JASPSS
مجلة المجتمع العربي لنشر الدراسات العلمية
ISSN: 2958-6798
الإصدار رقم (4)
16–كانون الثاني–2023
https://jaspss.com

بحث بعنوان

واقع الأمن الإلكتروني والسيبراني في المملكة الأردنية الهاشمية

هيام خلف فهد الجريبيع

مبرمج

بلدية لواء الموقر

الملخص

يتحدث الباحث عن واقع الأمن الإلكتروني والسيبراني في المملكة الأردنية الهاشمية، اذ أن قضية امن وحماية المعلومات تعتبر من اهم قضايا العصر الصناعية الرابعة كيف أصبح نجاح اي مؤسسه يعتمد بشكل كبير على ما تملكه من معلومات لكن العديد من المعلومات والأنظمة والبنية التحتية المتصلة في الشبكات عرض الحين والاخر حيث تواجه انواع شتى من الخروقات للمعلومات، كما تتعرض لي انشطه اجراميه تعطل خدمتها وتدمر ممتلكاتها، وتختلف هجمات إلهك من جهة لأخرى ومن مكان لأخر ومن زمان الى اخر مستخدمه ادوات واليات اختراق متجدده ومتطورة طوال الوقت.

ISSN: 2958-6798
الإصدار رقم (4)
16–كانون الثاني–2023
https://jaspss.com

Abstract

The researcher talks about the reality of electronic and cyber security in the Hashemite Kingdom of Jordan, as the issue of information security and protection is considered one of the most important issues of the Fourth Industrial Era. How has the success of any institution depended largely on the information it possesses, but many information, systems and infrastructure related to networks are presented now. In addition, the other, where you face various types of breaches of information, as you are exposed to criminal activities that disrupt its service and destroy its property, and your god's attacks differ from one side to another and from one place to another and from time to another using renewable and sophisticated penetration tools and mechanisms all the time.

المقدمة

يعد الأمن السيبراني في الوقت الحالي أهم عناصر الأمن في الدول المتحضرة وخاصةً مع التحول الكامل نحو السيبرانية في كافة جوانب الحياة. وتقوم فكرة الأمن السيبراني على تأمين البنية التحتية المعلوماتية للدول والتي تتمثل في المنشآت الهامة ونظم المعلومات الهامة ومنها نظم إدارة الحكومات الإلكترونية والتي تُدار بها مؤسسات الدول الحيوية، وكذلك النظم العسكرية والشرطية والقضائية والإقتصادية والصناعية والتجارية وغيرها. ويُعد ما يهددها هو تهديد للأمن القومي للدول. لذا قامت العديد من الدول بإعداد الهيئات التي تختص بحماية الأمن السيبراني، وأصبح هذا المفهوم هو جُلّ إهتمام حكومتنا الرشيدة . فقد سخرت له كافة الإمكانيات وأصبح من معايير قياس تحضّر ومدى إمكانيات الدول فيما يتعلق بالجاهزية السيبرانية لمواجهة التهديدات، والذي يقدم الإتحاد الدولي للإتصالات سنوياً مؤشراً يتم فيه ترتيب الدول بحسب الجاهزية.

أصبحت شبكه المعلومات الإلكترونية جزء لا يتجزأ من حياتنا اليومية اليوم جميع المؤسسات الحكومية والأهلية وحتى الاستخدامات الشخصية تستخدم المعلومات الرقمية وتقوم بمعالجتها وتخزينها ومشاركتها، ومع زيادة هذه المعلومات وانتشارها، اصبحت حماية هذه معلومات أكثر حيوية ولها تأثير فعال للأمن القومي واستقرارنا الاقتصادي.

إذا انه يعد الجهد المستمر في حماية شبكات وبيانات المؤسسات والافراد من الاستخدام الغير مصرح به او اي اذى او اختراق يلحق بالشبكة.

ان قضية امن وحماية المعلومات تعتبر من اهم قضايا العصر الصناعية الرابعة كيف أصبح نجاح اي مؤسسه يعتمد بشكل كبير على ما تملكه من معلومات لكن العديد من المعلومات والأنظمة والبنية التحتية

المتصلة في الشبكات عرض الحين والاخر حيث تواجه انواع شتى من الخروقات للمعلومات، كما تتعرض لي انشطه اجراميه تعطل خدمتها وتدمر ممتلكاتها، وتختلف هجمات إلهك من جهة لأخرى ومن مكان لأخر ومن زمان الى اخر مستخدمه ادوات واليات اختراق متجدده ومتطورة طوال الوقت.

