العدد سبعة وأربعون
تاريخ الإصدار: 2 – أيلول – 2022م
www.ajsp.net
ISSN: 2663-5798

"الأمن السيبراني ودرجة وعي المؤسسات بأهميته"

إعداد الباحثة:
سارة "محمد روحي" فتحي غزال
مبرمج
بلدية معان الكبرى

العدد سبعة وأربعون
تاريخ الإصدار: 2 – أيلول – 2022م
www.ajsp.net
ISSN: 2663-5798

الملخص:

في ظل التوجه الدولي الكبير أصبحت قضية أمن المعلومات السيبراني لها تحديات كبرى على الصعيدين الاقليمي والعالمي، ومع تزايد التهديدات الأمنية الإلكترونية في الاردن وغيرها من الدول العربية وجب على كل مؤسسة حماية منظومتها المعلوماتية بوعي مؤسساتها بمفهوم الأمن السيبراني وأهميته وعناصره وضوابطه وتنفيذ أدوات الأمن السيبراني وتدريب موظفيها واساليب ادارة المخاطر وتحديث الانظمة باستمرار مع تغير التقنيات وتطورها.

المقدمة:

انتشرت في الآونة الأخيرة كلمة الأمن السيبراني، ومع سماع هذه الكلمة كثيرا من خبراء مجال أمن المعلومات يتبادر الى أذهاننا أسئلة كثيرة منها، ما هو الأمن السيبراني وهل أمن المعلومات جزء من الأمن السيبراني وما الفرق بينهما ؟ وعلى من ينطبق هذا المصطلح وما هي التهديدات التي يحمي منها الأمن السيبراني ؟ وهل تقع على المؤسسات فقط أم على المؤسسات والأفراد. وقد لوحظ ان هنالك عدة أبعاد فيما يخص الأمن والفضاء السيبراني، البعد الأول هو الاقتصادي، فينقسم اقتصاد الإنترنت إلي مجالين رئيسيين، المجال الأول يتعلق بصناعة تكنولوجيا المعلومات والاتصالات (ICT) ، ويشمل تطوير أجهزة وبرمجيات وانتاجها وخدمات أخرى، أما المجال الثاني فهو مجال التجارة الإلكترونية من خلال فتح سوق حر علي شبكة الإنترنت . أما البعد الثاني فهو يتعلق بأمن المعلومات فنجد أن العديد من الدول تقوم بتخصيص قيمة كبيرة من ميزانيتها لأجل مجابهة الهجمات السيبرانية وتحديث وتطوير أنظمة الأمان لديها. أما البعد الثالث فهو البعد الأمني، وخير مثال علي ذلك هو مركز تكامل استخبارات التهديد السيبراني (CTIIC) بالولايات المتحدة الأمريكية الذي يعمل على التنسيق بين مختلف أجهزة الأمن الأمريكية الأخرى، مثل : مكتب التحقيقات الفيدرالي، وكالة الاستخبارات المركزية، ووكالة الأمن القومي ، فارتبط ظهور الأمن السيبراني بظهور الهجمات السيبرانية والتي حدثت بسبب استحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن الماضي كأداة لمعالجة وحفظ المعلومات رقمياً (Digital)، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية (CPU)، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية. وجاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2011، لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

وتعتبر اتفاقية بودابست (2001) الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، خطوة رائدة على مستوى التعاون بين الدول، وهي الوحيدة من حيث المدى وحجم الدول المنضمة إليها، دخلت حيز التنفيذ عام 2004، وتعتبر أداة إقليمية ملزمة لمكافحة الجريمة السيبرانية، عبر تحقيق الانسجام بين القوانين الوطنية، وقد شددت على ضرورة تحسين تقنيات التحقيق والبحث، وزيادة التعاون بين الدول، ومن الأسباب التي أدت الى الهجمات السيبرانية هي: انتشار الخدمات الالكترونية، ضعف الحماية السيبرانية، استغلال الفضاء السيبراني، المكاسب الكبيرة، سهولة التخفي، توفر أدوات الاختراقات.

قد وصف (segel 2016) كيف يعمل توسع الإنترنت على إعادة بلورة الأشكال التقليدية وقواعد القوة الدولية التي تعمل على نطاق واسع للدخول في عصر جديد للجيوبوليتيك، وتاريخ هذا التطور هو محور ملف استراتيجي قام بتجميعه المعهد الدولي للدراسات الاستراتيجية بلندن والذي يعرض بالتفصيل التطور التكنولوجي وآثاره السياسية بدءا من الخمسينات.

