה. משרד הבריאות פועל כמאסדר של המוסדות הרפואיים, ובכלל זה בתחום אבטחת המידע. מומלץ כי משרד הבריאות, כמאסדר בתחום הבריאות, ישלים את ביצוע מבדקי החדירה שהחל לבצע בכלל המוסדות הרפואיים בארץ ויקבע מתכונת עיתית להמשך ביצוע מבדקי חדירה במוסדות. עוד מומלץ כי משרד הבריאות יבחן את ממצאי מבדק החדירה שבוצע במרכז הרפואי א' ויפעל להטמיע בכלל המוסדות הרפואיים את ההמלצות המתבססות על ממצאי המבדק. כמו כן מומלץ שמשרד הבריאות יוודא כי כלל המוסדות הרפואיים מבצעים בעצמם מבדקי חדירה תקופתיים, יבחן את ממצאי המבדקים האלה, יעקוב אחר תיקון הליקויים שיעלו בהם ובהתאם לכך יפרסם המלצות לכלל המוסדות הרפואיים. נוסף על כך מומלץ שמשרד הבריאות ימשיך לפעול כדי לסייע במישור הלאומי לכל המוסדות הרפואיים להתמודד עם אתגרי אבטחת המידע הנוגעים למכשור הרפואי.

הרכש הממשלתי הוא נדבך מרכזי בפעילותם של הגופים הממשלתיים, שכן מרבית הפעילות הממשלתית תלויה ברכש של טובין או של שירותים. בפרק בנושא **התקשרויות בפטור ממכרז בתחום התקשוב** עלה כי היקף הרכש התקשובי בשנים 2019 - 2021 היה כ-14.4 מיליארד ש"ח, והוא היה כ-15.6% מסך הרכש הממשלתי בשנים אלו. היקף הרכש התקשובי שבוצע בפטור ממכרז בשנים 2019 - 2021 היה כ-1.79 מיליארד ש"ח, והוא היה כ-14.2% מסך הרכש התקשובי באותן שנים. ממצאי דוח זה מצביעים על שורה של ליקויים בתחום הרכש, בדגש על התקשרויות בפטור ממכרז בתחום התקשוב. להלן הליקויים העיקריים: המידע שמפרסמים לציבור מינהל הרכש ומערך הדיגיטל בתחום הרכש אינו תואם את המידע במערכת מרכב"ה, ובכך נפגעת השקיפות לציבור ויכולות הבקרה על פעילות הרכש הממשלתי; השימוש שעושים הגופים הממשלתיים בפטור ממכרז בעילת ספק יחיד ובעילת התקשרות של עד 50,000 ש"ח ברכש התקשובי גדול במאות אחוזים מהשימוש בהם ברכש הכללי; ואי-עמידה בהוראות הדין הנוגעות לפרסום התקשרויות. ההתפתחות המהירה של תחום התקשוב גורמת לכך שגופים ממשלתיים נדרשים ליישם חדשנות בתחום זה במהירות וביעילות, כדי למנוע את התיישנות הטכנולוגיה הרלוונטית עד להשלמת הליך הרכש. לצד זאת, יש לנהל את הליכי הרכש באופן הוגן, שוויוני ושקוף ובאופן העולה בקנה אחד עם הוראות הדין כדי להביא לתוצאות עסקיות וליעילות כלכלית. על הגופים הממשלתיים להקפיד על הוראות הדין והוראות התכ"ם הנוגעות לרכש הממשלתי. מומלץ כי מינהל הרכש יפעל לשיפור תהליך הרכש במערכת מרכב"ה, לרבות יישום בקרות ממוחשבות ובקרות מפצות, כדי לוודא את השלֵמות והמהימנות של המידע ולשפר את הפיקוח והבקרה השוטפים ואת תהליכי קבלת ההחלטות. על החשכ"ל והיחידה לחופש המידע לפעול לאכיפת פרסום ההתקשרויות של כלל הגופים בהתאם להוראות הדין ותוך הקפדה על מהימנות המידע המתפרסם לציבור.