التهديدات الإلكترونية والسيبرانية

يُمكن تصنيف التهديدات الإلكترونية والسيبرانية إلى نوعين. الجرائم الإلكترونية ضد الأفراد والشركات، وما إلى ذلك، والحرب السيبرانية ضد الدولة. لذلك، يستلزم الأمن السيبراني حماية البرامج والشبكات والمعلومات والبيانات الأخرى من الوصول غير المصرح به أو التغيير. وهو يستلزم جميع الأنشطة والعمليات الضرورية المتخذة لتقليل نقاط الضعف والتهديدات من أي نوع وإنفاذ السياسات اللازمة للاسترداد وضمان البيانات والوقاية والعمليات الأخرى المتصلة. وهي تشمل جميع العمليات والآليات التي تحمي المعدات الرقمية والسجلات والبيانات من الوصول غير المقصود وغير القانوني أو التدمير أو التلاعب.

في العالم المعاصر، برز الأمن السيبراني كجانب حاسم للعائلات والأفراد، وكذلك الشركات (مثل المؤسسات المالية والتعليمية وبيوت الأعمال والحكومة) التي تخزن وتجمع مجموعة واسعة من المعلومات السرية حول أجهزة الكمبيوتر ونقلها إلى الأجهزة الأخرى والشبكات المختلفة. بالنسبة للعائلات، تعتبر حماية البيانات التي يمكن أن تؤثر على الحياة الاجتماعية وكذلك التمويل الخاص أمرًا بالغ الأهمية.

قدم الإنترنت مجموعة واسعة من فرص التعلم ولكنه تسبب في العديد من المخاطر أيضًا. قد يستخدم المتسللون بنوايا خبيثة المعلومات الشخصية ومقاطع الفيديو وصور مستخدمي الإنترنت بشكل غير لائق على وسائل التواصل الاجتماعي مثل Twitter و Facebook و Instagram قد يتسببون في حوادث تهدد

الحياة. ظهرت منصات وسائل التواصل الاجتماعي كوسيلة شائعة للاتصال وتبادل البيانات مع الأفراد الآخرين. المكتسبة، أنشأت المنصات عددًا لا يحصى من الفرص للجرائم الإلكترونية، التي تنطوي على تسرب المعلومات والهويات الشخصية. لهذا السبب، من الضروري أن يفهم الناس كيفية الحماية من التهديدات السيبرانية، ويجب أن يفهموا التباينات بين العالمين الحقيقي والافتراضي. يجب أن يتعلم الفرد كيفية حماية المعلومات الشخصية وأجهزة الكمبيوتر من المتسللين ويجب أن يشارك في السلوك المناسب عبر الإنترنت للقضاء على التهديدات السيبرانية وإنشاء بيئة إلكترونية أكثر أمانًا.

أهمية الأمن السيبراني والإلكتروني

في سياق الحوسبة، يمر الأمن السيبراني بتحولات هائلة في التكنولوجيا وعملياتها في الأيام الأخيرة، وعلم البيانات يقود التغيير. استخراج الأمن أنماط الحوادث أو الرؤى من بيانات الأمن السيبراني والمباني المقابلة.

النموذج القائم على البيانات، هو المفتاح لجعل نظام الأمان آليًا وذكيًا. إلى فهم وتحليل الظواهر الفعلية بالبيانات والأساليب العلمية المختلفة، يتم استخدام تقنيات وعمليات وأنظمة التعلم الآلي، وهو أمر شائع ومعروف باسم علم البيانات.

ومن الضروري مناقشة الأمن السيبراني وأهميته والتركيز على بيانات الأمن السيبراني في العلوم، حيث يتم جمع البيانات من مصادر الأمن السيبراني ذات الصلة، وتُكمل التحليلات أحدث الأنماط المستندة إلى البيانات لتوفير حلول أمان أكثر فعالية.

