HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير للعام 2022 = 4.91

عنوان البحث

الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن

سناء احمد عبدالله الشديفات[1]

[1] وزارة الادارة المحلية، رئيس قسم الحاسوب، بلدية منشية بني حسن، الأردن.

بريد الكتروني: Sanaa.uoh@gmail.com

HNSJ, 2024, 5(1); https://doi.org/10.53796/hnsj51/56

تاريخ النشر: 2024/01/01م تاريخ القبول: 2023/12/15م

المستخلص

هدفت الدراسة إلى التعرف على الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن. وقد تناولت الدراسة أهمية الأمن السيبراني مفهومه وعناصره, كذلك أكدت الدراسة على إن حماية أمن المعلومات أصبح من الضروري الإهتمام به لأن اختراق المعلومات يشكل خطر على مؤسسات الدولة والأفراد مما يهدد أمن الدولة واستقرارها. وقد أنشأت الأردن المركز الوطني للأمن السيبراني والذي يعد مرجع للمؤسسات والبنوك والبلديات في الأردن، وباعتبار إن بلدية منشية بني حسن تعمل جاهده للحفاظ على أمن بيانتها ومعلوماتها جاءت هذه الدراسة للتعرف على كيفية حماية البيانات والمعلومات من الأختراق الأمني الذي يشكل تهديد للبيانات في إطار تهديدات الأمن السيبراني.

واعتمدت الدراسة على استخدام المنهج الوصفي لدراسة الظواهر الاجتماعية والإنسانية, حيث تقوم الدِّراسة على توظيف هذا المنهج لبيان الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن.

وقد توصلت الدراسة إلى مجموعة من النتائج والتوصيات, حيث أكدت الدراسة على ضرورة تأمين الفضاء الإلكتروني بشكل خاص بسبب الإختراقات الإلكترونية المعقدة لما يشكله من مخاطر متزايدة يمكن أن تسبب ضررًا أو تعطل الخدمات لدى المؤسسات والبلديات في الأردن. كما وأوصت الدراسة بشكل خاص بأن على بلدية منشية بني حسن حماية أمن المعلومات خصوصاً في ظل التحول الرقمي والخدمات الإلكترونية التي تطبقها البلدية مما يهدد أمن المعلومات والبيانات لقسم الحاسوب وتقنية المعلومات وباقي الأقسام.

الكلمات المفتاحية: الامن السيبراني، أمن المعلومات، قسم الحاسوب وتقنية المعلومات، بلدية منشية بني حسن

RESEARCH TITLE

CYBERSECURITY FOR DATA AND INFORMATION PROTECTION IN THE DEPARTMENTS OF THE MANSHEYET BENI HASSAN MUNICIPALITY

Sana'a Ahmed Abdullah Al-Shdefat[1]

[1] Ministry of Local Administration, Head of the Computer Department, Mansheyet Bani Hassan Municipality, Jordan.
Sanaa.uoh@gmail.com

HNSJ, 2024, 5(1); https://doi.org/10.53796/hnsj51/56

Published at 01/01/2024 **Accepted at 15/12/2023**

Abstract

The study aimed to identify Cybersecurity for Data and Information Protection in the departments of the Mansheyet Beni Hassan Municipality. The study addressed the importance of Cybersecurity, its concept and elements. The study also emphasized that protecting information security has become necessary to pay attention to because information penetration poses a threat to state institutions and individuals, which threatens the state's security and stability. Jordan has established the National Center for Cybersecurity, which is a reference for Institutions, Banks and Municipalities in Jordan. Considering that the Municipality of Manshiyet Bani Hassan works hard to maintain the security of its data and information, this study came to identify how to protect data and information from security breaches that pose a threat to the data within the framework of Cybersecurity threats.

The Study relied on the Use of the Descriptive Approach to study Social and Human Phenomena. The study is based on employing this approach to demonstrate Cybersecurity and the Protection of Data and Information in the Departments of the Manshiet Bani Hassan Municipality.

The Study reached a set of results and recommendations, also emphasized the necessity of securing Cyberspace in particular due to complex electronic penetrations, as they pose increased risks that could cause damage or disruption of services to institutions and municipalities in Jordan. The study also recommended in particular that the municipality of Mansheyet Bani Hassan must protect information security, especially in light of the digital transformation and electronic services implemented by the municipality, which threatens the security of information and data for Department of Computer and Information Technology and the rest of the all departments.

Key Words: Cybersecurity, Information Security, Department of Computer and Information, Mansheyet Bani Hassan Municipality.

المقدمة

يعد الفضاء الإلكتروني وكامل بنيته التحتية عرضة لمجموعة واسعة من المخاطر الناجمة عن التهديدات والمخاطر المادية والسيبرانية. ويستغل الفاعلون السيبرانيون ضعف الدول لسرقة المعلومات والأموال وتطوير القدرات لتعطيل أو تدمير أو تهديد الخدمات الإلكترونية الأساسية، وفي الواقع يصعب تأمين الفضاء الإلكتروني بشكل خاص بسبب الإختراقات الإلكترونية المعقدة والتي تشكل مخاطر متزايدة يمكن أن تسبب ضررًا أو تعطل في الخدمات التي يعتمد عليها أقتصاديات الدول والأمن الداخلي للدول.

لقد أدى التوسع الكبير في إستخدام ثورة المعلومات والأجهزة الدقيقة المرتبطة بها، لتغيير العديد من المفاهيم المتعلقة بالدولة والسيادة والأمن. وأصبح للفضاء السيبراني أهمية كبيرة سواء في المجالات العسكرية أو المالية أو الإدارية , لذا أصبح من أبرز سمات الحياة العصرية هو حماية أمن المعلومات, وإذا أخترقت المعلومات فان ذلك يشكل خطر على مؤسسات الدولة والأفراد على حد سواء، مما يهدد أمن الدولة واستقرارها على جميع المستويات، خاصة وأن تلك المخاطر تختلف في طبيعتها عن المخاطر التقليدية.

ولا شك إن الأردن جزء من المنظومة العالمية التي ترتبط بمؤسسات العالم أقتصادياً وسياسياً وأمنياً, وقد تم إنشاء المركز الوطني للأمن السيبراني لحماية أمنها الوطني من الأختراق الإلكتروني وحفظ البيانات والمعلومات والشبكات الإلكترونية, فلم يعد الأمن التقليدي هو الأمن الموجود على الأرض الذي يحمي الحدود والجغرافيا بل هناك حاجة للأمن السيبراني للحفاظ على البنية الإلكترونية للمؤسسات والدوائر الحكومية والخاصة في الأردن.

وتعد بلدية منشية بني حسن من البلديات الأردنية التي تعني أهتماماً بالغاً في الحفاظ على بياناتها, حيث يشكل قسم الحاسوب وتقنية المعلومات من الأقسام التي تتابع وتراقب الأقسام الأخرى من خلال تقديم الإرشادات والصيانة وتحليل البيانات والمعلومات وطرق حفظها والتعامل معها وبيان خطورة الأمن السيبراني على بيانات البلدية.

مشكلة الدراسة : تبرز إشكالية الدراسة من خلال بيان الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن, حيث شكل أمن البيانات السيبراني تهديداً للبيانات في البلديات ومؤسسات الدولة, كما لم يعد العمل التقليدي مجدياً في ظل ثورة المعلومات والتقنيات والتكنولوجيا بحيث أصبح العالم مربوط ألكترونياً وهذا الربط يشكل تهديد للأمن السيبراني.

أهمية الدراسة : تبرز أهمية الدراسة من نطاقيني نظري وتطبيقي .

الأهمية النظرية: قد تشكل أهمية البحث نقلة نوعية في معرفة الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن, وقد تفيد البلديات ومراكز البحث والمكتبات الأردنية والعربية لمعرفة خطورة الأمن السيبراني.