על הגופים המבוקרים מוטלת החובה לפעול בדרך מהירה ויעילה לתיקון הליקויים שהועלו בדוח זה, כדי להעלות את רמת ההגנה של הארגון ולהיערך להתמודדות מיטבית עם תקיפות סייבר. על הגופים להתאים את פעילותם לעולם רווי טכנולוגיות מתקדמות ולאתגרים שבפניהם הם יעמדו בשנים הקרובות. מתקפות הסייבר שאירעו לאחרונה מחדדות את הצורך בכך.

לסיום, חובה נעימה היא לי להודות לעובדי משרד מבקר המדינה, הפועלים במסירות לביצוע ביקורת באופן מקצועי, מעמיק, יסודי והוגן ולפרסום דוחות ביקורת אובייקטיביים, אפקטיביים ורלוונטיים.

משרד מבקר המדינה מתחייב להמשיך ולבקר את עמידת הגופים המבוקרים בפני סיכונים עכשוויים ועתידיים ולעסוק בתחומי הגנת הסייבר, טכנולוגיות המידע והגנת הפרטיות, לטובת אזרחי ישראל.

מתניהו אנגלמן

מבקר המדינה
ונציב תלונות הציבור

ירושלים, אייר התשפ"ג, מאי 2023

المقدمة

يعرض التقرير الموضوع على طاولة الكنيست نتائج الرقابة في مجالات حماية السايبر، وتكنولوجيا المعلومات وحماية الخصوصية.

أدى التقدم التكنولوجي الى أن المزيد والمزيد من المجالات في حياتنا تعتمد على أنظمة معلومات مركزية، وبموجب هذا من المتوقع أن تكون زيادة كبيرة في تواتر التهديدات السيبرانية ودرجة خطورتها. الى جانب الكثير من الإيجابيات التي يعود بها الفضاء المحوسب على الاقتصاد والمجتمع، هناك ازدياد في نطاق الهجمات السيبرانية التي تتطلب تعزيز مستوى الحماية والاستعداد للتعامل الأمثل مع الهجمات السيبرانية.

في العقد الماضي ازدادت الهجمات السيبرانية على المنظمات وعلى الأفراد في جميع أنحاء العالم. في سنة 2020 تم اكتشاف ما يزيد عن 9.5 مليون محاولة لهجمات سيبرانية تهدف الى تعطيل أنظمة الحوسبة ومنع القدرة على استخدامها- في هذه السنة تم الكشف عن 18 محاولة للهجوم في الدقيقة بالمتوسط; في النصف الأول من سنة 2020 تمت سرقة أو تسريب ما لا يقل عن 36 مليار من البيانات الشخصية الى الشبكة في أعقاب الهجمات السيبرانية.

مع بداية عملي كمراقب الدولة ومفوض شكاوى الجمهور، قمت بتعريف المجال السيبراني على أنه أحد المواضيع الأساسية التي سيتعامل معها مراقب الدولة. هذا بهدف فحص مدى استعداد وجهوزية الجهات التي تتم الرقابة عليها للتعامل مع المخاطر المهمة في الفضاء السيبراني، مع التهديدات الاستراتيجية ومع التحديات السيبرانية المستقبلية التي تواجهها. يتناول هذا التقرير بأكمله نتائج رقابة الدولة في مجال الحماية السيبرانية وأنظمة المعلومات. وهذه فصول التقرير:

أ. استخدام مستندات الهوية البيومترية- بطاقات الهوية وجوازات السفر.

ب. تكنولوجيا رقمية وأمن المعلومات والسيبرانية في خدمة السجون.

ج. حماية الخصوصية وأمن المعلومات في أنظمة مركز جباية الغرامات، الرسوم والتكاليف في سلطة التنفيذ والجباية.