يسمح مفهوم علم بيانات الأمن السيبراني بجعل عملية الحوسبة أكثر قابلية للتنفيذ وذكية مقارنة بالعمليات التقليدية في مجال الأمن السيبراني. في هذا البحث سوف نناقش ونلخص عددًا من العناصر المرتبطة بقضايا البحث والتوجهات المستقبلية. بالإضافة إلى كيفية التعلم الآلي القائم على إطار متعدد الطبقات لغرض نمذجة الأمن السيبراني، ومناقشة علم بيانات الأمن السيبراني والأساليب ذات الصلة ولكن أيضًا للتركيز على قابلية التطبيق نحو اتخاذ القرار الذكي المستند إلى البيانات لحماية.

في عصر الإنترنت المفتوح على مصراعيه، أصبح من المهم أكثر من أي وقت سبق تأمين البيانات والمعلومات والاتصالات الإلكترونية بشكل عام. مع كل عملية بحث عن الامن السيبراني تظهر أهمية الأمن السيبراني في عصر الإنترنت. تُعزى الحاجة إلى الأمن السيبراني إلى زيادة الاعتماد على التكنولوجيا، والاختراقات والقرصنة للشركات المختلفة، والتغيرات السريعة في التكنولوجيا التي سهلت الهجمات الإلكترونية الآلية. لا تزال الجرائم الإلكترونية تمثل تحديًا كبيرًا في القطاع التكنولوجي، وهذا يعني الحاجة إلى وجود أنظمة أمان إلكتروني أفضل لحماية المستخدمين من الهجمات الضارة. يجب توعية الناس بشأن الجرائم الإلكترونية لأن هذه هي الخطوة الأولى لوقف الجرائم الإلكترونية. يجب أن يتعاون الخبراء والشركات والهيئات الحكومية في تطوير الأنظمة التي تحمي مستخدمي الإنترنت حيث سيستمر عدد مستخدمي الإنترنت في الازدياد.

التجربة الأردنية الحديثة في الأمن السيبراني

يواجه الأردن أبعادًا جديدة تمامًا للأمن السيبراني، حيث أصبحت الحروب الإلكترونية والهجمات السيبرانية مدمرة بقدر دمار الحروب التقليدية أو الأهلية من النواحي المادية والمعنوية وقد تصل إلى الأضرار الجسدية والأرواح إن طالت الخوادم والحواسيب في منشآت صحية أو صناعية أو حربية.

منذ بداية التحول الرقمي على المستوى العالمي الذي يشمل كل القطاعات ونواحي الحياة التي تلامس جميع شرائح المجتمع، تم تطوير العمل بشتى أماكنه وتطبيقاته وتطورت المنتجات الجديدة بسرعة مع تغيير أساليب الإدارة سواء العامة (لمؤسسات الدول) والخاصة (لمؤسسات القطاع المدني التجاري) معتمدة التحول الرقمي على كل الأصعدة وذلك لتأمن أكبر قدر ممكن من المرونة لتحسين السرعة في وصول الخدمات والمنتجات للأسواق المحلية والعالمية، لا سيما خلال وبعد جائحة كورونا، وذلك لمليء الفجوة الحاصلة لبيئات العمل التي تم إدخالها حديثًا وبقوة نتيجة ظروف خاصة فرضتها الأحداث – مثل العمل من المنزل.

وكالعادة بعدما أصبحت المعلوماتية والملفات الرقمية التي باتت مخزنا لكل المنتوج البشري الحافظ للقيمة سواء على مستوى التوثيق أو الحفظ. فعلى سبيل المثال أصبحت التعاملات المالية والحوالات والمحافظ المالية والحسابات كلها أرقام مخزنة على أقراص الحواسيب، لا، وباتت تعتمد الحوسبة السحابية التي هي بحد ذاتها تتيح لتلك المعلومات أن تتواجد في فضاء رقمي غير محصور في مكان فيزيائي معين أو ثابت رغم وجود المراكز المعلوماتية المنتشرة والمحددة المكان لمالكيها، والذين هم غالبا شركات ربحية من القطاع الخاص والعالمي أيضا.

إطلاق العوالم والأكوان الافتراضية التي وبشكل سريع باتت مكانا تجاريا تباع فيه الأصول الرقمية المشفرة (كالأراضي والعقارات والمنتجات الفنية والسلع الافتراضية) ويتعامل فيها المشتركون (ومنهم حكومات دول، وعربية أيضا) بحركات مالية ضخمة باستخدام العملات الرقمية المشفرة.

