المركز الوطني
للأمن السيبراني
National Cyber
Security Center

النظام البيئي
للأمن السيبراني

Cybersecurity Ecosystem

المقدمة

- انطلاقا من اهمية استحداث واعتماد "البيئة السيبرانية الصحية"، حيث تتكامل مكونات النظام السيبراني من أجهزة وتقنيات في الوقت الحقيقي في تكوين نظم دفاعية ضد الهجمات السيبرانية.

- وتتمتع هذه الأجهزة بقدرات ذاتية تمكّنها من العمل سويًا للتنبؤ بالهجمات السيبرانية ومنعها، وتقليل انتشار الهجمات عبر الأجهزة المكونة للنظام السيبراني، والحد من الآثار الناجمة عن الهجمات، واستعادة عمل النظام بأسرع وقت.

- وتتميز النظم البيئية الرقمية اليوم بأنها سريعة التطور ولديها قابلية الانتشار والتوسع؛ فهي تنمو وتتطور مع تطور التكنولوجيا، وترتكز النظم البيئية السيبرانية الصحية على **ثلاث ركائز اساسية وهي:**

الاتمتـــة (Interoperability)

التوافقية (Interoperability)

المصادقة (Authentication)

المقدمة

- ولفهم أوضح حول النظم البيئية السيبرانية لا بد من تسليط الضوء على الهجمات السيبرانية التي باتت تأخذ شكلاً أكثر تعقيداً وتطورا، ومن خصائصها سرعة الانتشار والتجدد والقدرة على التأثير، مما يؤثر سلبا على توافر الانظمة وفعاليتها وكفاءتها، هذا من ناحية، ومن ناحية اخرى تعمل الحكومات والدول على تعزيز قدراتها السيبرانية لما له من أثر إيجابي على النمو والازدهار الاقتصادي وللحفاظ على أمنها القومي والوطني.

- لذلك تولي الدول اهتماما في تعزيز صمود البنى التحتية الحرجة والقطاعات الحيوية، مثل القطاع الصحي والمالي، والنقل، والقطاعات الدفاعية، والعسكرية. ومن هنا نلاحظ أهمية أن تعتمد الإجراءات الاحترازية المتخذة من الحكومات نهجاً دقيقاً ومحكماً بعيداً عن العشوائية وبالتشارك مع مكونات النظام البيئي السيبراني الوطني بتوقيت زمني لحظي ومتزامن للصمود في وجه التهديدات السيبرانية المعتمدة على نهج متسلسل بدءاً من الاستطلاع (Reconnaissance) ووصولا الى التمكن من الدخول الى الانظمة (Gaining Entry) وتأسيس نقطة وصول مستدامة (Establishing Persistence) وتنفيذ عمليات الهجوم. [1]

المقدمة

- ومن هنا تظهر اهمية التوافقية اللحظية في وقت شبه حقيقي (Time - Real) بين مكونات النظام السيبراني، في تبادل المعلومات الاستخبارية عن التهديدات السيبرانية والتي تتيح امكانية التنسيق في اعتماد آليات التصدي ذات الكفاءة العالية.

- ومثل النظم البيئية الطبيعية، يتألف النظام البيئي السيبراني من مجموعة متنوعة من المشاركين المتنوعين - الشركات الخاصة، والمنظمات غير الربحية، والحكومات، والأفراد، والعمليات، والأجهزة السيبرانية (أجهزة الحاسوب، والبرمجيات، وتكنولوجيات الاتصالات) - التي تتفاعل لأغراض متعددة. [2]

- ومن خلال مسودة الإطار الوطني الأردني للأمن السيبراني التي أطلقها المركز، تحدث حول أهمية النظام البيئي السيبراني ودعا الى حماية المؤسسات ومساعدة الآخرين على حماية أنفسهم وذلك لحماية النظام البيئي الأوسع التي تعمل به مؤسساتنا.

