דוח מבקר המדינה

סייבר ומערכות מידע

דוח מבקר המדינה

סייבר ומערכות מידע

ירושלים | כסלו התשפ"ג | דצמבר 2022

מס' קטלוגי 2022-S-003

ISSN 1948-0793

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

עיצוב גרפי: צוות אי.אר דיזיין בע"מ

תוכן העניינים

פתח דבר 7

المقدمة 9

Foreword 324

הגנת הסייבר והמשכיות עסקית ביחידת שירות עיבודים ממוכנים ברשות המיסים 13

הגנת הסייבר במגזר התחבורה 37

ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו 113

הקמת מערכת סחר חוץ חדשה ברשות המיסים - פרויקט "שער עולמי" 181

היבטים באסדרה ובפיקוח בנוגע לספקי המים המקומיים בתחום הגנת הסייבר 241

דוח ביקורת מיוחד

הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות 257

פתח דבר

הדוח המונח היום על שולחן הכנסת הוא ראשון מסוגו, והוא מציג את תוצאות הביקורת בתחום הגנת הסייבר, טכנולוגיות המידע והגנת הפרטיות.

מרחב הסייבר כולל מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן דיגיטלי, נתוני תעבורה ובקרה. המרחב מאופיין בהתפתחות טכנולוגית מהירה, החודרת לכל תחומי החיים ומעצבת את הפעילות החברתית, הכלכלית והמדינתית של האנושות. למרחב הסייבר ולקדמה הטכנולוגית יתרונות רבים לכלכלה ולחברה, אך גלומים בהם איומים שעלולים להשפיע על הרציפות התפקודית של הארגון, על שלמות תהליכים ועל סודיות המידע הארגוני.

נוכח איומי הסייבר ההולכים וגוברים שעימם מתמודדת מדינת ישראל בשנים האחרונות, הגדרתי, עם תחילת כהונתי כמבקר המדינה ונציב תלונות הציבור, 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 העתידים המונחים לפתחם.

כדי לפתח ולחזק את יכולותיו המקצועיות של משרד מבקר המדינה בתחום הסייבר ומערכות המידע, ננקטו כמה פעולות עיקריות ובכללן הקמת אגף ביקורת סייבר, שייעודו ביצוע ביקורת בתחום זה, נוסף על האגף הייעודי לביקורת בתחום מערכות מידע וטכנולוגיות מידע; גיוס עובדים בעלי רקע מקצועי ייחודי בתחום הסייבר; קידום תהליך הסמכה בין-לאומית של עובדי המשרד כמבקרי מערכות מידע (CISA); התקשרות עם יועצים חיצוניים בתחום הגנת המידע והסייבר המלווים את צוותי הביקורת בתחומים אלו.

נוסף על כך, במסגרת ביקורת הגנת הסייבר ביצע משרד מבקר המדינה צעד תקדימי בארץ ובקרב מוסדות ביקורת מדינה בעולם - מבדקי חדירה למערכות הממוחשבות של כמה גופים מבוקרים המדמים תקיפת סייבר. מבדק החדירה נעשה לצורך איתור פגיעויות במערכת הממוחשבת העלולות לסכן את איתנותה בעת ניסיון תקיפה, וכפועל יוצא מכך לשבש את תפקודו השוטף של המערך שנבדק. הבדיקות נעשו בתיאום עם הגוף המבוקר, והגופים המבוקרים תיקנו כבר במהלך הביקורת חלק מהליקויים שעלו בה.

בשנים 2021 - 2022 ביצע משרד מבקר המדינה ביקורות ייעודיות בנושא הסייבר ואבטחת המידע בתחומי התשתית, החינוך, התחבורה, הבריאות, הכספים והרשויות המקומיות. נבדקו, בין היתר, מערכות המידע והגנת הסייבר במסגרת תהליכי הבחירות לכנסת ה-21, ה-22 וה-23; מאגרים ביומטריים; הגנת הסייבר על מכשירים רפואיים; ניהול מערכות מידע ברשויות המקומיות. במסגרת הביקורות נבחנו הנושאים האלה: שלמותן ואיתנותן של מערכות המידע בגופים המבוקרים; יעילות ההגנות והבקרות הממוחשבות המוטמעות בהן; הגנה על מידע אישי ופרטי במערכות הממשלתיות; השקעה ב-IT; היערכות מוקדמת לאירועי סייבר והתאוששות מאסון; היערכות להתקפות סייבר ופגיעה בתשתיות מדינה קריטיות ועוד. הפרקים בנושאים הללו פורסמו לציבור בדוחות השנתיים של משרדנו.