كل ذلك أصبح شيقا، لكن الأكثر تشوقا وحماسا هم المجرمون والمحتالون الرقميون الذين تواجدوا من بدء انتشار الرقمنة والإنترنت وانتشار الحواسيب، لكن الآن هم أكثر ذكاء ودهاء وحرفة وجاهزية؛ لأن العائد من الأعمال الإجرامية والسرقات الرقمية بات كبيرا وكبيرا جدا أكبر مما اعتاد عليه البشر من قبل.

ذلك الأمن كما اصطلح عليه «الأمن السيبراني». الأمن السيبراني هو العمل الأمني الذي يهدف لحماية أجهزة الحاسوب وأنظمتها والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة ومن سرقة أو تلف برامجها أو بيانتها الإلكترونية. وذلك التعريف يشمل العمل الأمني السيبراني بدءا من الحوكمة والقوانين والتشريعات والمواصفات والمقاييس والإجراءات الاحترازية والحلول الوقائية وانتهاء بالتحري والبحث والتحليل التقني وتتبع الأدلة والتوثيق والتطبيق الجزائي والملاحقة القانونية بكل ما تحويه من إجراءات وأدوات واختصاصات وما تحتاجه من موارد بشرية وتقنية وعينية.

الجريمة الإلكترونية في الأردن

هي كل جريمة نصت عليها القوانين الأردنية وتم ارتكابها عن طريق الشبكة العنكبوتية (الإنترنت) سواءً تمثلت بفعل أو الامتناع عن فعل جرمه القانون، ومنها جرائم مواقع التواصل الاجتماعي، لذلك تم تشريع قانون الجرائم الإلكترونية، وقد تضمن عدة مواد، تضمنت التعريف بأهم المصطلحات الإلكترونية، والعقوبات وهي عقوبة الدخول للشبكة المعلوماتية، وعقوبة إدخال أو نشر برنامج الغاء أو حذف، عقوبة

التقاط أو باعتراض أو بالتنصت أو أعاق أو حور أو شطب، بطاقات الائتمان أو بيانات المعلومات المالية والمصرفية، تحويل الأموال من نظام معلومات أو موقع الكتروني، تضاعف العقوبة بحق كل من قام بسبب تأدية وظيفته، الأعمال الإباحية والاستغلال الجنسي، تسهيل وترويج الدعارة، الذم والقدح والتحقير عن طريق الشبكة المعلوماتية، التهديد الإلكتروني، الدخول على البيانات غير المتاحة للجمهور، دخول الضابطة العدلية الأماكن للتفتيش، عقوبة الاشتراك والتدخل والتحريض، ارتكاب أي جريمة معاقب عليها بموجب أي تشريع، مضاعفة عقوبة التكرار، إقامة الدعوى أمام المحاكم الأردنية.

تحديات الأمن السيبراني في الأردن

وسط إقبال وتوسع كبيرين في استخدام وسائل التقنية والانترنت في المملكة، يتزايد خطر وتهديدات الأمن السيبراني التي تتطور يوما بعد يوم مع التطور التقني المتسارع، ما يستدعي الاحتياط والتجهز لمواجهة مثل هذه التهديدات التي قد تحدث آثارا كارثية على الاقتصاد والامن والمجتمع حال حصولها، وهو ما تدركه الحكومة تماما مؤكدة اول من امس انها تعمل اليوم على قدم وساق وخصوصا مع وجود المركز الوطني للامن السيبراني الذي وثق العام الماضي حوالي 900 حالة لهجمات سيبرانية.

إن حرب المعلومات هي سمة هذا العصر، في ضوء تطوّر تقنيَّات الاتّصال وأدوات التوَّاصل الرَّقمي، وكلَّما تطوَّرت أنظمة المعلومات حول العالم، نشطت دول ومنظَّمات ومؤسَّسات وأشخاص لاختراق تلك الأنظمة، لافتا الى ان دول العالم ومنها الأردن تتعرض إلى هجمات سيبرانيّة متزايدة، تتفاوت في أعدادها وأهدافها، وهذه الهجمات تركّز على المؤسسات السِّياديَّة، وعلى أهداف ماليَّة واقتصاديَّة، وعلى الأفراد أيضاً.