إن العصر الرقمي الذي نعيشه يجعل من الأمن السيبراني أمرًا ضروريًا لا غنى عنه لا سيما مع ثورة البيانات في فضاء الإنترنت، وإنترنت الأشياء، و أن مدى جاهزية المؤسسات للهجمات السيبرانية والجريمة الممكنة على تقنيات الاتصالات والمعلومات والسلوكيات

العدد سبعة وأربعون
تاريخ الإصدار: 2 – أيلول – 2022م
www.ajsp.net
ISSN: 2663-5798

الضارة التي تحدث عبر الفضاء الإلكتروني والتي تتجاوز اختصاص الجيوسياسي وتكتيكات تحقيق القانون والأساليب التقليدية تقاس عن طريق التقنيات المتوفرة لديها، إضافة إلى العنصر البشري.

وبين مساد أن الاستراتيجية الوطنية للأمن السيبراني تقوم على ركائز عدة، أهمها خلق بيئة سيبرانية آمنة وصلبة، وحماية البنية التحتية للمعلومات الحيوية الوطنية، علاوة على الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها، وكذلك وضع الأطر القانونية والتنظيمية لتعزيز سلامة وحيوية الفضاء الإلكتروني.

من المهم توعية الأفراد بضرورة تحديث الأنظمة وتغيير كلمة المرور لأجهزتهم دورياً، والتأكد من الروابط قبل فتحها، وتعيين أخصائيين بالأمن السيبراني في المؤسسات، ومراقبة ورصد أي نمط تعاملات غريبة في الشبكة لحمايتها من الاختراق.

وأصدر الأردن في سبيل تعزيز أمنه السيبراني "الإستراتيجية الوطنية للأمن السيبراني"، وأنشأ مركزاً يُعنى بإدارة هذا المرفق الحيوي على المستوى الوطني. وصنّف قبالين الأمن السيبراني ضمن ما يسميه "القوة الناعمة" التي تستخدمها الدول لتحقيق أهداف عدة، فإن كثيرين يعتقدون بأن مفهومه يقتصر على حماية المراسلات والوثائق والفضاء الإلكتروني أو توفير الحماية من وسائل الاختراق وأنه مرتبط بأمن المعلومات، لكنه في حقيقة الأمر أوسع من ذلك بكثير.

فما هو الفرق بين أمن المعلومات والأمن السيبراني:

أصبح الأمن السيبراني وأمن المعلومات مفهومان هامان للغايه في مجال التكنولوجيا وأصبحا مستخدمان كثيراً هذه الايام، لكن كثير من الناس الذين يستخدمونهما يخلطون بينهما او يستخدمونهما كأنهما نفس الشيء هذا لابد من بيان الأمن السيبراني وأمن المعلومات.

- الأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا تهتم بذلك.
- أمن المعلومات يهتم بأمن المعلومات الفيزيائية "الورقية" بينما لا يهتم الأمن السيبراني بذلك.

ما هو السايبر؟

سايبر (بالإنجليزية cyber): هي مصطلح درج استخدامه لوصف الفضاء الذي يضم الشبكات المحوسبة و**شبكات الاتصال** والمعلومات وأنظمة التحكّم عن بعد. تختلف استخدامات السايبر من **دولة** لأخرى وفقا لأولويات الدول: فهناك السايبر المدني الأمني والاستخباراتي. ويتكوّن السايبر من ثلاثة مكوّنات – :**الأجهزة**(Hardware) ، البرمجيات الرقمية **(Software)** وطاقم المطوّرين والمبرمجين.

مفهوم الأمن السيبراني:

حيث اعتبرا الكاتبان (Neittaanmäki Pekka,Lehto Martti) أن الأمن السيبراني عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر على البرمجيات أوبأجهزة الحاسوب أو الشبكات وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة .

وعُرّف الأمن السيبراني أيضاً بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".

وقد قمت خلال بحثي باستخلاص مفهوم الأمن السيبراني على أنه الوسائل والادوات والتدريبات والاجراءات الأمنية المستخدمة في مواجهة القرصنة وكشف الفيروسات وحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين والحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب او الشبكات.