الأهمية التطبيقية: حيث تبرز الأهمية التطبيقية في بيان أهمية الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن, وبيان أهمية ما قد يشكله الإقتحام الألكتروني من مخاطر على أمن المعلومات لبلدية منشية بني حسن. لذا أصبحت الحاجة في الأردن إلى إيجاد منظومة أمنية إلكترونية تكافح التهديد الإلكتروني, وقد يشكل المركز الوطني الأردني للأمن السيبراني أبرز المنظومات الأمنية التي تكافح الهجمات

الإلكترونية على مؤسسات الدولة الأردنية والبلديات الأردنية.

أهداف الدراسة : سعت الدراسة لبيان الأهداف التالية :

1- مفهوم الأمن السيبراني وأهميته.
2- بيان العناصر الرئيسة للأمن السيبراني.
3- بيان أنواع التهديدات السيبرانية.
4- بيان وظائف المركز الوطني للأمن السيبراني الأردني.
5- بيان دور قسم الحاسوب وتقنية المعلومات في بلدية منشية بني حسن.

أسئلة الدراسة : سعت الدراسة للإجابة على التساؤلات التالية :

1- ما مفهوم الأمن السيبراني؟ وما أهميته؟
2- ما العناصر الرئيسة للأمن السيبراني؟
3- ما أنواع التهديدات السيبرانية؟
4- ما وظائف المركز الوطني للأمن السيبراني الأردني ؟
5- ما دور قسم الحاسوب وتقنية المعلومات في بلدية منشية بني حسن ؟

منهجية الدراسة: أستخدمت الدراسة المنهج الوصفي التحليلي كطريقة لدراسة الظواهر أو المشكلات العلمية من خلال القيام بالوصف بطريقة علمية، لتحليل الظواهر الأجتماعية الأمنية ومن ثم الوصول إلى تفسيرات منطقية لها دلائل وبراهين تمنح الباحث القدرة على تحليل وتفسير دور الأمن السيبراني في تعزيز الأمن الوطني الأردني.

مصطلحات الدراسة

الأمن السيبراني : هو الأمن الذي يهتم ويعتني بالتطبيقات الإلكترونية وتطبيق التقنيات، والعمليات، والضوابط، بقصد حماية الأنظمة والبيانات، وشبكات الحواسيب، والبرامج الداخلية، والأجهزة الكمبيوترية، ومن التعرض للهجمات الإلكترونية التي قد تشكل تدميراً للبنية التحتية الإلكترونية مما يؤثر ذلك على أمن الدولة وأقتصادها .[1]

أمن المعلومات : هي مجموعة من الإجراءات والأدوات الأمنية التي تحمي على نطاق واسع معلومات المؤسسة الحساسة من سوء الإستخدام أو الوصول غير المصرح به أو التعطيل أو الإتلاف. ويشمل أمان المعلومات الأمن المادي والبيئي والتحكم في الوصول، والأمان عبر الإنترنت[2].

قسم الحاسوب وتقنية المعلومات : هو قسم يهتم بتقنية المعلومات لكافة التطبيقات والأنظمة التكنولوجية الحديثة التي تستخدمها البلديات والمؤسسات من أجل تحسين أداء العمل وزيادة الإنتاجية، والقيام بتحليل وإعداد وتصميم وتقييم أنظمة الحاسوب لكل أقسام البلدية [3].

بلدية منشية بني حسن : مؤسسة أهليه مستقلة مالياً وإدارياً، ذات شخصية إعتبارية مناط بها إحداث أو إلغاء أو

---

[1] – الخزاعله , عبير (2021). مفهوم الأمن السيبراني, موقع موضوع , 17, تشرين ثاني , الاردن.

[2] – الفتلاوي, أحمد عبيس نعمة(2016). "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر". مجلة المحقق الحلي للعلوم القانونية والسياسية,العراق.

[3] – ابو سليمان، محمد عبدالمنعم (2018).أهمية تكنولوجيا المعلومات والاتصالات في بناء اقتصاد المعرفة.المجلة المصرية لعلوم المعلومات,22-168 , ,مصر.

تعيين حدود منطقتها، ووظائفها وسلطتها بمقتضى أحكام القانون. ومن خلال المجلس البلدي يتم التخطيط وأتخاذ القرارات بشأن ما يجب القيام به وإدارة كافة الخدمات والمرافق والمشاريع المحلية المناطه بها[4].

المبحث الأول : مفهوم الأمن السيبراني وعناصره

يعرف الأمن السيبراني على أنه "مجموعة من الآليات والوسائل والإجراءات التي تهدف إلى حماية البيانات والبرمجيات وأجهزة الكمبيوتر من الهجمات والأختراقات التي قد تهدد الأمن الوطني للدول"، وتشكل المليشيات والفواعل غير الحكومية المنفذ الرئيسي للهجمات السيبرانية بغرض تدمير شبكة الأمن المعلوماتي لدى الدول, وللدفاع عن ذلك لابد من تطوير القدرة على الأستجابة السريعة للهجمات السيبرانية، والعمل على تطوير الأدوات السيبرانية وتعزيز قدراتهم[5].

أن تعزيز أنظمة الأمن السيبراني في الأردن قد أسهم في دعم قطاع الأعمال وتوفير بيئة آمنة للإستثمار. ويلعب الأمن السيبراني دورًا مهمًا في سباق العالم نحو التحول الرقمي. وتبرز أهمية المركز الوطني للأمن السيبراني في حماية المؤسسات الرسمية ومختلف القطاعات الأقتصادية الحيوية والبلديات، بأعتبار أن البنية التحتية في الأردن "جاهزة لتعزيز الأمن السيبراني والتحول الرقمي، وهو ما يجب تسريعه" ليشجع الأستثمار ويحسن بيئة الأعمال.[6]

وأن الهجمات الإلكترونية تتزايد في كل الأوقات، حيث يتم تخزين معظم البيانات على الأنظمة السحابية، مما يجعل عملية الأختراق أسهل بكثير وهذه المشكلة تتطلب أنظمة أمن سيبراني قوي. وقد تشكل حماية البيانات تكلفة مادية عالية على بلدية منشية بني حسن، مما يشكل تحديًا أمام تعزيز الأمن السيبراني، بالإضافة إلى ذلك فإن نقص الوعي والمعرفة بمفهوم الأمن السيبراني يزيد من هذه المشكلة لدى البلديات[7].

أن الهجمات الإلكترونية تحدث بعدة طرق، يمكن أن تشمل: التخريب والتعطيل وسرقة المعلومات وأستغلال البيانات بقصد الإضرار بسمعة البلدية، وتعطيل أنظمه معينه، وأستبدال المعلومات، وطلب المال مقابل البيانات. لذلك أصبح من الضروري توفير جدران حماية للأجهزة الشخصية للموظفين الذين يعملون في البلدية ومن الضروري تدريبهم على حماية البيانات وعملية تخزين المعلومات بشكل صحيح وآمن. لأن الأمن السيبراني يعزز النمو والتقدم في مختلف الأعمال وأن العلاقات الدولية أصبحت الآن مبنية على ضمان الأمن السيبراني. [8]

فالأمن السيبراني هو ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة. ويُعرف أيضًا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية.

---

[4] – قبيلات حمدي(2017).التشريعات الناظمة لعمل مجالس المحافظات والبلدية والمحلية في الأردن، الوكالة الالمانية واللجنة الوطنية الاردنية لشؤون المراة ، الاردن.

[5] – Lehto Martti , Neittaanmäk Pekka(2015) .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing,. Switzerland

[6] – المبيضين , ابراهيم (2022). التهديدات السيبرانية من أكثر الجرائم انتشارا حول العالم,صحيفة الغد, 25, تموز , الاردن.

[7] – Lehto Martti , Neittaanmäk Pekka(2015) .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing,. Switzerland.

[8] – الخزاعلة , عبير (2021). مفهوم الأمن السيبراني, موقع موضوع , 17, تشرين ثاني, الاردن.