وفي سبيل مواجهة الهجمات السيبرانية، يجب على أي شخص أو مؤسَّسة للتَّواصل مع المركز الوطني للأمن السيبراني للإبلاغ عن تعرُّضه لأيِّ اختراق، باتالي سيقوم المركز ضمن اختصاصه بتتبع مصدر الاختراق في حال وقوعه.

إن المركز الذي تأسس في الأردن يهدف الى بناء منظومة فعالة للأمن السيبراني على مستوى الوطن وتطويرها وتنظيمها بهدف حماية المملكة من تهديدات أي هجوم سيبراني، مشيرا الى ان 4 بالمائة من الهجمات الالكترونية على الأردن العام الماضي كانت لأهداف تجسس وأخرى سياسية واقتصادية.

معظم الهجمات السيبرانية على الأردن العام الماضي جاءت من 40 دولة حول العالم، مؤكدا صعوبة تحديد الدولة التي صدر منها الهجوم حيث قد يستخدم المهاجم بنية تحتية في أي دولة كانت، وإن الهجمات استهدفت الشبكة الداخلية وأنظمة التشغيل لعدد من المؤسسات الرسمية والأفراد.

تطوير استراتيجية الأمن السيبراني الاردني

يمكن للتطور التكنولوجي أن يجعل الحياة اليومية أسرع وأفضل وأكثر سهولة، كما أن نتاجات الثورة الصناعية الرابعة قد تسهم بشكل كبير في حماية الجنس البشري من الكوارث والأزمات من خلال التنبؤ بها قبل حدوثها لإنقاذ المزيد من الأرواح، والتعجيل في تحقيق أهداف التنمية المستدامة، لكن الإنجازات الرقميّة تلك قد تسهم في تهديد الخصوصية وتقليص المساواة والاعتداء على أمن المعلومات أو البيانات الخاصة بالفرد وصولا إلى الدول والحكومات. أدركت الكثير من الحكومات المخاطر المحدقة لقطاع تكنولوجيا المعلومات والفضاء الرقمي الذي صار متأصلًا في كل مناحي الحياة، فاتخذت إجراءات وسنّت أساليب قانونية في هذا المجال لتعزيز بيئة رقمية آمنة وموثوقة إضافة إلى بناء قدرات وطنية لضمان مواجهة

التهديدات وحوادث أمن المعلومات والهجمات السيبرانية. يعد بناء استراتيجية سيبرانية وطنية بهدف حماية الفضاء السيبراني للدول ورفع مستوى الأمان المعلوماتي فيها، أولوية مُلحَّة بالنسبة لصناع القرار في سياساتهم الدفاعية خاصة في ظل تزايد تقديم الخدمات الإلكترونية وانتشار استخدام التقنية الرقمية بشكل واسع. كما تعمل كبرى الشركات في العالم على حماية مصالحها الاقتصادية وأعمالها ونشاطاتها بما يتوافق ويتماشى مع التطور التقني والمعلوماتي ومتطلباته القانونية من أسس ومعايير وسياسات من شأنها مواجهة المخاطر السيبرانية وفقا للتعليمات والإرشادات والأنظمة القانونية التي فرضتها الدولة التابعة لها. لا يمكننا أن ننكر أن قطاع الاختصاص في الأمن السيبراني لا يزال غير واضح الملامح، إلا أن الكثير من الدول ومن بينها الأردن تعمل على تطوير أساليب جديدة لاجتذاب وتثقيف الأفراد الموهوبين والاحتفاظ بهم، إضافة إلى استحداث تخصصات جامعية تُعنى بالأمن السيبراني أو علم البيانات أو أمن المعلومات. كما نظم المشرع الاردني قانون الأمن السيبراني في الأردن في عام ٢٠١٩م وأتت الإرادة الملكية السامية بالموافقة عليه في شهر ايلول من نفس العام، كما وافق مجلس النواب على إنشاء مجلس ومركز للأمن السيبراني، بهدف حماية المملكة من تهديدات وحوادث الأمن السيبراني. في الحقيقة لا يمكن أن تصبح الدولة آمنة في الفضاء السيبراني دون بناء كوادر وطنية تُعنى بالحفاظ على الأمن السيبراني وتنظيم إدارة فعالة لمخاطر الأمن السبيراني، إضافة إلى تعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية والتعاون والشراكات لأجل ذلك. إن الدول التي لا تسعى إلى حماية أمن معلوماتها من خلال بناء استراتيجية سيبرانية قد تهدم ثقة مواطنيها والمقيمين والمستثمرين في الفضاء السيبراني لهذه الدولة، إضافة إلى تقليل المخاطر السيبرانية من خلال خفض عدد الهجمات والسيطرة على آثارها، وأخيراً لا يمكن أن ينمو الاقتصاد الوطني في ظل وجود إمكانية خسائر محتملة من حوادث سيبرانية. لكن الكثير من العقبات قد تواجه تلك الدول خاصة في ظل