تعريف النظام البيئي للأمن السيبراني

- النظام البيئي للأمن السيبراني هو شبكة من المكونات التي تعمل على تقديم واتاحة منتجات وخدمات الأمن السيبراني وأمن المعلومات، وتشمل بائعي أجهزة وبرامج أمن المعلومات، والاستشاريين، وخبراء الأدلة الرقمية، ووكالات المقاييس، ومرافق الاعتماد والتعليم، والمؤتمرات والمجلات الأكاديمية، والكتب، والمجلات، والمتسللين، وأدواتهم. [3]

ركائز النظام البيئي السيبراني الصحي والأمن

1- الأتمتة (Automation)

تتيح الاتمتة امكانية الاستجابة بسرعة متوافقة مع سرعة الهجوم، بدلا من اعتماد الاستجابة اسنادا الى العنصر البشري التي قد تأخذ وقتا، كما وتتيح امكانية استخدام الوسائل الدفاعية المستجدة والحديثة والتي قد تكون غير معروفة للعنصر البشري بعد. [4.1]

ركائز النظام البيئي السيبراني الصحي والأمن

2- التوافقية (Interoperability)

تتيح التوافقية بين الانظمة المختلفة امكانية الدفاع المشترك وبشكل سلس وبعيدا عن القيود التقنية، واتاحة امكانية تبادل المعلومات وتكوين صورة موحدة ومشتركة عن الوضع الراهن في النظام البيئي السيبراني. [4.2]

إن العمل المستقل للأجهزة ومكونات النظام البيئي مثل الجدران النارية (Firewalls)، وأنظمة مكافحة التسلل (Intrusion Detection Systems)، وأنظمة مكافحة البرمجيات الضارة (Anti-Malware Software) واعتماد سياسات منفصلة وغير متوافقة لا سيما ان هذه الانظمة تم تطويرها من قِبل موردين مختلفين، قد يؤثر سلبا على صمود ومرونة النظام البيئي السيبراني، ولتجنب هذه السلبيات لا بد أن تتعامل هذه الانظمة مع بعضها البعض استنادا الى سياسات موحدة والتزامٱ بالمعايير العالمية المعتمدة بعيدٱ عن القيود التقنية لكل نظام على حدة.

ركائز النظام البيئي السيبراني الصحي والأمن

3- المصادقة (Authentication)

ان تنوع مكونات النظام البيئي السيبراني من افراد وأجهزة وانظمة وتشاركهم في ادارة واستخدام المصادر المتاحة قد يسوق الى الاذهان طرح السؤال التالي "من المسؤول عن ماذا" أي تحديد صلاحيات هذه المكونات والية تعاملها مع المصادر المختلفة، ومن هنا تبرز اهمية المصادقة في تحديد صلاحيات المستخدمين من انظمة وأفراد وضمان التحقق من هوية المستخدم وأنهم مسؤولون عن العمليات التي تم تنفيذها من قِبلهم. [4.3]

وهناك العديد من طرق المصادقة المعتمدة ومنها:

- شيء تعرفه (something you know) : كلمة سر
- شيء تملكه (something you know) : بطاقة دخول
- شيء هو أنت (something you know) : بصمة الاصبع أو بصمة العين

خصائص النظام البيئي السيبراني الصحي [4.4]

1- المعلومات متصلة عبر الزمان والمكان:

يتم نقل المعلومات داخل النظام البيئي بسرعة بين الآخرين، ويساعد الاحتفاظ بالمعلومات على اكتشاف الأنماط مع الوقت ويمكن استخدام الأنماط في اكتشاف المعلومات والبيانات الحساسة وحمايتها.

2- التعلم السريع وبشكل عالمي:

تتعلم الآلات من بعضها البعض ويتعلم الناس من الآلات.

3- اعتمادية أكبر:

تعمل الآلات والبشر معا لتحسين الإسناد عند الحاجة مع تعزيز الخصوصية.

4- تحليلات جديدة:

يتم دمج البيانات من مصادر متعددة ومنفصلة أو تجميعها أو تحويلها بطريقة أخرى لإنشاء معلومات استخباراتية جديدة.

خصائص النظام البيئي السيبراني الصحي

5- وصول أكبر للشبكة:

يتم فصل محتوى الأمان عن آليات التسليم وإدارته كأحد أصول النظام البيئي.

6- تكتيكات دفاعية جديدة:

تتيح السياسات الأمنية المشتركة والمعلومات الاستخبارية الجديدة بحيث الهجمات تعمل مرة واحدة فقط (أي ضحية واحدة أو جهاز واحد) إن وجدت.

7- تغذية راجعة لدورة حياة الأمن البيئي:

تعمل ردود الفعل الغنية من العمليات إلى الواجهة الأمامية للنظام والتكنولوجيا على تقليل التكاليف، وتقصير دورات الاعتماد، وتحسين صحة النظام البيئي.