العناصر الرئيسة للأمن السيبراني

يشكل الأمن السيبراني أبرز مظاهر العصر الأمنية والذي يتشكل موقعه في الفضاء الإلكتروني, فهو عابر للحدود والجغرافيا في ظل العولمة التي تستند على عوامل الربط الأقتصادي واللأمني والسياسي حيث أن العالم مربوط في منظومة إلكترونية تقوم على أساس (أمان التطبيق، أمن المعلومات، وأمن الشبكة, وأمن المستخدم النهائي، والأمن التشغيلي) والتي يمكن تلخيصها كما يلي:[9]

أولاً: أمان التطبيق : ويعني إبقاء البرامج والأجهزة خالية من التهديدات. حيث أنه يوفر التطبيق المخترق طريقة للوصول إلى البيانات المصممة لحمايتها، ويبدأ الأمان الناجح في مرحلة التصميم، قبل نشر البرنامج أو الجهاز بوقت طويل. ويتعلق أمان التطبيقات بالحفاظ على تطبيقات البرامج منيعة أمام التهديدات. في حين أن هذا يمثل تركيزًا كبيرًا للشركات التي تطور وتبيع تطبيقاتها وخدماتها السحابية على الأهتمام بأمن تطبيقاتها. ويعد التهيئة الخاطئة لإعدادات الأمان سببًا رئيسيًا لخروقات بيانات الحساب السحابي. وتستخدم الشركات خدمة سحابية رئيسية، مثل Microsoft 365 ، لكنها لا تدرك أنها بحاجة إلى تخصيص إعدادات الأمان الخاصة بها من الإعدادات الافتراضية. ومن الأسباب الرئيسية لسوء تهيئة التطبيق السحابي هي:[10]

1- قلة الوعي بسياسات أمان السحابة.
2- عدم وجود ضوابط ورقابة كافية.
3- استخدام الكثير من الواجهات للتحكم.
4- سلوك إهمال من الداخل (على سبيل المثال ، خطأ مستخدم).
5- الإجراءات مثل إعداد ضوابط متعددة العوامل وأمتيازات الإدارة، وهي خطوات ستتخذها خدمات أستشارات الأمن السيبراني للمساعدة في تعزيز أمان التطبيق ومنع اختراق تطبيقاتك.

ثانياً : أمن المعلومات : يغطي أمن المعلومات حماية بيانات الشركة والبيانات التي تجمعها من العملاء أو البائعين. وتحتاج معظم الشركات إلى الألتزام بواحد أو أكثر من معايير أمن المعلومات، ويمكن أن يكون لهذه المعايير عقوبات صارمة إذا كان الإهمال يؤدي إلى أختراق معلومات التعريف الشخصية. وتنظر شركات الأمن السيبراني في كيفية جمع البيانات وتخزينها ونقلها، من خلال وضع وسائل حماية لضمان تشفير البيانات حسب الحاجة لحمايتها من الإختراق.[11]

ثالثاً : تخطيط التعافي من الكوارث : تسعى العديد من الشركات للحصول على المساعدة من خدمات إستشارات الأمن السيبراني عندما يتعلق الأمر بتخطيط التعافي من الكوارث. هذا هو المفتاح للحفاظ على العمل من بين 60٪ من تلك التي تتضاعف بعد وقوعها ضحية لهجوم إلكتروني، وتشتمل حماية التعافي من الكوارث على مكونين مهمين:[12]

---

[9] – الأشقر , جبور منى(2016). السيبرانية هاجس العصر. بيروت: جامعة الدول العربية – المركز العربي للبحوث القانونية والقضائية،لبنان..

[10] – الفتلاوي أحمد عبيس نعمة(2016). "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر". مجلة المحقق الحلي للعلوم القانونية والسياسية,

[11] – محمود لمى عبدالباقي, و كيطان اسراء نادر(2021)"المسؤولية الدولية عن الاضرار التي تحدثها الهجمات الإلكترونية". مجلة العلوم القانونية 36 (كانون اول):336_362.مصر.

[12] – الموسوي، علي محمد كاظم (2019). المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان

1- إستراتيجيات لمنع حدوث إختراق أو إصابة بالبرامج الضارة.

2- الأستعدادات للشفاء السريع في حالة وقوعك ضحية لهجوم.

رابعاً: أمن الشبكة : ويعني ممارسة تأمين شبكة الكمبيوتر من المتطفلين ، سواء كانوا مهاجمين مستهدفين أو برامج ضارة إنتهازية. ويتضمن أمان الشبكة حماية شبكتك المادية وجميع الأجهزة المتصلة بها. وتستخدم معظم الشركات جدران الحماية لمراقبة حركة المرور الواردة والصادرة بحثًا عن التهديدات. ويعد تأمين شبكتك اللأسلكية والتأكد من حدوث أي إتصالات عن بُعد من خلال طرق مشفرة من الطرق التي تضمن بها خدمات الأمن السيبراني أمان الشبكة. وقد تم تصميم أمان الشبكة لضمان وصول المستخدمين المصرح لهم فقط إلى الشبكة، وعدم حدوث أي سلوكيات مشبوهة داخل الشبكة من شأنها أن تشير إلى حدوث خرق.[13]

خامساً: أمن المستخدم النهائي : ويعرف أمان المستخدم النهائي أيضًا باسم أمان نقطة النهاية، ويشير هذا إلى حماية الأجهزة التي يعمل بها المستخدمون أنفسهم. ويعد أمان المستخدم النهائي أمرًا حيويًا، نظرًا لأن 91٪ من الهجمات الإلكترونية تبدأ برسالة بريد إلكتروني للتصيد الإحتيالي. وتتضمن بعض الأنواع الأكثر شيوعًا لحماية المستخدم النهائي التي يجب أن تتمتع بها ما يلي:[14]

1- تحديث الأجهزة باستمرار.

2- إدارة مكافحة الفيروسات / مكافحة البرامج الضارة.

3- تصفية DNS لحظر المواقع الضارة.

4- حماية البرامج الثابتة لمنع الخروقات في طبقة البرامج الثابتة.

5- أقفال الشاشة المحمية برمز المرور.

6- الإدارة عن بعد وكشف الجهاز.

سادساً: الأمن التشغيلي: ويعني العمليات والقرارات الخاصة بمعالجة أصول البيانات وحمايتها، والأذونات التي يمتلكها المستخدمون عند الوصول إلى شبكة والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أومشاركتها كلها تندرج تحت هذه المظلة. ويتضمن الأمن التشغيلي إتخاذ خطوة إلى الوراء والنظر إلى إستراتيجيتك الأمنية بالكامل ككل للتأكد من أن جميع التكتيكات الأمنية تعمل في أنسجام خلال عملياتك، وعدم تعارض أي منها مع بعضها البعض. وعند تقديم الأستشارات الأمنية التشغيلية، سيحاول MSP التفكير كمهاجم. سيقومون بفحص جميع المجالات المختلفة لبيئة التكنولوجيا الخاصة بك لمعرفة مكان حدوث الخرق المحتمل. فالأمن التشغيلي هو المظلة التي تشمل جميع عمليات أمن تكنولوجيا المعلومات الخاصة بك. كما إنه يضمن أن العملية ككل لا تقوم فقط بتأمين جميع مناطق الخرق المحتمل، بل تقوم أيضًا بتحديث إستراتيجياتها الأمنية بانتظام لمواكبة أحدث التهديدات والتقدم الأمني.[15]

---

[13] – الدليمي، حسام جاسم محمد أحمد(2018). التطور التكنولوجي واثره في سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية القانون والعلوم السياسية– جامعة الانبار، الانبار، العراق.

[14] – حمد عبيس نعمة الفتلاوي وزهراء عماد محمد(2020). تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد44، العدد1، كلية القانون والعلوم السياسية –جامعة الكوفة، الكوفة، العراق.

[15] – العظامات، جمال(2015). جريمة العدوان في الهجمات الالكترونية في القانون الدولي العام، مجلة المنارة للدراسات القانونية والإدارية، المجلد21، العدد4، مركز المنارة للدراسات والأبحاث، المغرب.

وهناك عدد من الأنواع المختلفة من البرامج الضارة والتي تشكل تهديد لأمن المعلومات والتي قد تحدث تدمير للمعلومات أو عطب للبيانات بحيث تصبح مفقودة تماماً مما يثير حالة من التهديد لأمن الدولة وخاصة إذا تعلقت المعلومات والبيانات بقضايا تمس أمن المواطن والدولة والتي من أبرزها :[16]

1- الفيروسات: وهي برنامج ذاتي النسخ يربط نفسه بملف نظيف وينتشر في جميع أنحاء نظام الكمبيوتر، ويصيب الملفات بشفرات ضارة.