التطور التكنولوجي وتزايد التهديدات السيبرانية المواكبة له، بما في ذلك تهديدات نشطاء القرصنة الإلكترونية، ومجموعات الجرائم الإلكترونية المنظمة التي تمثل تهديدا على الأمن القومي.

أساليب تطور الأمن الإلكتروني والسيبراني في الأردن

أصبح أمن المعلومات والشبكات من أهم الاحتياجات لدى الوزارات والدوائر والمؤسسات الحكومية، وبالتالي أصبح يجب توفير ما يلي:

- تنفيذ الاجراءات والسياسات الكفيلة لضمان الحماية الكاملة للمقدرات والأنظمة والمعلومات .
- العمل على تقييم وتدقيق وضع أنظمة أمن وحماية المعلومات من كافة النواحي للتأكد من الالتزام بالسياسات والمقاييس المعتمدة وتقديم التوصيات لتحسين المستوى الأمني.
- إدارة أجهزة حماية الشبكات والأنظمة.
- رفع كفاءة الموظفين من خلال التدريب النوعي المتخصص.
- الفحوصات الدورية للأنظمة لكشف الثغرات.
- تحليل سجلات الحركات والبيانات المتوفرة لكشف التطفل ومتابعة أنماط الأنشطة التطفلية وتقييم المخاطر المحتملة.
- الإعلانات التوعوية والتحذيرات مثل تعميم إنذارات التطفل والتحذيرات من الثغرات.
- التعامل مع الثغرات الأمنية الموجودة أو المحتملة بتحليلها والاستجابة لها والتوعية بطرق التعامل معها.
- التعامل مع الأدلة الرقمية الخاصة بأمن المعلومات وبالتعاون مع الجهات المعنية.
- إدارة حوادث تكنولوجيا المعلومات والتعامل معها والاستجابة لها والتقليل من آثارها.

- التعامل مع الحوادث وتشمل استقبال التبليغات والتقارير عن الحوادث والمساهمة في عزل أنظمة المعلومات المصابة واحتواء المخاطر عن طريق تحليل الحوادث والاستجابة لها وتوفير الدعم الفني والتنسيق مع الجهات المعنية.
- خدمة الفحص الأمني للمواقع الإلكترونية الحكومية
- فحص المواقع الإلكترونية الحكومية المستضافة في المركز، والمستضافة خارج المركز بالتنسيق مع مديريات تكنولوجيا المعلومات التابعة لها وتقديم تقرير التوصيات لمعالجة الثغرات.
- الكشف المبكر لحالات الاختراق التي قد تتعرض لها الأنظمة والمواقع الإلكترونية الحكومية وتبليغ الجهات المعنية عند اكتشاف حوادث الاختراق لمعالجتها بالسرعة الممكنة.
- تقديم الاستشارة الفنية الخاصة بأمن وسلامة المواقع الإلكترونية عند طرح أي عطاء إنشاء أو تطوير للمواقع الإلكترونية الحكومية.

دور إدارة أمن المعلومات في فاعلية الحكومة الإلكترونية

إن إدارة أمن معلومات الحكومة الإلكترونية هى إحدى التحديات الرئيسة التي تواجه تطبيق الحكومة الإلكترونية, ويتعلق أمن معلومات الحكومة الإلكترونية بحماية بيانات ومعلومات ووثائق هذه الحكومة من الكشف والإفشاء المتعمد أو العرضي (غير المتعمد) للأفراد غير المخولين, ويتعلق أيضا بحماية بيانات ومعلومات ووثائق الحكومة الإلكترونية من إجراء أية تعديلات غير مصرح بها, وحماية هذه البيانات والمعلومات من التخريب والإهلاك والضياع, كما يُعني أمن معلومات الحكومة الإلكترونية بحماية نظم معلومات الحكومة الإلكترونية وحماية الأصول المعلوماتية للحكومة الإلكترونية وتوفير رقابة فاعلة على