8- الشمولية:

يملك قدرات شاملة مدمجة في شبكة ويب دائمة الاتساع تمتد إلى ما هو أبعد من المفاهيم التقليدية للإنترنت العام أو تكنولوجيا المعلومات والخدمات.

خصائص النظام البيئي السيبراني الصحي

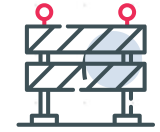
9- الفاعلية:

القدرة على الدفاع ضد جميع أنواع التهديدات السيبرانية.

10- يتسم بالذكاء:

القدرة على استشعار البيئة والتعرف على الأنماط ومشاركة المعلومات في الوقت الفعلي تقريبًا عبر القطاعات والمجتمعات على المستويين البشري والآلي.

11- خالي من عوائق السياسات:



وجود خيارات أمنية يتم تجسيدها في سياسات رقمية قابلة للتكوين بدلًا من أن تكون "مثبتة" في تصميمات الشبكة أو النظام أو تفرضها قيود التكنولوجيا أو أوجه القصور فيها.

12- المطور/المحسن:

تخصيص القدرات وصنع القرار بين البشر والآلات من أجل الاستفادة بشكل أفضل من نقاط القوة وأوقات الدورات لكل منهما، بما يتوافق مع الحفاظ على خفة الحركة.

خصائص النظام البيئي السيبراني الصحي

13- الفهم والوضوح:

يعبر عن الأمن من خلال مصطلحات المستخدم أو أصحاب المصلحة بدلاً من "المصطلحات" الأمنية المتخصصة والاعتراف بأن الجميع أصحاب مصلحة في الأمن السيبراني.

14- الموثوقية والضمان:

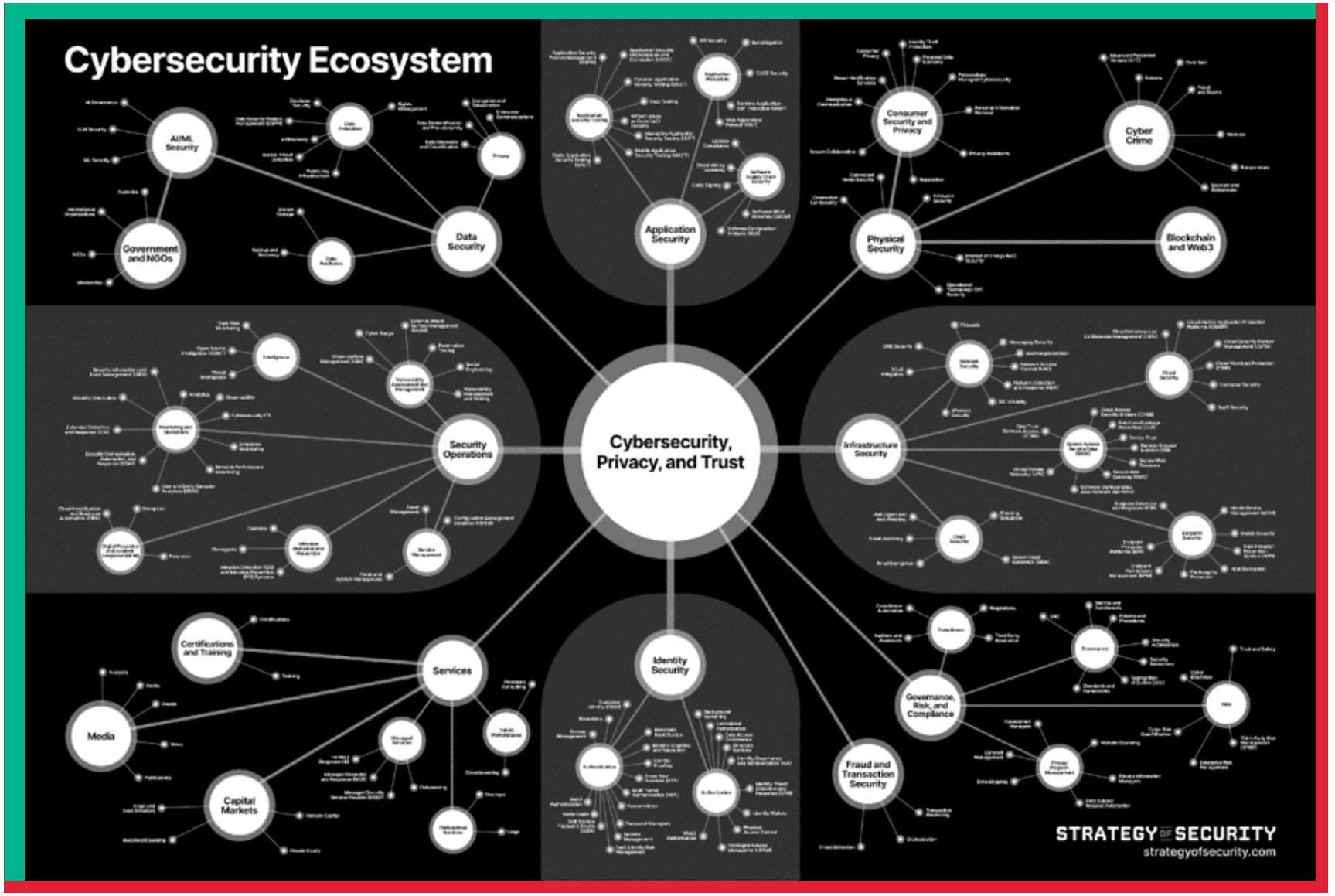
قادرة على الحفاظ على ثقة المستهلك مع مرور الوقت.