وما يميز الأمن السيبراني أنه ذو طابع متعدد التخصصات الاجتماعية والتقنية، له قدرة استيعابية عالية من الذاكرة أي أنه شبكة خالية من الحجم، يمتلك درجة عالية من التغيير والترابط وسرعة التفاعل.

العدد سبعة وأربعون
تاريخ الإصدار: 2 – أيلول – 2022م
www.ajsp.net
ISSN: 2663-5798

أهمية الأمن السيبراني:

تظهر أهميته في كافة المجالات من خلال توفير الحماية الفائقة وخصوصية المعلومات والبقاء على سريتها وسلامتها وتجانسها وتحقيق وفرة البيانات وجاهزيتها عند الحاجة وتقوم بحماية الاجهزة والشبكات من الاختراقات استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها باستخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني، توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.

عناصر الأمن السيبراني:

لابد من توافر مجموعة عناصر تعمل مع بعضها البعض لتحقيق الهدف من الأمن السيبراني ومن أهمها:

التقنية: تشكل التقنيه والتكنولوجيا دوراً في غاية الأهمية في حياة الأفراد والمؤسسات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات واعتمادها على جدران ووسائل الحماية التي سنتطرق الى توضيحها لاحقا واستخدام البرامج الضارة ومكافحة الفيروسات .

الأشخاص: يتوجب على كل شخص من مستخدمين البيانات والأنظمة في المؤسسات استخدام مبادئ حماية البيانات الرئيسية لتحديد كلمة مرور قوية لتفادي فتح الروابط الخارجية والمرفقات عبر البريد الالكتروني وعمل نسخ احتياطية للبيانات.

الأنشطة والعمليات: يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني، والتصدي لهجماته بكل كفاءة.

البنية التحتية للأمن السيبراني:

أضاف المجلس تعريفا جديدا على مشروع القانون وهو "البنية التحتية الحرجة" وهي مجموعة الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية أو الأصول السيبرانية والانظمة التي بعد تشغيلها المستمر ضرورة ضمان أمن الدولة واقتصادها وسلامة المجتمع. فقد تتعرض البنية التحتية لمجموعة من التهديدات التي تؤدي الى تدمير الاسطول والمعلومات، اعطينا الخدمه واطلاق المعلومات او تعديلها، التجسس على الشبكات، توجب علينا حماية البنية التحتية من خلال ضوابط أساسية للأمن السيبراني، تم جمعها وتلخيصها ضمن نقاط بحسب أهميتها.

الضوابط الاساسية للامن السيبراني في المؤسسات:

1- حوكمة الأمن السيبراني (Cybersecurity Governance).

- يجب إنشاء إدارة معنية بالأمن السيبراني في المؤسسة مستقلة عن إدارة تقنية المعلومات والاتصالات ICT/ IT ويفضل ارتباطها مباشرة برئيس المؤسسة أو من ينيبه، مع الأخذ بالاعتبار عدم تعارض المصالح.
- تضمين مسؤوليات الامن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود العاملين في الجهة لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع المؤسسة، التوعية بالأمن السيبراني (عند بداية المهنة الوظيفية وخلالها)، تطبيق متطلبات الأمن السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمن السيبراني للجهة، يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالمؤسسة.

العدد سبعة وأربعون
تاريخ الإصدار: 2 – أيلول – 2022م
www.ajsp.net
ISSN: 2663-5798

2- تعزيز الأمن السيبراني (Cybersecurity Defense).

من خلال التحقق من هوية المستخدم (User Authentication) بناءً على إدارة تسجيل المستخدم وإدارة كلمة المرور، وإدارة تصاريح وصلاحيات المستخدمين(Authorization) بناء على مبادئ التحكم بالدخول والصلاحيات ومبدأ الحاجة إلى المعرفة والاستخدام "Need-to-know and Need-to-use"، ومبدأ الحد الادنى من الصلاحيات والامتيازات " Privilege Least "، ومبدأ فصل المهام "Segregation of Duties" .

3- صمود الأمن السيبراني (Cybersecurity Resilience).

من خلال التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني، ووضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال المؤسسة (Disaster Recovery Plan)، وضع خطط التعافي من الكوارث.

4- الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity).

من خلال تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للمؤسسة بصيغة قابلة للاستخدام عند إنتهاء الخدمة، فصل البيئة الخاصة بالمؤسسة وخصوصاً الخوادم الافتراضية عن غيرها من البيئات التابعة لمؤسسات أخرى في خدمات الحوسبة السحابية.