2- أحصنة طروادة : وهي نوع من البرامج الضارة التي تتنكر في شكل برامج شرعية. ويخدع مجرمو الإنترنت المستخدمين لتحميل أحصنة طروادة على أجهزة الكمبيوتر الخاصة بهم حيث يتسببون في إتلاف أو جمع البيانات.

3- برنامج التجسس: وهو برنامج يسجل ما يفعله المستخدم سرًا ، بحيث يمكن لمجرمي الإنترنت الإستفادة من هذه المعلومات. على سبيل المثال، يمكن لبرامج التجسس التقاط تفاصيل بطاقة الأئتمان.

4- برامج الفدية: وهي برامج ضارة تقوم بتأمين ملفات المستخدم وبياناته، مع التهديد بمسحها ما لم يتم دفع فدية.

5- برامج الإعلانات المتسللة: برامج إعلانية يمكن إستخدامها لنشر البرامج الضارة.

6- شبكات الروبورت : وهي شبكات الكمبيوتر المصابة ببرامج ضارة والتي يستخدمها مجرمو الإنترنت لأداء المهام عبر الإنترنت والذي يدير ويتحكم بشبكة الأجهزة المخترقة ويستغلها في تنفيذ هجماته الرئيسية.

وقد برز أستخدام الأمن السيبراني بعد الثورة التقنية والتكنولوجية حيث تم أستخدامه من قبل الفواعل غير الحكومية والتي شكلت تهديد للشبكات الألكترونية الدولية والتي من أبرزها: [17]

1- الدول: فالدولة هي الفاعل الأساسي الذي يمتلك العالم الأفتراضي لما لها من مكانة وخصوصية وصلاحيات في أجوائها الفضائية وما تتميز فيه من التفوق التكنولوجي والمؤهلات التي ترشحها لتبني هذه المكانة.

2- الفواعل غير الحكومية: وهي المنظمات والشركات عابرة القومية التي تستخدم التكنولوجيا في عمالها والتي يمكنها أختراق المواقع الإلكترونية وأستهداف الأنظمة الدفاعية للدول.

3- المنظمات الإجرامية: وتقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات وأختراق الحسابات البنكية وتحويل الأموال في أطار السوق السوداء.

4- الشركات المتعددة الجنسيات تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدول، فخوادم الشركات مثل قوقل والفيسبوك

[16] – طلال ياسين العسي وعدي أحمد عناب(2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19، العدد الاول، جامعة الزرقاء، الاردن.

[17] – فاطم بيرم(2020). السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية:الصين نموذجاً، المجلة الجزائرية للامن الانساني ، المجلد الخامس، العدد الاول ، مخبر الامن الانساني–جامعة باتنة، الجزائر.

والمايكروسوفت والتي يسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتشتغل الأسواق، وتؤثر في أقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها[18].

5- الجماعات الإرهابية: والتي تعد من أبرز الفواعل الدولية، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجُدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.

6- الأفراد العاديين: وقد أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية، وتشكل ظاهرة الويكيليكس أبرز الوثائق السرية التي نشرت ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها، ما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.

أنواع التهديدات السيبرانية

تتمثل التهديدات التي يواجهها الأمن السيبراني في ثلاثة جوانب:[19]

1. تشمل الجرائم الإلكترونية جهات فاعلة فردية أو مجموعات تستهدف الأنظمة لتحقيق مكاسب مالية أو التسبب في تعطيلها.
2. غالبًا ما تتضمن الهجمات الإلكترونية جمع معلومات ذات دوافع سياسية.
3. يهدف الإرهاب السيبراني إلى تقويض الأنظمة الإلكترونية لإثارة الذعر أو الخوف.

إذًا، كيف يمكن للجهات الخبيثة السيطرة على أنظمة الكمبيوتر؟ فيما يلي بعض الأساليب الشائعة المستخدمة لتهديد الأمن السيبراني:[20]

1. البرامج الضارة: تعد البرامج الضارة أحد أكثر التهديدات السيبرانية شيوعًا، وهي برامج أنشأها مجرم إلكتروني أو متسلل لتعطيل جهاز الكمبيوتر الخاص بالمستخدم الشرعي أو إتلافه. غالبًا ما تنتشر البرامج الضارة عبر مرفق بريد إلكتروني غير مرغوب فيه أو تنزيل يبدو شرعيًا، ويمكن أن يستخدمها مجرمو الإنترنت لكسب المال أو في هجمات إلكترونية ذات دوافع سياسية.
2. الفيروس: برنامج ذاتي النسخ يلتصق بملف نظيف وينتشر في جميع أنحاء نظام الكمبيوتر، مما يؤدي إلى إصابة الملفات برموز ضارة.
3. أحصنة طروادة: نوع من البرامج الضارة المتخفية في هيئة برامج شرعية. يخدع مجرمو الإنترنت المستخدمين لتحميل أحصنة طروادة على أجهزة الكمبيوتر الخاصة بهم حيث تتسبب في تلف البيانات أو جمعها.
4. برامج التجسس: برنامج يسجل سرًا ما يفعله المستخدم، حتى يتمكن مجرمي الإنترنت من الاستفادة من هذه المعلومات. على سبيل المثال، يمكن لبرامج التجسس التقاط تفاصيل بطاقة الائتمان.

---

[18] – Marie Baezner, Patrice Robin,(2018) Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS),.

[19] – إسماعيل زروقة. (2019,). الفضاء السيبراني والتحول في مفاهيم القوة والصراع, مجلة العلوم القانونية والسياسية, مصر.

[20] – رغدة ، البهي. (2018). الردع السيبراني :المفهوم والإشكاليات والمتطلبات . مجلة الدراسات الإعلامي.,مصر.

5. برامج الفدية: برامج ضارة تعمل على تأمين ملفات المستخدم وبياناته، مع التهديد بمسحها ما لم يتم دفع فدية.
6. برامج الإعلانات المتسللة: برامج إعلانية يمكن استخدامها لنشر البرامج الضارة.
7. شبكات الروبوت: شبكات من أجهزة الكمبيوتر المصابة بالبرامج الضارة والتي يستخدمها مجرمو الإنترنت لأداء المهام عبر الإنترنت دون إذن المستخدم.[21]
8. حقن SQL: يعد حقن SQL (استعلام اللغة المنظمة) نوعًا من الهجمات الإلكترونية المستخدمة للتحكم في البيانات وسرقتها من قاعدة البيانات. يستغل مجرمو الإنترنت نقاط الضعف في التطبيقات المستندة إلى البيانات لإدراج تعليمات برمجية ضارة في قاعدة بيانات عبر عبارة SQL ضارة. وهذا يتيح لهم الوصول إلى المعلومات الحساسة الموجودة في قاعدة البيانات[22].
9. التصيد: يحدث التصيد الإحتيالي عندما يستهدف مجرمو الإنترنت الضحايا برسائل بريد إلكتروني تبدو وكأنها من شركة شرعية تطلب معلومات حساسة. غالبًا ما تُستخدم هجمات التصيد الاحتيالي لخداع الأشخاص لتسليم بيانات بطاقة الائتمان والمعلومات الشخصية الأخرى.
10. هجوم قطع الخدمة (هجوم رفض الخدمة): حيث يقوم مجرمو الإنترنت بمنع نظام الكمبيوتر من تلبية الطلبات المشروعة عن طريق إغراق الشبكات والخوادم بحركة المرور. وهذا يجعل النظام غير قابل للاستخدام، مما يمنع المنظمة من القيام بوظائف حيوية[23].

تركز بروتوكولات الأمان الإلكترونية أيضًا على أكتشاف البرامج الضارة في الوقت الفعلي، ويستخدم الكثيرون التحليل الإرشادي والسلوكي لمراقبة سلوك البرنامج ورمزه للدفاع ضد الفيروسات أو أحصنة طروادة التي تغير شكلها مع كل عملية تنفيذ (البرامج الضارة متعددة الأشكال والمتحولة). يمكن لبرامج الأمان أن تحصر البرامج الضارة المحتملة في فقاعة أفتراضية منفصلة عن شبكة المستخدم لتحليل سلوكها ومعرفة كيفية أكتشاف الإصابات الجديدة بشكل أفضل[24].