عمليات الوصول Access إلى هذه البيانات والمعلومات في كل المستويات. ويعد أمن معلومات الحكومة الإلكترونية أحد المكونات الرئيسة والحيوية لبناء الثقة بين المواطنين وهذه الحكومة. إن عدم توفير المستوى الكافي من أمن المعلومات للحكومة الإلكترونية يعد أحد المعوقات الرئيسة لتطوير خدمات الحكومة الإلكترونية, وعليه, يمكن القول أن سياسات ومعايير أمن المعلومات يجب أن تتوافق مع توقعات المواطنين المتعلقة بمستويات الأمن المطلوبة عند التعامل مع الحكومة الإلكترونية. وفي ظل انتشار مبادرات ومشروعات الحكومة الإلكترونية في الكثير من دول العالم فقد تزايدت الأخطار التي تهدد أمن الحكومة الإلكترونية, وهذه الأخطار تؤثر في مستوى فاعلية الحكومة الإلكترونية. ولمواجهة هذه الأخطار التي تهدد أمن هذه الحكومة فقد تم استخدام كل الوسائل والأساليب التي تكفل تحقيق الأمن وتبني ثقة المستفيدين في الحكومة الإلكترونية. ويجري التعامل مع إدارة أمن معلومات الحكومة الإلكترونية كعنصر جوهري يساهم في تحقيق فاعلية هذه الحكومة والتزاماتها وتعهداتها نحو جميع المستفيدين من خدماتها ويؤدي الى توفير المخرجات التى تتوافق مع متطلبات هؤلاء المستفدين وتفي بحاجاتهم المتعددة. وتؤكد الدراسات السابقة في مجال أمن المعلومات والحكومة الإلكترونية على أن هناك مجموعة من المتطلبات والممارسات والقواعد والأدلة الإرشادية التي تعمل مع بعضها في منظومة متكاملة لتحقيق الأمن المطلوب والحماية الكافية للحكومة الإلكترونية. وتأتي هذه الدراسة للتعريف بالحكومة الإلكترونية وأهميتها وأهدافها ومزاياها, كما تتناول هذه الدراسة دور إدارة أمن المعلومات في تحقيق فاعلية هذه الحكومة.

استراتيجية أمن المعلومات تأتي في اطار مفهوم الامن الوطني

ان الاستراتيجية جاءت استجابة للتهديدات التي تفرضها التغيرات الهائلة والسريعة في تكنولوجيا المعلومات والاتصالات وهي مفتاح رئيس وخطوة اولى لضمان أمن المعلومات والامن السيبراني وتهدف الى تعزيز الأمن الوطني الأردني من خلال منع الهجمات الإلكترونية وتقليل المخاطر على البنى التحتية الحيوية الحرجة وبالتالي تعزيز الاقتصاد الاردني عن طريق زيادة الثقة بأنظمة المعلومات الحكومية والخاصة .

والفضاء السيبراني هو المجال المجازي لأنظمة الحاسوب والشبكات الإلكترونية؛ حيثُ تخزن المعلومات إلكترونيًا وتتم الاتصالات المباشرة على الشبكة، لذا فهو عالم غير مادي يشمل موضوعات مثل المعلومات الشخصية، والمعاملات الإلكترونية، والملكية الفكرية وغيرها.

وشرعت الوزارة بالتعاون مع مركز تكنولوجيا المعلومات الوطني بإعداد الخطة التنفيذية لإنشاء فريق "سيرت الاردن" الذي سيقوم بمساعدة الجهات المستفيدة من القطاعين العام والخاص على الاستجابة لحوادث امن المعلومات والتقليل من آثارها كما سيسهم برفع الوعي العام بالتهديدات التي تفرضها المتغيرات بالفضاء السيبراني.

وإن الخطة تعتمد على استغلال الموارد المتاحة بحيث يتم إنشاء الفريق بكلف مقتدر عليها وعلى عدة مراحل تبدأ المرحلة الأولى بتقديم الخدمات للجهات الحكومية ومن ثم تمتد الخدمات لتشمل قطاع البنى التحتية الحرجة والشركات المتوسطة والصغيرة والافراد .