5- الأمن السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity).

التقييد الحازم والتقسيم المادي والمنطقي عند ربط الأنظمة أو الشبكات الصناعية مع شبكات خارجية، مثل: الإنترنت أو الدخول عن بعد أو الاتصال اللاسلكي.

وهنالك ثلاثة كيانات رئيسية يجب أن تتم حمايتها في الأمن السيبراني وهي:

- أجهزة الكمبيوتر والأجهزة الذكية والراوترات.
- الشبكات.
- السحابة الالكترونية .

وتتلخص التقنيات الشائعة المستخدمة لحماية هذه الكيانات بأهم أدوات الأمن السيبراني للحماية من الهجمات الالكترونية وهي:

1- جدار الحماية Firewall

يعرف **جدار الحماية** أو ما يطلق عليه "الجدار الناري" على أنه: جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب، ويكون أداة مخصصة أو برنامج على جهاز حاسوب آخر، الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور برنامج طبقاً لقواعد معينة.

2- برامج مكافحة الفيروسات Antivirus Software

ستنبهك برامج مكافحة الفيروسات إلى الإصابة بالفيروسات والبرامج الضارة، كما سيقدم العديد منها خدمات إضافية مثل فحص رسائل البريد الإلكتروني للتأكد من خلوها من المرفقات الضارة أو روابط الويب.

3- خدمات البنية التحتية للمفاتيح العمومية (PKI Services) فماذا نعني ب (PKI)؟

البنية التحتية للمفاتيح العامة هي الترتيبات التي يتم بها ربط المفتاح العام مع المستخدم بواسطة مصدر الشهادة (Certificate Authority CA)، هوية المستخدم يجب أن تكون فريدة لكل مصدر شهادة، يتم ذلك عن طريق برمجيات خاصة في مصدر الشهادة، من الممكن ان تكون هذه البرمجيات تحت اشراف بشري، جنباً إلى جنب مع برمجيات مُنَسِقة في مواقع مختلفة ومتباعدة.

العدد سبعة وأربعون
تاريخ الإصدار: 2 – أيلول – 2022م
www.ajsp.net
ISSN: 2663-5798

يربط العديد من الأشخاص PKI فقط بـ **SSL** أو TLS، وهي التقنية التي تقوم بتشفير إتصالات الخادم والمسؤولة عن HTTPS والقفل الذي تراه في أشرطة عناوين متصفحك.

4- خدمات الكشف المُدارة

في عام 2018 لم يعد مجرد وجود دفاعات تتفاعل مع التهديدات أمرًا كافيًا –بل يجب أن تكون تلك الدفاعات استباقية وقادرة على تحديد الهجمات الالكترونية قبل أن تتسبب في حدوث مشكلات.

5- اختبار الاختراق

يحاول اختبار (**pen test**) محاكاة نوع الهجوم الذي قد تواجهه الشركة من المتسللين المجرمين، بدءًا من اختراق كلمة المرور وحقن الشفرة وحتى التصيد الاحتيالي.

6- تدريب الموظفين

قد لا تفكر في تدريب الموظفين على أنه "أداة" ولكن في النهاية، يعد وجود موظفين على دراية بمخاطر الهجمات الالكترونية، ويفهمون دورهم في الأمن السيبراني أحد أقوى أشكال الدفاع ضد الهجمات الالكترونية. هناك العديد من أدوات التدريب التي يمكنك الاستثمار فيها لتثقيف الموظفين حول أفضل ممارسات الأمن السيبراني. يمكن أن يحدث شيء بسيط فرقًا كبيرًا مثل التحديثات المنتظمة على استراتيجيات الأمن السيبراني واتباع العادات الصحيحة لاستخدام كلمات المرور، من المهم أيضًا تقديم دورات تدريبية أو عمليات محاكاة حول اكتشاف الروابط المشبوهة أو رسائل البريد الإلكتروني الاحتيالية التي قد تكون جزءًا من هجوم التصيد الاحتيالي.

يجب توفير المهارات المتخصصة والتدريب اللازم للعاملين في المجالات الوظيفية ذات العلاقة المباشرة بالأمن السيبراني في المؤسسة، وتصنيفها بما يتماشى مع مسؤولياتهم الوظيفية فيما يتعلق بالأمن السيبراني، بما في ذلك:

1- موظفو الإدارة المعنية بالأمن السيبراني.

2- الموظفون العاملون في تطوير البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للمؤسسة.