د. جعل الخدمات الحكوميّة متاحة في العصر الرَقمي للأشخاص ذوي الإعاقة وللأشخاص اللذين لا يستخدمون الوسائل الرَقميَة.

ه. نظام الحماية السيبرانية في مؤسسة التأمين الوطني.

و. إتاحة الخدمات الحكومية في العصر الرقمي.

ز. التعاقدات بإعفاء من إجراء مناقصات في مجال تكنولوجيا المعلومات والاتصال.

موضح بهذا، أن أول خمسة فصول مرت بعملية سرية، وقررت اللجنة الفرعية لشؤون رقابة الدولة في الكنيست عدم وضعها جميعها على طاولة الكنيست انما نشر قسم منها فقط، بموجب البند 17 لقانون مراقب الدولة، لعام 1958 [صيغة مدمجة]. فيما يلي مسح لجزء من فصول التقرير:

تعد مستندات التعريف الموثوقة مفتاح للعديد من العمليات في القطاع الحكومي وقطاع الأعمال. قبل حوالي عقد من موعد نهاية الرقابة، في سنة 2013، بدأ في اسرائيل الانتقال الى مستندات التعريف

البيومترية- بطاقات هوية ذكية وجوازات سفر بيومترية- التي من المفترض أن تستبدل مستندات التعريف من النوع القديم، التي تعتبر سهلة التزييف، ومن الممكن أن تستخدم من قبل جهات إرهابية أو إجرامية وحتى تستخدم للهجرة غير القانونية. في الفصل بموضوع **استخدام مستندات التعريف البيومترية- بطاقات الهوية وجوازات السفر** وجد أنه على الرغم من أن الانتقال الى بطاقات الهوية الذكية بدأ قبل حوالي عقد للمواطنين الذين أبدوا رغبتهم لذلك، وبشكل ملزم لجميع المواطنين في شهر تموز 2017 وتم استثمار 430 مليون شيكل جديد حتى الآن في إصدارها، حتى تموز 2022، يملك الملايين من المواطنين بطاقات من النوع القديم، سهل التزييف. كشفت الرقابة أيضا عن أوجه قصور جوهرية في عدة مجالات أساسية: تأخير كبير في الانتقال الى التوثيق الوطني البيومتري وعدم استخدامه؛ أوجه قصور في الحفاظ على المعطيات البيومترية في الأنظمة المحوسبة لسلطة السكان والهجرة؛ وصعوبة في التعامل مع ازدياد الطلب على إصدار مستندات تعريف بيومترية. نظرا لخطورة الرقابة، يوصى بأن تعمل سلطة السكان والهجرة على إصلاح أوجه القصور، وأن يتحقق وزير الداخلية من اتخاذ الإجراءات لإصلاح أوجه القصور في المجالات المذكورة، بما في ذلك التحقق من إصلاح أوجه القصور في مجال الأمن وحماية المعلومات بالتنسيق مع الجهات المهنية المؤتمنة على ذلك: الشاباك، الشرطة والنظام السيبراني الوطني. في السنوات الأخيرة حصلت تغييرات كبيرة في الجوانب المتعلقة بالمشروع الوطني البيومتري، بما في ذلك طرأ تحسن كبير في القدرات التكنولوجية في المجال البيومتري وزاد بشكل كبير نطاق استخدام الخدمات المحوسبة التي تتطلب التعريف الآمن. إتمام الإنتقال الى التوثيق الوطني البيومتري، من خلال إزالة العوائق القانونية والتكنولوجية التي تصعب استخدامه وملائمة المشروع للتغييرات التي حصلت في السنوات الأخيرة، من الممكن أن يزيد من استخدام مستندات التعريف البيومترية ومن المتوقع أن يعود ذلك بفوائد كبيرة للجوانب الأمنية، الاقتصادية والخدمة للجمهور.