15- صالح للاستخدام:

يتمتع بخصائص التجميع والتكوين والتشغيل والأداء التي تتسم بالبساطة والفعالية، بدلاً من كونها معقدة للغاية وعرضة للخطأ.

مكونات النظام البيئي للأمن السيبراني

- **الأجهزة والبرامج:** يتضمن ذلك الخوادم وأجهزة الحاسوب وأجهزة الهواتف المحمولة والشبكات والبرامج الموجودة عليها.[5]
- **أدوات الأمان:** وهي أجهزة وبرامج تحمي هذه الأجهزة، مثل: جدران الحماية، وبرامج مكافحة الفيروسات، و أنظمة كشف التسلل ومنعها، وأدوات التشفير. [5]
- **القواعد والإجراءات:** إرشادات لإدارة الأمن السيبراني والحفاظ عليه في المؤسسات، ويشمل: صلاحيات الوصول، وكلمات المرور، والاستجابة للحوادث والتهديدات، والنسخ الاحتياطي للبيانات واستعادتها. [5]
- **الأشخاص:** كل من يستخدم الأجهزة، وهم: متخصصو تكنولوجيا المعلومات، ومتخصصو الأمن السيبراني، والمستخدمين. [5]
- **المعايير:** النظم والمبادئ التوجيهية التي تحدد معايير ممارسات الأمن السيبراني، مثل: مسودة الإطار الوطني الأردني للأمن السيبراني، وNIST، وGDPR.[5]
- **التهديدات:** جمع المعلومات وتحليلها ومشاركتها حول التهديدات القائمة والمحتملة. [5]
- **الشركاء:** الجهات والأطراف الخارجية التي توفر حلول أو خدمات أو مكونات مختلفة متكاملة مع النظام البيئي للأمن السيبراني. [5]



يوضح الشكل مكونات النظام البيئي للأمن السيبراني

التهديدات و التحديات

التهديدات:[6]

1. هجمات البرامج الضارة، وهي: Viruses، Worms، Trojan horses، Ransomware، Spyware.
2. هجمات الهندسة الاجتماعية.
3. هجمات التصيد الاحتيالي وتشمل: Standard phishing، Spear phishing، Whaling، SMS phishing.
4. هجمات اعتراض تبادل البيانات مثل: Man-in-the-middle attacks (MitM)
5. هجمات حرمان الخدمة: Denial-of-service (DoS) & Distributed denial-of-service (DDoS)
6. هجمات الحقن للغات الاستعلام الهيكلية: (SQL Injection)
7. هجمات "يوم الصفر": Zero-day

التهديدات و التحديات

التهديدات:[6]

8. هجمات البرمجة النصية لمواقع الويب: (Cross-site scripting (XSS) and cross-site request forgery).
9. هجمات التجسس والتنصت: (Eavesdropping)
10. هجمات كشف/ كسر كلمات المرور: (cracking password) وهي: Brute force attack، Dictionary attack، Rainbow table attack.
11. هجمات تعبئة بيانات الاعتماد: (Credential stuffing)

التهديدات و التحديات

التحديات:[7]