وتستمر برامج الأمان في تطوير دفاعات جديدة حيث يحدد متخصصي الأمن السيبراني التهديدات الجديدة وطرقًا جديدة لمكافحتها. لتحقيق أقصى أستفادة من برامج أمان المستخدم النهائي، ويحتاج الموظفون إلى التثقيف حول كيفية أستخدامها. والأهم من ذلك، أن استمرار تشغيله وتحديثه بشكل متكرر يضمن قدرته على حماية المستخدمين من أحدث التهديدات السيبرانية.[25]

---

[21] – لطفي , وفاء (2022). الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا, المجلد 23، العدد 1 –, جامعة 6 أكتوبر., مصر.

[22] – عادل عبدالصادق. (2021). المناعة الاسيبرانية والتنمية المستدامة في منطقة الشرق الأوسط وشمال إفريقيا. المعهد الأوروبي للبحر الأبيض المتوسط، وقعات كبيرة:تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط.

[23] – قناة المملكة (2022). "الوطني للأمن السيبراني": نعمل على نشر التوعية وبناء القدرات الوطنية, 24, اذار, الأردن.

[24] – Newman, E. (2016). Human Security: Reconciling Critical Aspirations with Political 'Realities'. British Journal of Criminology Advance Access, 56(6), 1165–1183.

[25] – لطفي , وفاء (2022). الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا, المجلد 23، العدد 1 –, جامعة 6 أكتوبر., مصر.

المبحث الثاني : المركز الوطني للأمن السيبراني الأردني (المهام والوظائف).

أنشئ المركز الوطني للأمن السيبراني بموجب قانون الأمن السيبراني رقم 16 لسنة 2019 كمؤسسة حكومية ذات أستقلال مالي وإداري معني ببناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية الفضاء السيبراني للمملكة الإردنية الهاشمية من تهديدات الفضاء السيبراني[26].

ويهدف المركز الوطني للأمن السيبراني في الأردن لتعزيز قدراته ليكون يتماشى مع أفضل المعايير الدولية لتحقيق هدفين رئيسيين: إنشاء مركز العمليات الأمنية للتكنولوجيا التشغيلية وتحويل المركز الوطني للأمن السيبراني إلى مركز وطني، والمساهمة في تحسين الأمن السيبراني في الأردن بما يتماشى مع أفضل المعايير الدولية[27].

وقد أصدر المركز الوطني للأمن السيبراني في الأردن مسودة الإطار الوطني للأمن السيبراني، بهدف حماية أنظمة المعلومات في القطاعين العام والخاص من التهديدات السيبرانية ومواكبة الممارسات الدولية ومواجهة المخاطر السيبرانية المختلفة من خلال تطوير القدرات الفنية والبشرية والإدارية في المؤسسات. ويقدم المركز للوزارات والدوائر والمؤسسات الحكومية العديد من الخدمات المتعلقة بأمن وسلامة المعلومات والشبكات لضمان سرية البيانات وتوثيقها وتوافرها عند الحاجة إليها.

ويسعى المركز إلى تدريب وتأهيل وتوعية وتثقيف موظفي القطاع العام والخاص وكافة فئات المجتمع وإكسابهم المعرفة والمهارات اللأزمة للحد من المخاطر والتهديدات وفقاً لأفضل الممارسات في مجال الأمن السيبراني وبما يضمن أعلى مستوى من الكفاءة، وجعل الأردن مركز إبداع وتميز إقليمي ودولي في هذا المجال[28].

لقد أصبح أمن المعلومات والشبكات من أهم احتياجات الوزارات والدوائر والمؤسسات الحكومية في الأردن. ولذلك فإن من المهام والوظائف المناط بها المركز الوطني للأمن السيبراني القيام بما يلي:[29]

1. تنفيذ الإجراءات والسياسات لضمان الحماية الكاملة للموارد والأنظمة والمعلومات.
2. تقييم ومراقبة تطوير أنظمة أمن وحماية المعلومات من جميع النواحي، للتأكد من الألتزام بالسياسات والمعايير المعتمدة وتقديم التوصيات لتحسين الأمن.
3. إدارة معدات حماية الشبكات والأنظمة.
4. رفع قدرات الموظفين من خلال التدريب النوعي المتخصص.
5. إجراء فحوصات دورية للأنظمة لأكتشاف نقاط الضعف.
6. تحليل سجلات الحركة والبيانات المتاحة للكشف عن التطفل ومتابعة أنماط الأنشطة التطفلية وتقييم المخاطر المحتملة.
7. إعلانات وتحذيرات توعوية، مثل تعميم تحذيرات الأقتحام والتحذيرات من نقاط الضعف.
8. معالجة الثغرات الأمنية الحالية أو المحتملة من خلال تحليلها والأستجابة لها والتثقيف بشأنها.

---

[26] – قناة المملكة (2022). للمركز الوطني للأمن السيبراني تعامل مع 544 حادثة أمن سيبراني في النصف الأول من 2022, 28, اب, الاردن.

[27] – قناة المملكة (2022). "الوطني للأمن السيبراني": نعمل على نشر التوعية وبناء القدرات الوطنية, 24, اذار, الأردن.

[28] – خضر , مجد (2016). تعريف الأمن الوطني,موقع موضوع , 23, شباط, الاردن.

[29] – المبيضين , ابراهيم (2022). التهديدات السيبرانية من أكثر الجرائم انتشارا حول العالم,صحيفة الغد, 25, تموز , الاردن.

9. معالجة الأدلة الرقمية للأمن السيبراني، بالتعاون مع الجهات المعنية.
10. إدارة ومعالجة والأستجابة ومنع حوادث تكنولوجيا المعلومات.
11. معالجة الحوادث، بما في ذلك تلقي الإخطارات والتقارير الخاصة بالحوادث، والمساهمة في عزل أنظمة المعلومات المصابة، واحتواء المخاطر من خلال تحليلها والأستجابة لها، وتقديم الدعم الفني، والتنسيق مع الجهات المعنية.
12. فحص المواقع الحكومية التي يستضيفها المركز والتي يتم إستضافتها خارج المركز بالتنسيق مع مديريات تقنية المعلومات التابعة له، ورفع تقارير التوصيات لمعالجة الثغرات الأمنية.[30]
13. الكشف المبكر عن حالات الأختراق التي قد تتعرض لها الأنظمة والمواقع الإلكترونية الحكومية وإبلاغ الجهات المعنية عند أكتشاف حوادث الأختراق لمعالجتها في أسرع وقت ممكن.
14. تقديم المشورة الفنية بشأن سلامة المواقع الإلكترونية عند تقديم أي عطاء لإنشاء أو تطوير المواقع الحكومية.

وقد شكل المركز الوطني للأمن السيبراني واحدة من المؤسسات المختصة في مواجهة تهديدات الأمن السيبراني بأعتبار إن حرب المعلومات هي تهديدات هذا العصر, وقد ساهم التطوّر التقنيَّ والاتِّصالي وأدوات التوَّاصل الرَّقمي على حاجة الدول لمواجهات هذه التقنيات لأنها من الجانب الآخر هي تحديات وتهديدات للأمن السيبراني وأن حوزتها من قبل الفئات الإرهابية ستكون تدمير حقيقي لبيانات الدول الأقتصادية والسياسية والأجتماعية, وهي في حالة طردية فكلَّما تطوَّرت أنظمة المعلومات حول العالم، كلَّما نشطت دول ومنظَّمات ومؤسَّسات وأشخاص لأختراق تلك الأنظمة[31].

والأردن شانها شأن الدول الأخرى فهو مهدد من قبل الجهات العابثه سواء كانت دول أو مؤسسات أو أفراد, وأن الأردن تعرض إلى ما نسبته (27%) من الهجمات السيبرانيَّة، أي نحو (240) هجوماً كانت من نوع الهجمات المعقَّدة, حيث برز دور المركز الوطني للأمن السيبراني ضمن أختصاصه بتتبُّع مصدر الأختراق في حال وقوعه[32].