صحيح لتشرين الثاني 2022، يتم تنفيذ حوالي 2.9 مليون هجمة سيبرانية بالمتوسط في مؤسسة التأمين الوطني، ومنها حوالي- 66,000 هجمة قد تسبب ضرر. مثل الدول الأخرى، فان اسرائيل معرضة لهجومات سيبرانية لأغراض الفدية وسرقة المعلومات. عدا عن هذا، نظرا للإقليم الجيو- سياسي المعقد أمنيا، تعد اسرائيل هدفا واسع النطاق للمهاجم السيبراني المحتمل، الذي يرغب في إلحاق الضرر في المرونة والأمن الوطني لاسرائيل. يشمل التقرير فصل بموضوع **تنظيم الحماية السيبرانية في مؤسسة التأمين الوطني**. تتطلب جهة كمؤسسة التأمين الوطني صياغة استجابة تنظيمية كافية تشمل توجيه من قبل نظام السايبر الوطني، توجيه من قبل سلطة حماية الخصوصية والتنسيق بينهم لتأمين الحماية الأمثل. في ضوء كميات المعلومات المحفوظة في مؤسسة التأمين الوطني ومخاطر تسريبها يوصى بأن تقوم لجنة التوجيه العليا، التي تتمثل مهمتها بفحص أي من الجهات تعتبر حيوية ولهذا تحتاج الى حماية الكترونية، بتعزيز فحص مؤسسة التأمين الوطني كجهة بنية تحتية حاسوبية حرجة. يوصى أيضا، أنه حتى انتهاء الفحص أن يتم ترتيب واجهة مهنية بين نظام السايبر الوطني لمؤسسة التأمين الوطني بهدف منح الرد المباشر، نقل التقارير، التحكم بإصلاح العيوب وما الى ذلك. بالإضافة يوصى أن تقوم لجنة التوجيه بفحص ما اذا كانت هناك جهات أخرى تملك قواعد بيانات ذات نطاق مشابه لمؤسسة التأمين الوطني وتعريفها على أنها جهة بنية تحتية حاسوبية حرجة، وبهذا تحسين حماية البنى التحتية الحيوية في دولة اسرائيل.

يشير الفصل بموضوع **حماية الخصوصية وأمن المعلومات في أنظمة مركز جباية الغرامات، الرسوم والتكاليف في سلطة التنفيذ والجباية** الى أوجه قصور في مجال حماية الخصوصية وأمن المعلومات في أنظمة المعلومات في مركز جباية الغرامات الموجودة في سلطة التنفيذ والجباية، على الرغم من أن نظام التشغيل في مركز جباية الغرامات معرف على أنه قاعدة بيانات تلزم مستوى حماية عالية.

من بين أوجه القصور التي وجدت: عدم وجود توثيق وصول مستخدمي نظام التشغيل التابع لمركز جباية الغرامات الموجودة في النظام ونتيجة ذلك عدم وجود تحكم بهذا الوصول; عدم إجراء تعقب مناسب للأحداث الشاذة التي تحصل في النظام; عدم كفاية إدارة عملية منح الأذونات للنظام التشغيلي لمركز جباية الغرامات ومراقبتها والتحكم بها; نطاق وصول غير محدود للمعلومات الموجودة به لمستخدمي النظام; إدارة غير سليمة لأذونات ممنوحة لموظفي مركز المعلومات الهاتفي للنظام; بالإضافة الى خطر اختراق مهاجمين خارجيين لأنظمة مركز جباية الغرامات. يجب على سلطة التنفيذ والجباية ومركز جباية الغرامات العمل بأقرب فرصة بموجب تعليمات الجهات ذات العلاقة لمنع تسرب معلومات من المنظمة والحفاظ على سلامتها. قاعدة بيانات المعلومات الموجودة في مركز جباية الغرامات واسعة النطاق وتشمل معلومات حساسة بخصوص حوالي 3 مليون مدين. مبالغ الدين الموجودة بمعالجة مركز جباية الغرامات وصلت حتى موعد الرقابة لحوالي 6.8 مليارد شيكل جديد. من هنا تنبع الحاجة الى الحفاظ على أنظمة المعلومات، التي خصصت لمنع الإضرار بسلامة المعلومات والاستمرارية الوظيفية لمركز جباية الغرامات بتقديم الخدمة، منع تسرب معطيات ومعلومات من قاعدة بيانات المعلومات ومنع كشفها لجهات غير مخولة لهذا.