1. الذكاء الاصطناعي وتعلم الآلة (Artificial Intelligence (AI) and Machine Learning (ML)).
2. إنترنت الأشياء (IoT).
3. الحوسبة الكمومية (Quantum Computing)
4. التحديات القانونية والأخلاقية (Legal and Ethical Challenges)
5. التهديدات السيبرانية للصحة الرقمية (Threats to Digital Health)
6. هجمات التحكم في الطائرات المسيرة (Drone control attacks)

مكافحة التهديدات والاستجابة لها

تقنيات الكشف والاستجابة: [7], [8]

1. الاستخبارات المعلوماتي للتهديدات (Threat intelligence)
2. جدران الحماية (Firewalls)
3. برامج مكافحة البرمجيات الخبيثة (Anti-malware / Anti-virus software)
4. برامج اكتشاف الأجهزة الطرفية والاستجابة لها (Endpoint detection and response (EDR) systems)
5. أنظمة كشف التسلل (Intrusion detection systems - IDS)
6. أنظمة منع التسلل (Intrusion prevention systems - IPS)
7. تقنيات التشفير (Encryption Technologies)
8. إدارة الهويات والوصول (Identity and Access Management - IAM)
9. التحليل السلوكي (Behavioral Analysis)

مكافحة التهديدات و الاستجابة لها

خطط الطوارئ والاستعداد:

1. خطة الاستجابة للحوادث (Incident Response Plan)[7]

- تحديد إجراءات الاستجابة التفصيلية.
- تحديد الأدوار والمسؤوليات
- انشاء قنوات اتصال فعالة وشاملة
- الامتثال القانوني والتنظيمي
- وضع مقاييس فعالة لتحديد فاعلية الخطة
- تحليل الأثر على الأعمال
- التحسين والتطوير المستمر

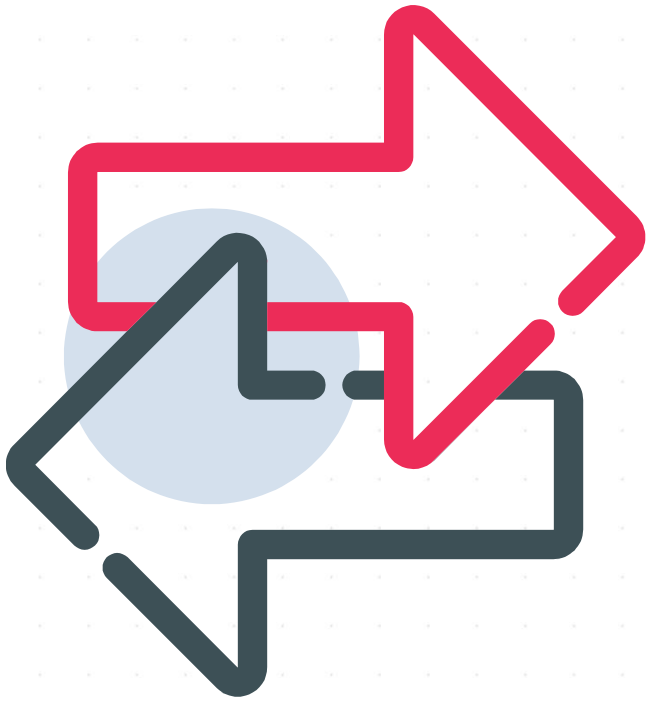
مكافحة التهديدات و الاستجابة لها

خطط الطوارئ والاستعداد:

2. خطة التعافي من الحوادث (Disaster Recovery Plan)[8]

- تحديد الأدوار والمسؤوليات
- تحديد وتوثيق التهديدات المحتملة
- تحديد وتوثيق البيانات، والتقنيات، والأجهزة، والأدوات المهمة والحرجة
- تحديد وتوثيق جميع الأجزاء المادية
- تحديد مكان وكيفية عمل نسخة احتياطية من المعلومات التجارية المهمة
- انشاء قنوات اتصال فعالة
- التدريب والتعليم للتعافي من الحوادث

التعاون وتبادل المعلومات



- أن الحلقة الأضعف غالبًا ما تكون هي التي تسبب خرق البيانات او الهجوم السيبراني، ويمكن أن يشمل ذلك البائعين، والموردين الخارجيين، والعملاء، او الموظفين، لذلك من الضروري أن تتخذ المؤسسات نهجًا استباقيًا تجاه الأمن السيبراني والتركيز على حماية أصولها وذلك يتضمن (تثقيف الموظفين والعملاء حول التهديدات وتحقيق أفضل الممارسات للبقاء آمنين عبر الإنترنت)

- ومساعدة الآخرين على حماية أنفسهم وذلك من خلال (مشاركة المعلومات حول التهديدات ونقاط الضعف عبر التواصل المنتظم مع المنظمات والمؤسسات والموردين والشركاء والمشاركة في مبادرات تبادل المعلومات)، وذلك يمكن للمؤسسات أن تساعد بعضها البعض في تحديد المخاطر والتخفيف من حدتها.