ويعد هذا جزء من وظائف المركز الوطني للأمن السيبراني من خلال بناء منظومة فعالة لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفعالية بما يضمن سلامة الأشخاص والممتلكات والمعلومات. وقد تم التعامل مع (897) حادث سيبراني مسجل لدى المركز الوطني للأمن السيبراني خلال عام 2021. وتعد المؤسسات العسكرية والأمنية والأقتصادية والمالية، وشركات الأتصالات، وقطاع الطاقة والغاز, وشركات الكهرباء، والمؤسسات الحكومية، والسفارات الأردنية في الخارج من أبرز الجهات المستهدفة بهجمات الأمن السيبراني[33].

[30] – وكالة الانباء الاردنية (2022). ولي العهد يؤكد أهمية تطوير منظومة الأمن السيبراني, 8, ايلول , الاردن.

[31] – عبد الصادق, عادل(2012). القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني,المركز العربي لابحاث الفضاء الالكتروني , 22, تشرين اول, مصر.

[32] – المبيضين , ابراهيم (2022). التهديدات السيبرانية من أكثر الجرائم انتشارا حول العالم,صحيفة الغد, 25, تموز , الاردن.

[33] – القراله , محمد (2022). الاردن تعرض الى 897 هجمة سيرانية خلال عام 2021 , صحيفة الراي ,21, شباط, الاردن.

وفي الأردن برزت التحليلات بأن الجهات التي تقف خلف محاولات الهجمات السيبرانية هي دول ومجموعات مدعومة من دول، ومجموعات مرتبطة بالتنظيمات الإرهابية، وعصابات الجرائم السيبرانية بهدف الكسب المادي، وتوزعت الحوادث السيبرانية المسجلة عام 2021 حسب جهات التهديد: 34% منها مرتبطة بالمستخدمين، و27% كانت من دول أو مجموعات مرتبطة بدول، و26% مرتبطة بالجرائم السيبرانية، و13% مرتبطة بالتنظيمات المتطرفة أو الإرهابية[34].

لقد أعتمد الأردن أيضًا نهجًا استباقيًا للأمن السيبراني وإدارة فعالة للمخاطر الإلكترونية من أجل حماية أقتصادها وأمنها، من خلال إستراتيجية وطنية واضحة مدعومة بتشريعات شاملة للأمن السيبراني ونهج مؤسسي للحوكمة السيبرانية لمواجهة التهديد والحفاظ على قدرة الدفاع السيبراني على المدى الطويل. بالإضافة إلى بنية الأمن السيبراني المتطورة، أنشأ الأردن أيضًا مركزًا وطنيًا للأمن السيبراني في عام 2020 والذي يتطلع إلى تعزيز قدرة المملكة على التحكم في التهديدات الرقمية[35].

المبحث الثالث: دور قسم الحاسوب وتقنية المعلومات (IT) في بلدية منشية بني حسن

تعد بلدية منشية بلدية بني حسن من البلديات الرائدة في تحصين بياناتها من الأمن السيبراني, ويعود الفضل لما يتمتع به موظفي قسم الحاسوب وتقنية المعلومات في البلدية من كفاءة عالية في الخبرات والمؤهلات والقدرات الحاسوبية، حيث يعتني القسم بكافة التطبيقات والأنظمة الحديثة التي تستخدمها البلديات في سبيل تحسين أداء العمل ومسؤوليته في الحفاظ على معلومات البلدية وتحليل وإعداد البيانات المتنوعة لأقسام البلدية، من خلال ربط كافة الأقسام في أيطار نظم معلوماتية موحد وخاصة أقسام إدارة الموارد البشرية، والديوان، والإدارة المالية، وأقسام المحاسبة، والمساحة والتنظيم وكل ما يتعلق بكل مفاهيم الأتمته والأرشفة لمعلومات وبيانات بلدية منشية بني حسن.

وقد ترجمة بلدية منشية بني حسن هذه الأعمال والتقنيات من خلال ربط شامل ومتكامل للأقسام في قسم الحاسوب وتقنية المعلومات في تخزين البيانات، وقواعد البيانات. الذي يتولى مسؤوليته على كل الأجهزة الألكترونية في البلدية مثل طابعات وأنظمة الأتصال والإنترنت والوحدات التقنية المختلفة، وتسجيل الحضور والانصراف فيما يسمى بالبصمة الإلكترونية التي تضبط عمل الموظفين .[36]

لم يتوقف الأمر عند هذا الحد، ولكن يقوم قسم الحاسوب وتقنية المعلومات بوظيفة تنفيذ الخطط والأفكار الجديدة من أجل تحسين المشاركة، والتخلي عن البرامج القديمة التي أصبحت غير مجدية مثل تبني نظم الخدمات الالكترونية الحديثة لوزارة الإدارة المحلية وكل ما هو جديد من نظم إلكترونية، لذلك فأن مهام قسم تكنولوجيا المعلومات كثيرة ومتشعبة وتختلف من قسم إلى أخرى حسب طبيعة صناعتها ونوع التطبيقات والشبكات التي تحتاج إليها من أجل العمل.

وتبز مهام مسؤولية قسم الحاسوب وتقنية المعلومات في بلدية منشية بني حسن بالمهام التالية :[37]

[34] – قناة المملكة (2022). "الوطني للأمن السيبراني": نعمل على نشر التوعية وبناء القدرات الوطنية, 24, اذار , الاردن.

[35] – وكالة الانباء الاردنية (2022). ولي العهد يؤكد أهمية تطوير منظومة الأمن السيبراني, 8, ايلول , الاردن.

[36] – الموسوي، علي محمد كاظم (2019). المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان

[37] – احمد , فهمي (2023). الاختلافات بين حوكمة الأمن السيبراني وحوكمة تكنولوجيا المعلومات, موقع روت , 14, كانون ثاني , مصر.

1. الإشراف على جميع أنظمة الشبكة داخل البلدية، والمساهمة في الوضع الأساسي لتشغيل الإدارات والأقسام المختلفة.
2. قيام موظف قسم الحاسوب وتقنية المعلومات بالتفقد الدوري للأجهزة الكمبيوتر لدى الأقسام, وتقديم الحلول فيما يتعلق بأداء الأجهزة الإلكترونية.
3. توفير دعم فني مباشر وغير مباشر من أجل تصميم نظام شبكي قوي لعدم أختراق حساباته في إطار حفظ البيانات من هجمات الأمن السيبراني.
4. مشاركة قسم الحاسوب وتقنية المعلومات في وضع إستراتيجية تتضمن أساسيات عمل البلدية، وتقديم الحلول العملية لجميع الموظفين والمشاكل المتعلقة بطريقة أداء العمل.
5. القيام بمهام التخطيط والتنظيم لكل إدارات وأقسام البلدية لحفظ البيانات من هجمات الأمن السيبراني .
6. القدرة على حل المشاكل بكل دقة دون ضغط أو توتر.
7. صيانة وتفقد الأجهزة في البلدية بشكل دوري ومستمر, وبيان الحاجة والكمية الكافية لأنظمة أجهزة الكمبيوتر الإلكترونية.
8. القدرة التقنية والمعرفة الجيدة باللغة الإنجليزية ومصطلحات هذا المجال.
9. إمتلاك مهارات جيدة في كيفية حماية الشبكات والبيانات.
10. التشييك المستمر لمدى توافق الأجهزة الإلكترونية مع متطلبات العمل، وفي حالة الاجتياج الفايروسي لأي جهاز فإن القسم مستعد لحفظ البيانات من هجمات الأمن السيبراني.
11. الأهتمام بأكبر مساحة من بيانات ومعلومات الأجهزة الإلكترونية للبلدية حيث يجب أن تكون نسخة أحتياطية منها في قسم الحاسوب في حال حدث أي مشكلة في المساحات التخزينية للأجهزة في الأقسام.
12. مراقبة أداء النظام الخاص بالشبكات وأكتشاف أي مشكلة تشفير في البيانات.
13. عمل التحليلات الإحصائية المناسبة للبيانات والمعلومات لأي قسم من أقسام البلدية، للمساعدة في أتخاذ القرارات الإدارية المناسبة.