ازدادت خلال السنوات الأخيرة التهديدات السيبرانية على نظام الصحة، بما في ذلك المراكز الطبية. بالإضافة تم الإبلاغ على أن قطاع الصحة كان أحد القطاعات العشرة الأكثر تعرضا للهجوم في اسرائيل خلال سنة 2021. ان احدى الطرق للاستعداد للتهديدات السيبرانية هي إجراء اختبارات اختراق للمنظمة، للكشف عن نقاط الضعف في غلاف الحماية والعمل على تقليلها، وفي حالات عدم القدرة على معالجة نقاط الضعف هذه- إبلاغ إدارة المنظمة حول المخاطر المحتملة وإدارتها بشكل مستمر. يشمل هذا التقرير فصلا بموضوع **الرقابة السيبرانية في المركز الطبي أ' – اختبار اختراق البنى التحتية وشبكة الاتصال**. تم الكشف في اختبار الاختراق هذا عن 13 نتيجة مهمة في خمسة مجالات: التجزئة والتحكم في التدفق; التحكم في الوصول الى الشبكة; حماية المحطات والخوادم; برمجية غير محدثة، ووصول غير محمي. كانت عشرة من النتائج بدرجة خطورة عالية وثلاثة بدرجة خطورة متوسطة. في أعقاب اختبار الاختراق قامت إدارة المركز الطبي أ' بإصلاح بضعة أوجه قصور، وخاصة قامت بإجراء تحديث حول مستوى آمان أنظمة معينة. وفق تقييم إدارة المركز الطبي، فان التكلفة الإجمالية لإصلاح العيوب من الممكن أن تصل الى أكثر من – 10 مليون شيكل جديد في السنة بشكل مستمر. يوصى بأن تقوم الإدارة بصياغة خطة عمل أفقية للقضاء على المخاطر أو تقليلها في حالات لا يمكن بها إصلاح العيوب التي ظهرت. بالإضافة الى ذلك، يوصى بإجراء اختبارات اختراق وفقا لخطة منتظمة. تعمل وزارة الصحة كمنظم للمؤسسات الطبية، بما في ذلك بمجال أمن المعلومات. يوصى بأن تقوم وزارة الصحة، كمنظم في مجال الصحة، بإتمام إجراء اختبارات الاختراق التي بدأت بالقيام بها في جميع المؤسسات الطبية في البلاد ووضع خطة دورية للاستمرار بإجراء اختبارات الاختراق في المؤسسات. يوصى أيضا أن تفحص وزارة الصحة نتائج اختبار الاختراق الذي أجري في المركز الطبي أ' وتعمل على تنفيذ التوصيات التي تستند على نتائج الاختبار في جميع المؤسسات الطبية. أضف الى ذلك يوصى بأن تقوم وزارة الصحة بالتحقق بأن جميع المؤسسات الطبية تقوم بإجراء اختبارات اختراق دورية بنفسها، فحص نتائج هذه الاختبارات، ومتابعة إصلاح أوجه القصور التي ظهرت ووفق ذلك نشر توصيات لجميع المؤسسات الطبية. يوصى بالإضافة الى ذلك، أن تقوم وزارة الصحة بالاستمرار بالعمل لمساعدة جميع المؤسسات الطبية على المستوى الوطني بالتعامل مع تحديات أمن المعلومات التي تتعلق في الأجهزة الطبية.