דוח זה מיוחד בכך שהוא עוסק כולו בתוצאות ביקורת המדינה בתחום הגנת הסייבר ומערכות המידע. ואלה פרקי הדוח:

א. הגנת הסייבר והמשכיות עסקית ביחידת שירות עיבודים ממוכנים ברשות המיסים

ב. הגנת הסייבר במגזר התחבורה

ג. ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו

ד. הקמת מערכת סחר חוץ חדשה ברשות המיסים - פרויקט "שער עולמי"

ה. היבטים באסדרה ובפיקוח בנוגע לספקי המים המקומיים בתחום הגנת הסייבר

ו. הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות

הביקורת בנושאים האמורים העלתה ליקויים בתחומים אלה: ניהול משתמשים והרשאות; תיעוד וניטור של הגישה לרשת ובקרה עליה; הגנת עמדות ושרתים; סגמנטציה ובקרת זרימה; עדכניות התוכנות; ההקפדה על גישה מאובטחת למערכות, הגנה על מידע אישי של מיליוני אזרחים ועוד.

בשנים האחרונות אנו עדים להתקפות סייבר מסוגים שונים, אירועי כופרה ונוזקה, הונאות, מעילות וגניבת מידע עסקי. זירת הסייבר אף הפכה לזירת לוחמה בין ארגוני טרור ופשיעה למדינות ואף בין מדינות. בשנים הבאות צפוי גידול ניכר בחדירת מרחב הסייבר לשגרת היום-יום, לנוכח התפתחותם של מוצרי Internet of Things) IOT), מכוניות אוטונומיות ועוד, ובהתאם צפויה עלייה ניכרת בשכיחותם של איומי סייבר ובמידת חומרתם.

על הגופים המבוקרים מוטלת החובה לפעול בדרך מהירה ויעילה לתיקון הליקויים שהועלו בדוח זה, כדי להעלות את רמת ההגנה של הארגון ולהיערך לטיפול מיטבי לתקיפות סייבר; להתאים את פעילותם לעולם רווי טכנולוגיות מתקדמות ולאתגרים שבפניהם 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.

אנו במשרד מבקר המדינה מתחייבים להמשיך ולבקר את עמידת הגופים המבוקרים בפני סיכונים עכשוויים ועתידיים ולעסוק בתחומי הגנת הסייבר, טכנולוגיות מידע והגנת הפרטיות, לטובת אזרחי ישראל והעולם כולו.

מתניהו אנגלמן
מבקר המדינה
ונציב תלונות הציבור

ירושלים, כסלו התשפ"ג, דצמבר 2022

المقدمة

ان التقرير المطروح على طاولة الكنيست يعتبر الأول من نوعه، ويعرض نتائج الرقابة في مجال الحماية السيبرانية وتكنولوجيا المعلومات وحماية الخصوصية.

يشمل حيز السايبر الحواسيب والأنظمة الميكانيكية والشبكات والبرامج والمعلومات المحوسبة، المحتوى الرقمي ومعطيات المرور والتحكم. يتميز هذا الحيز بالتطور التكنولوجي السريع الذي يخترق جميع مجالات الحياة ويشكل النشاط الإجتماعي والاقتصادي والسياسية البشرية. يتمتع الحيز السيبراني والتطور التكنولوجي بالكثير من المزايا للاقتصاد والمجتمع، لكن تتأصل به تهديدات التي من الممكن أن تؤثر على الاستمرارية الوظيفية للمنظمة وعلى سلامة العمليات وسرية المعلومات التنظيمية.

في ضوء التهديدات السيبرانية المتزايدة التي تتعامل معها دولة اسرائيل في السنوات الأخيرة، عندما توليت منصب مراقب الدولة ومفوض شكاوى الجمهور، حددت، المجال السيبراني كواحد من مواضيع الأساس التي ستتناولها رقابة الدولة. بهدف فحص مدى استعداد وجهوزية الجهات الخاضعة للرقابة على التعامل مع المخاطر الكبيرة في المجال السيبراني ومع التهديدات الاستراتيجية وتحديات السايبر المستقبلية التي تواجهها.

من أجل تطوير وتعزيز القدرات المهنية لمكتب مراقب الدولة في مجال السايبر وأنظمة المعلومات، تم اتخاذ عدة خطوات أساسية من ضمنها إنشاء قسم رقابة سيبرانية المخصص لتنفيذ الرقابة في هذا المجال، بالإضافة الى القسم المخصص للرقابة في مجال أنظمة المعلومات وتكنولوجيا المعلومات ; تجنيد موظفين ذوي خلفية مهنية فريدة في مجال السايبر ; تعزيز عملية الحصول على تأهيل دولي لموظفي المكتب كمراقبي أنظمة المعلومات (CISA) ; التعاقد مع مستشارين خارجيين في مجال أمن المعلومات والسايبر التي ترافق طواقم الرقابة في هذه المجالات.

بالإضافة الى ذلك، في إطار رقابة الحماية السيبرانية قام مكتب مراقب الدولة بخطوة سباقة في الدولة وفي مؤسسات رقابة الدولة في العالم- باختبارات اختراق للأنظمة المحوسبة للعديد من الهيئات الخاضعة للرقابة التي تحاكي هجوما سيبرانيا. أجري اختبار الاختراق بهدف كشف نقاط ضعف في النظام المحوسب الذي من شأنه أن يشكل خطرا على قوته في أي محاولة هجومية، ونتيجة ذلك تشويش العمل المنتظم للنظام الذي تم اختباره. تم إجراء الاختبارات بالتنسيق مع الجهة الخاضعة للرقابة، وقامت الجهات الخاضعة للرقابة بإصلاح قسم من العيوب التي ظهرت خلال الرقابة.

خلال السنوات 2021 - 2022 قام مكتب مراقب الدولة بعمليات رقابة خاصّة بموضوع السايبر وأمن المعلومات في مجالات البنى التحتية والتربية والمواصلات والصحة والأموال والسلطات المحلية. من بين الكثير من الأمور، تم فحص أنظمة المعلومات والحماية السيبرانية في إطار إجراءات الانتخابات للكنيست ال-21, ال-22 وال-23; قواعد البيانات البيومترية; الحماية السيبرانية على الأجهزة الطبية; إدارة نظم المعلومات في السلطات المحلية. في إطار الرقابة تم اختبار المواضيع التالية: سلامة وقوّة نظم المعلومات في الهيئات الخاضعة للرقابة; نجاعة الحمايات والضوابط المحوسبة التي تحتويها; حماية المعلومات الخاصة والشخصية في النظم الحكومية; استثمار في- IT; الاستعداد المسبق لأحداث سيبرانية والتعافي من الكوارث; الاستعداد لهجومات سيبرانية وإصابة البنى التحتية الحيوية في الدولة والمزيد. تم نشر هذه الفصول الخاصة بهذه المواضيع للجمهور في إطار التقارير السنوية لمكتبنا.

هذا التقرير خاص حيث أنه يتناول بشكل كامل، نتائج رقابة الدولة في مجال الحماية السيبرانية وأنظمة المعلومات. وهذه فصول التقرير:

أ. الحماية السيبرانية وتواصل العمل في وحدات خدمة المعالجة المحوسبة في سلطة الضرائب

ب. حماية سيبرانية في قطاع المواصلات

ج. إدارة معلومات بيومترية في جيش الدفاع الاسرائيلي وحمايته السيبرانية

د. إنشاء نظام تجارة خارجية جديد في سلطة الضرائب- مشروع "بوابة عالمية"

ه. جوانب التنظيم والرقابة فيما يتعلق بموردي المياه المحليين في مجال الحماية السيبرانية

و. الحماية السيبرانية لنظم المعلومات في وزارة التربية والتعليم, أمن المعلومات في امتحانات البجروت وفي علامات امتحانات البجروت

كشف التحقيق في المواضيع المذكورة عن عيوب في هذه المجالات: إدارة المستخدمين والتصاريح; توثيق ومراقبة الوصول الى الشبكة والتحكم بها; حماية المحطات والخوادم; التجزئة والتحكم في التدفق; تحديثات البرامج; الحرص على الوصول الآمن للأنظمة، حماية معلومات تخص ملايين المواطنين والمزيد.

شهدنا في السنوات الأخيرة هجومات الكترونية من أنواع مختلفة، حوادث فدية وأضرار، احتيال، اختلاس وسرقة معلومات تجارية. حتى أن الساحة السيبرانية أصبحت ساحة حرب بين منظمات الإرهابية والإجرامية والدول وحتى بين الدول. في السنوات القادمة، من المتوقع ازدياد اختراق الحيز السيبراني في الروتين اليومي، على ضوء تطور منتجات IOT (Internet of Things)، سيارات ذاتية القيادة والمزيد، ووفق ذلك من المتوقع زيادة كبيرة في وتيرة التهديدات السيبرانية ودرجة خطورتها.

يجب على الجهات الخاضعة للرقابة العمل بصورة سريعة وناجعة لإصلاح أوجه القصور التي طرحت في هذا التقرير، من أجل زيادة مستوى حماية المنظمة والإستعداد لمعالجة أمثل للهجمات السيبرانية; وملائمة نشاطهم لعالم مشبع تكنولوجيا متطورة والتحديات التي سيواجهونها في السنوات القادمة. ان الهجومات السيبرانية التي حدثت مؤخرا تشدد على الحاجة لذلك.

أخيرا، يسعدني أن أشكر موظفي مكتب مراقب الدولة، الذين يعملون بتفان لإجراء عمليات الرقابة بشكل مهني، عميق، أساسي وعادل ونشر تقارير رقابة موضوعية وناجعة وذات صلة.

نتعهد، نحن في مكتب مراقب الدولة بالاستمرار في فحص تعامل الهيئات الخاضعة للرقابة مع المخاطر الحالية والمستقبلية والعمل في مجالات حماية السايبر، تكنولوجيا المعلومات وحماية الخصوصية، من أجل مصلحة مواطني اسرائيل والعالم أجمع.

متنياهو أنجلمان

مراقِب الدولة
ومفوَّض شكاوى الجمهور

القدس، كانون الأول (ديسمبر) 2022