وترى الباحثة أنه يمكن لبلدية منشية بني حسن الحماية من التهديدات السيبرانية من خلال الإجراءات التالية:[38]

1. لابد من القيام بتحديث البرامج ونظام التشغيل الخاص بها: وهذا يعني إن قسم الحاسوب وتقنية المعلومات تستفيد من أحدث تصحيحات الأمان.
2. دور قسم الحاسوب وتقنية المعلومات باستخدام برامج مكافحة الفيروسات: الحلول الأمنية مثل Kaspersky Total Security والتي تكتشف التهديدات وتزيلها، والحفاظ على تحديث البرامج للحصول على أفضل مستوى من الحماية.
3. يقوم قسم الحاسوب وتقنية المعلومات باستخدام كلمات مرور قوية: يجب التأكد من عدم إمكانية تخمين كلمات المرور الخاصة بسهولة.

[38] – الشديفات, سناء احمد (2024).رئيس قسم الحاسوب والإعلام , بلدية منشية بني حسن, الأردن.

4. لا يجوز فتح مرفقات البريد الإلكتروني الواردة من مرسلين غير معروفين فمن الممكن أن يكونوا مصابين ببرامج ضارة.
5. عدم النقر على الروابط الموجودة في رسائل البريد الإلكتروني الواردة من مرسلين غير معروفين أو مواقع ويب غير مألوفة: هذه طريقة شائعة لانتشار البرامج الضارة.
6. تجنب أستخدام شبكات WiFi غير الآمنة في الأماكن العامة: الشبكات غير الآمنة تجعلك عرضة لهجمات الوسيط.
7. توعية الموظفين بطرق الحماية الأمنية للبيانات والمعلومات ومن المخاطر الالكترونية المتعددة، من خلال عمل ورشات توعية وإعلانات مستمرة وبروشورات دورية.

وترى الباحثة من خلال قسم الحاسوب وتقنية المعلومات إن لديها برامج مكافحة فايروسات لكنها تحتاج الى نسخ منها بأصدارات حديثة لعمل تحديث دوري لبرامج مكافحة الفيروسات وبرامج الأمان الأخرى، وبالتالي فإنها ستكون في مأمن من الهجمات الإلكترونية، ولكن هذا ليس هو الحال. في بعض الأحيان، يمكن للمتسللين الدخول إلى النظام عن طريق أستغلال كلمة مرور ضعيفة أو إيجاد طرق للدخول إلى نظام يفتقر إلى المصادقة متعددة العوامل – وهي طريقة مصادقة تطلب من المستخدمين تقديم أكثر من إثبات هوية لتسجيل الدخول[39].

وهنا تطرح الباحثة رئيسة قسم الحاسوب وتقنية المعلومات في بلدية منشية بني حسن بعض الإرشادات لموظفي البلدية للحماية البيانات والمعلومات من مخاطر الأمن السيبراني والأختراقات المختلفة من خلال القيام بما يلي :

1- يجب أن يفهم موظفي البلدية مدى سهولة قيام مجرمي الإنترنت بإرتكاب الهجمات وأتخاذ موقف أستباقي.
2- يجب المحافظة على تحديث البرامج والأجهزة وتطويرها بشكل دوري.
3- على قسم الحاسوب وتقنية المعلومات إنشاء سياسات عمل محددة بوضوح وإجراء تدريب على الأمن السيبراني للموظفين ورؤوساء الأقسام.
4- القيام بتنفيذ الحلول والخدمات التي يمكن أن تساعد في العثور على الهجمات الإلكترونية والرد عليها.
5- عمل ورشات توعية وبشكل دوري حول كل ما يتعلق بالأمن السيبراني، وكذلك بروشورات، وإعلانات على مواقع البلدية والصفحات الالكترونية، ومواقع التواصل الاجتماعي بمخاطر الأمن السيبراني وطرق الحفاظ على المعلومات والبيانات.
6- أعطاء الدورات التدريبة الكافية في مجال أمن المعلومات والشبكات لموظفي البلدية وخصوصاً موظفي قسم الحاسوب وتقنية المعلومات.

وترى الباحثة ومن منظور تكنولوجيا المعلومات، بأنه من الواجب على رؤساء البلديات أن يسعوا جاهدين لتوظيف المواهب والقدرات المناسبة في قسم الحاسوب وتقنية المعلومات لحماية وتطوير البانات والمعلومات قي الأقسام، ووضع تدريب وأختبار منتظم على الأمن السيبراني في الخطة التطويرية للبلدية، وربما استئجار شركات خارجية لإجراء اختبارات الأختراقات للعثور على نقاط الضعف المحتملة. ابدأ بتحديد "جواهر التاج لمؤسستك"، أي

[39] – وكالة الإنباء الأردنية (2023). المدن الذكية"و"الأمن السيبراني"يختتمان مشروع التوعية, 13, تشرين ثاني , الأردن.

معلوماتك الأكثر عرضة للخطر أو الحساسية، ثم قم بتعزيز الأمن حول ذلك. ويجب على الجميع أيضًا أن يفهموا مدى سهولة وصول مجرمي الإنترنت إلى الأنظمة والموارد وأن يكونوا في حالة تأهب في جميع الأوقات, ويجب أن يعمل موظفي قسم الحاسوب وتقنية المعلومات مع مركز الأمن السيبراني الأردني الوطني لمواكبة أحدث المشكلات الأمنية، والعمل على الأخذ بخبرات البنوك الأردنية لتنفيذ الحلول التي تحبط المتسللين، وتمرير كل تلك المعلومات إلى الموظفين في أقسام البلدية للأستفادة منها.

الخاتمة والنتائج والتوصيات

أولاً: الخاتمة

شكَّلت خاتمة الدِّراسة حصيلة النتائج التي تمثل الإجابة عن أسئلة الدِّراسة بالإضافة إلى تقديم مجموعة من التوصيات, وقد تناولت الدِّراسة الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن, وبينت الدراسة أن الفضاء الإلكتروني معرض للمخاطر الناجمة عن التهديدات والمخاطر المادية والسيبرانية. ويستغل الفاعلون السيبرانيون ضعف الدول لسرقة المعلومات والأموال وتطوير القدرات لتعطيل أو تدمير أو تهديد الخدمات الالكترونية الأساسية. وقد أكدت الدراسة على تأمين الفضاء الإلكتروني بشكل خاص بسبب الأختراقات الإلكترونية المعقدة لما يشكله من مخاطر متزايدة يمكن أن تسبب ضررًا أو تعطل في الخدمات لدى المؤسسات والبلديات في الأردن.

وبينت الدراسة أن الأمن السيبراني له أهمية كبيرة سواء في المجالات العسكرية أو المالية أو الإدارية, لذا من المهم هو حماية أمن المعلومات والبيانات لما يشكله من خطر على مؤسسات الدولة والبلديات على حد سواء, وبينت الدراسة أن إنشاء المركز الوطني للأمن السيبراني هو لحماية أمنها السيبراني من الأختراق الإلكتروني وحفظ البيانات والمعلومات والشبكات الألكترونية للمؤسسات والدوائر الحكومية والخاصة في الأردن.

وأكدت الدراسة أن بلدية منشية بني حسن من البلديات الأردنية التي تعني اهتماماً بالغاً في الحفاظ على بياناتها, حيث يشكل قسم الحاسوب وتقنية المعلومات القسم الرئيسي في الحفاظ على أمن البيانات والمعلومات في البلدية وأقسامها من خلال تأمين أنظمة الحماية المناسبة في كافة الأقسام. كما يتابع ويراقب الأقسام الأخرى من خلال أتباع الإرشادات الي يصدرها المركز الوطني للأمن السيبراني للحفاظ على أمن البيانات والمعلومات والتوعية بالمخاطر والتهديدات المحتملة على بيانات البلدية.

ثانياً : نتائج الدراسة :

1- بينت الدراسة أن الفضاء الإلكتروني معرض للمخاطر الناجمة عن التهديدات والمخاطر المادية والسيبرانية. ويستغل الفاعلون السيبرانيون ضعف الدول لسرقة المعلومات والأموال وتطوير القدرات لتعطيل أو تدمير أو تهديد الخدمات الألكترونية الأساسية.

2- أكدت الدراسة على ضرورة تأمين الفضاء الإلكتروني بشكل خاص بسبب الأختراقات الألكترونية المعقدة لما يشكله من مخاطر متزايدة يمكن أن تسبب ضررًا أو تعطل الخدمات لدى المؤسسات والبلديات في الأردن.

3- بينت الدراسة أن الأمن السيبراني له أهمية كبيرة سواء في المجالات العسكرية أو المالية أو الإدارية, لذا من المهم هو حماية أمن المعلومات, لما يشكله من خطر على مؤسسات الدولة والبلديات على حد سواء.

4- بينت الدراسة أن إنشاء المركز الوطني للأمن السيبراني، هو لحماية أمنها السيبراني من الأختراق الألكتروني وحفظ البيانات والمعلومات والشبكات الألكترونية للمؤسسات والدوائر الحكومية والخاصة في الأردن.

5- أكدت الدراسة أن بلدية منشية بني حسن من البلديات الأردنية التي تعني اهتماماً بالغاً في الحفاظ على بياناتها, حيث يشكل قسم الحاسوب وتقنية المعلومات من الأقسام التي تتابع وتراقب الأقسام الأخرى من خلال الإرشاد والصيانة الدورية للأنظمة وبيان خطورة الأمن السيبراني على بيانات البلدية .

ثالثا :التوصيات

1- أوصت الدراسة بأنه من الضروري على الحكومات الأردنية أن تعزز الأمن السيراني لأنه يرتبط باستقرار الأردن وسلامة بيانات الأمن الوطني الأردني.

2- على وزارة الإدارة المحلية أن تدرك أهمية الأمن السيبراني حيث أصبح مطلبًا أساسيًا تسعى جميع البلديات إلى تحقيقه نظرًا للمخاطر التي تنجم عنه من الأختراق والتدمير.

3- على القيادات السياسية في الأردن إدراك إن الأردن جزء من المنظومة العالمية التي ترتبط بمؤسسات العالم اقتصادياً وسياسياً وامنياً ولا بد من حماية أمنها الوطني من الأختراق الألكتروني وحفظ البيانات والمعلومات والشبكات الألكترونية.

4- من الضروري على بلدية منشية بني حسن حماية أمن المعلومات باعتبار أن اختراق المعلومات يشكل خطر على البلدية، مما يهدد أمن المعلومات والبيانات لقسم الحاسوب وتقنية المعلومات والأقسام الأخرى.

5- أوصت الباحثة بضرورة تحديث برامج مكافحة الفايروسات وأنظمة حماية المعلومات، والأهتمام بالإصدارات الحديثة لما له من أهمية في حفظ المعلومات والبيانات لقسم الحاسوب وتقنية المعلومات والأقسام الأخرى في بلدية منشية بني حسن من الأختراقات والمخاطر السيبرانية .

المراجع

اولا: المراجع العربي

ابو سليمان، محمد عبدالمنعم (2018).أهمية تكنولوجيا المعلومات والاتصالات في بناء اقتصاد المعرفة.المجلة المصرية لعلوم المعلومات,22-168 , ,مصر.

احمد , فهمي (2023). الاختلافات بين حوكمة الأمن السيبراني وحوكمة تكنولوجيا المعلومات, موقع روت , 14, كانون ثاني , مصر.

إسماعيل زروقة. (,2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع, مجلة العلوم القانونية والسياسية, مصر.

الأشقر , جبور منى(2016). السيبرانية هاجس العصر. بيروت: جامعة الدول العربية – المركز العربي

للبحوث القانونية والقضائية،لبنان..

حمد عبيس نعمة الفتلاوي وزهراء عماد محمد(2020). تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد44، العدد1، كلية القانون والعلوم السياسية –جامعة الكوفة، الكوفة، العراق.

الخزاعلة , عبير (2021). مفهوم الأمن السيبراني, موقع موضوع , 17, تشرين ثاني, الاردن.

خضر , مجد (2016). تعريف الأمن الوطني,موقع موضوع , 23, شباط, الاردن.

الدليمي، حسام جاسم محمد أحمد(2018). التطور التكنولوجي واثره في سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية القانون والعلوم السياسية– جامعة الانبار، الانبار، العراق.

رغدة ، البهي. (2018). الردع السبيراني :المفهوم والإشكاليات والمتطلبات . مجلة الدراسات الإعلامي.,مصر.

الشديفات, سناء احمد (2024).رئيس قسم الحاسوب والإعلام , بلدية منشية بني حسن, الأردن.

طلال ياسين العسي وعدي أحمد عناب(2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19، العدد الاول، جامعة الزرقاء، الاردن.

عادل عبدالصادق. (2021). المناعة الاسيبرانية والتنمية المستدامة في منطقة الشرق الأوسط وشمال إفريقيا. المعهد الأوروبي للبحر الأبيض المتوسط، وقعات كبيرة:تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط.

عبد الصادق, عادل(2012). القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني,المركز العربي لابحاث الفضاء الالكتروني , 22, تشرين اول, مصر.

العظامات، جمال(2015). جريمة العدوان في الهجمات الالكترونية في القانون الدولي العام، مجلة المنارة للدراسات القانونية والإدارية، المجلد21، العدد4، مركز المنارة للدراسات والأبحاث، المغرب.

فاطمة, بيرم(2020). السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية:الصين نموذجاً، المجلة الجزائرية للامن الانساني ، المجلد الخامس، العدد الاول ، مخبر الامن الانساني–جامعة باتنة، الجزائر.

الفتلاوي أحمد عبيس نعمة(2016). "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر". مجلة المحقق الحلي للعلوم القانونية والسياسية,

قبيلات حمدي(2017).التشريعات الناظمة لعمل مجالس المحافظات والبلدية والمحلية في الأردن، الوكالة الالمانية واللجنة الوطنية الاردنية لشؤون المراة ، الاردن.

القراله , محمد (2022). الاردن تعرض الى 897 هجمة سيرانية خلال عام 2021 , صحيفة الراي ,21, شباط, الاردن.

قناة المملكة (2022). "الوطني للأمن السيبراني": نعمل على نشر التوعية وبناء القدرات الوطنية, 24, اذار, الأردن.

قناة المملكة (2022). المركز الوطني للأمن السيبراني تعامل مع 544 حادثة أمن سيبراني في النصف الأول

من 2022, 28, اب, الاردن.

لطفي , وفاء (2022). الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا, المجلد 23، العدد 1 –, جامعة 6 أكتوبر., مصر.

المبيضين , ابراهيم (2022). التهديدات السيبرانية من أكثر الجرائم انتشارا حول العالم,صحيفة الغد, 25, تموز , الاردن.

محمود لمى عبدالباقي, و كيطان اسراء نادر(2021)"المسؤولية الدولية عن الاضرار التي تحدثها الهجمات الإلكترونية". مجلة العلوم القانونية 36 (كانون اول):336_362.مصر.

الموسوي، علي محمد كاظم (2019). المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان

وكالة الإنباء الأردنية (2023). المدن الذكية"و"الأمن السيبراني"يختتمان مشروع التوعية, 13, تشرين ثاني , الأردن.

وكالة الانباء الاردنية (2022). ولي العهد يؤكد أهمية تطوير منظومة الأمن السيبراني, 8, ايلول , الاردن.

وكالة الانباء الاردنية (2022). ولي العهد يؤكد أهمية تطوير منظومة الأمن السيبراني, 8, ايلول , الاردن.

ثانيا : المراجع الاجنبية

Lehto Martti , Neittaanmäk Pekka(2015) .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing,. Switzerland

Lehto Martti , Neittaanmäk Pekka(2015) .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing,. Switzerland.

Newman, E. (2016). Human Security: Reconciling Critical Aspirations with Political 'Realities'. British Journal of Criminology Advance Access, 56(6), 1165-1183.

Marie Baezner, Patrice Robin,(2018) Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS),.