3- الوظائف التنفيذية الإشرافية.

الخاتمة:

يتم تحقيق الامن السيبراني من خلال وضع برنامج أمني متكامل يتضمن تحليل الفجوات ووضع استراتيجيات وسياسات ومعايير لأمن المعلومات والأمن السيبراني ومتابعة تطبيقها وفق الآليات المناسبة ومراجعتها بشكل دوري وعند اللزوم، واتخاذ الإجراءات اللازمة لاعتمادها، ويتم إدارة مخاطر أمن المعلومات والأمن السيبراني والتي تتضمن تحديد وتقييم المخاطر السيبرانية ذات العلاقة وبالتنسيق مع كافة الوحدات التنظيمية المعنية والجهات الخارجية وتقييم مستوى أمن المعلومات والأمن السيبراني بشكل مستمر ورفع التقارير والتوصيات بخصوصها لإدارة المؤسسة واللجان ذات العلاقة، تتقييم كفاءة وفاعلية ضوابط وإجراءات أمن البيانات والمعلومات أثناء حفظها وتخزينها ومعالجتها ونقلها وإتلافها والمطبقة ضمن بيئة المؤسسة التقنية والفيزيائية ووفقاً للسياسات الموضوعة لهذه الغاية، وتقييم كفاءة أمن البنية التحتية لتقنية المعلومات من خلال المتابعة والمراقبة لمؤشرات الأداء والأدوات المناسبة بالإضافة إلى وضع السياسات والإجراءات اللازمة لمراقبة ومراجعة سجلات الأحداث الأمنية.

المصادر والمراجع:

العمامرة، فارس والحمامصة، ابراهيم. (2022). الامن السيبراني (المفهوم وتحديات العصر), الاردن: عمان، دار الخليج للنشر والتوزيع.

أبو زيد، عبد الرحمن عاطف. (٢٠١٩). الأمن السيبراني في الوطن العربي .. دراسة حالة المملكة العربية السعودية المركز العربي للبحوث والدراسات علي الموقع بتاريخ٦/٤/٢٠٢٠:

http://www.acrseg.org/list.aspx?r=24734

الهيئة الوطنية للامن السيبراني (2018). الضوابط الاساسية للامن السيبراني.

دحماني، سليم. (2018). أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة – أنموذجا – (2001–2017)، رسالة ماجستير غير منشورة، جامعة محمد بو ضياف المسيلة.

المهتدي، سوسن. (2022). الامن السيبراني في المدن الذكية، الاردن، عمان.

سمير، بارة. (2017). الأمن السيبراني (Cyper Security) في الجزائر: السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني. العدد الرابع، ط2، ص255–280.

المراجع الاجنبية:

Lehto, M., & Neittaanmaki, P. (Eds.). (2015). Cyber security: Analytics, technology and automation (Vol. 78, p. 258). London: Springer.

Craigen, D., Diakun-Thibault, N., & Purse, R.(2014). Defining Cybersecurity.Technology Innovation Management Review, 4(20): pp 13-21.

Oxford University Press.(2014) .Oxford Online Dictionary. Oxford: OxfordUniversity Press.October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity.

Singer, P. W., & Friedman, A. (2013) .Cybersecurity and Cyberwar: What Everyone Needs to Know.New York: Oxford University Press.

Hoscheidt, M., Eichner, E. (2014) LEGAL AND POLITICAL MEASURES TO ADDRESS CYBERCRIME, United Nations: UFRGSMUN UFRGS Model, v.2, p 446.

Hannes, E., Tim, M . (2017). " Cyber Security" oxford bibliographies , LAST MODIFIED.

الخميس 18 يونيو 2020، استرجع في 15 حزيران،2022 من

https://www.independentarabia.com/node/127951

انسايكلوبيديا، استرجع في 16 حزيران، 2022 https://political-encyclopedia.org/dictionary

أهم أدوات الأمن السيبراني للحماية من الهجمات الالكترونية استرجع في 20 حزيران من

https://www.rmg-sa.com

Summary:

In light of the tremendous international trend, the issue of cyber information security has become a significant challenge at the regional and global levels. With the increase in electronic security threats in Jordan and other Arab countries, every institution must protect its information system with the awareness of its institutions of the concept of cybersecurity and its importance, elements and controls, implement cybersecurity tools and train its employee's risk management methods and systems constantly update as technologies' change and evolve.