تعتبر الممتلكات الحكومية ركيزة أساسية في عمل الجهات الحكومية، حيث أن معظم النشاط الحكومي يتعلق بشراء السلع أو الخدمات. في فصل موضوع **التعاقدات المعفاة من المناقصات في مجال تكنولوجيا المعلومات والاتصال**، تم الكشف عن أن نطاق مشتريات الاتصالات في السنوات 2019 - 2021 كان حوالي 14.4 مليارد شيكل جديد، الذي اعتبر حوالي 15.6% من إجمالي الممتلكات

الحكومية في هذه السنوات. تشير نتائج هذا التقرير الى سلسلة من أوجه القصور في مجال الممتلكات، على وجه الخصوص التعاقدات ذات الإعفاء من المناقصات في مجال تكنولوجيا المعلومات والاتصال. فيما يلي أهم أوجه القصور: المعلومات التي يتم نشرها للجمهور من قبل إدارة الممتلكات والنظام الرقمي في مجال الشراء لا تلائم المعلومات الموجودة في نظام إجمالي الحوسبة الرقمية في المكاتب الحكومية، وهذا يضر الشفافية للجمهور وقدرة التحكم بنشاط الشراء الحكومي; استخدام الهيئات الحكومية للإعفاء من المناقصات بحجة مزود واحد وبحجة التعاقد حتى 50,000 شيكل جديد في مشتريات الاتصال يزيد بمئات بالمئة من استخدامها في الشراء العام; وعدم استيفاء تعليمات القانون التي تتعلق بنشر التعاقدات. التطور السريع في مجال الاتصال يعني أن الجهات الحكومية مطالبة بتطبيق الحداثة في هذا المجال بسرعة ونجاعة، لمنع تقادم التكنولوجيا ذات العلاقة حتى إتمام عملية الشراء. الى جانب ذلك، يجب إجراء عمليات الشراء بشكل عادل، منصف وشفاف بشكل يتفق مع أحكام القانون للحصول على نتائج عملية ونجاعة اقتصادية. يجب على الجهات الحكومية الحرص على تعليمات القانون وأنظمة الأموال والقطاع التي تتعلق بالشراء الحكومي. يوصى بأن تقوم الإدارة بالعمل على تحسين عملية الشراء في نظام إجمالي الحوسبة المقطعية في المكاتب الحكومية، بما في ذلك تطبيق التحكم المحوسب والضوابط التعويضية، للتحقق من اكتمال وموثوقية المعلومات وتحسين الإشراف والرقابة المستمرة وعمليات اتخاذ القرارات. يجب على إدارة المحاسب العام والوحدة لحرية المعلومات العمل على إنفاذ نشر تعاقدات جميع الجهات وفقا لتعليمات القانون والحرص على مصداقية المعلومات التي يتم نشرها للجمهور.

يجب على الجهات التي تتم الرقابة عليها العمل بصورة سريعة وناجعة لإصلاح العيوب التي ظهرت في هذا التقرير، لزيادة مستوى حماية المنظمة والاستعداد للتعامل الأمثل مع الهجمات السيبرانية. يجب على الجهات تكييف نشاطها لعالم مشبع بالتقنيات المتقدمة والتحديات التي ستواجهها في السنوات القريبة. الهجومات السيبرانية التي حدثت في الآونة الأخيرة تشدد على الحاجة الى ذلك.

أخيرا، يجب علي أن أشكر موظفي مكتب مراقب الدولة، الذين يعملون بتفان للقيام بالرقابة بشكل مهني، متعمق وشامل وعادل ونشر تقارير رقابة موضوعية وناجعة وذات صلة.

يتعهد مكتب مراقب الدولة بمواصلة الرقابة على عمل الجهات التي تتم الرقابة عليها في ظل المخاطر الحالية والمستقبلية والعمل في مجالات الحماية السيبرانية، تكنولوجيا المعلومات وحماية الخصوصية، لصالح مواطني اسرائيل.

متنياهو انجلمن

مراقب الدولة
ومفوض شكاوى الجمهور

القدس، آيار- مايو 2023