ولفت الى انه سيتم قريبا تشكيل نواة فريق السيرت وتأهيله ليبدأ بتقديم خدماته الفعلية للمعنيين في مطلع العام المقبل.

جهود الوزارة في مجال أمن المعلومات أدت الى توقيع مذكرة تفاهم مع مجموعة "بالادن" الاميركية لتحقيق مجموعة من الاهداف في مجال امن المعلومات والشبكات، وذلك من خلال اقتناء افضل التكنولوجيا وتمكين الاردن من الاطلاع على افضل الممارسات في مجالات حماية البنية التحتية للمعلومات الحرجة من الهجمات السيبرانية، والحد من مواطن الضعف للبنى التحتية الحيوية للمعلومات، وتحسين وقت الاسترداد من الهجمات التي تحدث، وتوفير آلية لتعزيز البنية التحتية، والتدريب على برامج التوعية في أمن المعلومات، والاستثمار لتطوير صناعة محلية للأمن السيبراني في الأردن، بهدف جعل الأردن رائدا إقليميا في هذا المجال.

ضمن جهود الوزارة في أمن المعلومات فقد عقدت بالتعاون مع الاتحاد الدولي للاتصالات (إمباكت) أخيرا ورشة عمل اقليمية تحت عنوان "الامن السيبراني" هدفت الى زيادة الوعي بالسياسات والمنهجيات والتقنيات المتبعة لمكافحة القرصنة على الانترنت بما في ذلك كيفية حماية الاطفال على الانترنت، وشارك في الورشة المشغلون والجهات التنظيمية من 8 دول عربية بحضور مكثف من المختصين في الاردن.

وفي مجال تحديث السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد بين التل ان الوزارة انتهت من إعداد مسودة السياسة العامة المقترحة 2012 التي ستعالج قضايا التطورات التكنولوجية والقضايا القانونية والتنظيمية التي تفرزها هذه التطورات ولاسيما الانتقال المتسارع نحو الاتصالات المندمجة المبنية على بروتوكول الإنترنت وتوفير خدمات جديدة ومتطورة للمواطنين والشركات اضافة الى تعزيز

استقلالية هيئة تنظيم قطاع الاتصالات الادارية والمالية لتمكينها من القيام بمهامها وتنفيذ قراراتها بشكل فعال.

إن السياسة تدعو الى توفير الظروف الملائمة للوصول إلى المنافسة الفعالة في قطاع الاتصالات وتوفير البيئة المناسبة لتحفيز الاستثمار في قطاعي الاتصالات وتكنولوجيا المعلومات وتطوير ونشر المحتوى المحلي والعربي بما فيها تطبيقات الهواتف النقالة.

وفيما يتعلق بقطاع البريد تدعو المسودة الى الاستمرار في إصلاحات قطاع البريد لضمان قدرته على التطور والاستجابة لمتطلبات السوق والمتطلبات الاجتماعية من خلال توفير خدمات بريدية بجودة عالية وأسعار مناسبة ومتاحة في جميع انحاء المملكة.

المراجع

سليمان, مروة. "نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية." المجلة المصرية للعلوم الاجتماعية والسلوكية 6.6 (2022): 114-130.

النوايسة, et al. "جرائم التجسس الإلكتروني في التشريع الأردني دراسة تحليلية." دراسات (علوم الشريعة والقانون) 57.46 (2019): 467-482.

عبد الله ذيب. "جريمة الدخول غير المصرح به الواقعة على الشبكات الإلكترونية الحكومية (دراسة مقارنة على التشريعات الأردنية والفلسطينية)." (2020).

بن سعيد بن علي أبو داسر, عبد الله, and عبد الله. "حماية الملكية الفكرية في الأمن السيبراني." روح القوانين 92.1 (2020): 415-510.

الزهراني, et al. استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة: دراسة مقارنة. Diss. جامعة نايف العربية للعلوم الأمنية, 2020.

العتيبي، and عبد الرحمن بن بجاد شارع. دور الأمن السيبراني في تعزيز الأمن الإنساني. 2017 .Diss.

الغبيوي, مالك بن فهد عبد الهادي, الحارثي, & سلطان بن منير. مشرف. (2020). الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية).