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 الحكوميَة 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