- ومن وسائل مساعدة الآخرين ايضًا، توفير التدريب والتعليم حول أفضل ممارسات الأمن السيبراني وذلك لمساعدة الموظفين على فهم المخاطر واتخاذ الخطوات اللازمة لحماية أنفسهم، أننا من خلال المساعدة في ضمان أمن شركائنا وموردينا، فإننا لا نحميهم فحسب، بل نخلق أيضًا بيئة آمنة لأعمالنا أيضًا.

التعاون وتبادل المعلومات

- تلعب المدارس والجامعات أيضًا دورًا مهمًا في رفع مستوى الوعي حول الأمن السيبراني بين عامة السكان. يتضمن ذلك تثقيف الطلاب والموظفين وأعضاء هيئة التدريس حول المخاطر والتهديدات التي قد تواجههم عبر الإنترنت وكيفية حماية أنفسهم. ويمكن القيام بذلك من خلال ورش العمل والندوات والموارد التعليمية الأخرى.

- علاوة على ذلك، من أجل بناء نظام بيئي مستدام للأمن السيبراني، هناك حاجة لتشجيع التعاون وتبادل المعلومات بين المؤسسات الأكاديمية والقطاع الخاص والمنظمات الحكومية. وهذا يسمح بتبادل المعرفة والموارد، ويمكّن من تطوير حلول جديدة لتحديات الأمن السيبراني الناشئة.

الملخص

- تعتبر النظم البيئية السيبرانية من التحديات المتزايدة في عصر التكنولوجيا، حيث تتشكل هذه النظم من مجموعة متنوعة من المشاركين مثل الشركات والحكومات والأفراد والأجهزة السيبرانية. يهدف هذا النظام إلى بناء بيئة مستدامة للأمن السيبراني وحماية المعلومات.
- تتألف مكونات النظام البيئي للأمن السيبراني من الأجهزة والبرامج وأدوات الأمان والقواعد والإجراءات والأشخاص، والمعايير، والتهديدات، والشركاء. وتواجه هذه النظم تحديات متنوعة مثل هجمات البرمجيات الضارة والهندسة الاجتماعية والتحديات التكنولوجية مثل الذكاء الاصطناعي وإنترنت الأشياء.
- في مواجهة التهديدات، يتطلب الأمر استخدام تقنيات الكشف والاستجابة مثل الاستخبارات التهديدات وبرامج مكافحة الفيروسات، بالإضافة إلى وجود خطط للاستجابة للحوادث والتعافي منها. يتعين أيضا على المؤسسات التعاون وتبادل المعلومات لتعزيز أمنها وأمان الشركاء.
- يبرز دور التثقيف والتدريب للموظفين والعملاء في تعزيز الأمان السيبراني، ويشير الى ضرورة التعاون بين المؤسسات والمؤسسات التعليمية لرفع مستوى الوعي حول التهديدات السيبرانية. بشكل عام، يتعين على الجميع المشاركة في بناء بيئة آمنة ومستدامة للأمان السيبراني.

المراجع

- Enabling Distributed Security in Cyberspace, Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action
https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf
- “Enabling Distributed Security in Cyberspace – Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action” U.S. Department of Homeland Security, 2011
- An Integrative Framework for the Study of Information Security Management Research. John D’Arcy (University of Notre Dame, USA) and Anat Hovav (Korea University, Korea)
- https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf
4.1: page 8,
4.2: page 11,
4.3: page 17,
4.4: page 22-24
- https://nordvpn.com/cybersecurity/glossary/cybersecurity-ecosystem
- https://nordvpn.com/blog/what-is-a-cyber-attack/
- Aljazera Co.
- https://www.splunk.com/en_us/blog/learn/threat-hunting-vs-threat-detecting.html
- https://reciprocity.com/blog/incident-response-plan-vs-disaster-recovery-plan/
- https://www.crashplan.com/resources/guide/cybersecurity-disaster-recovery-planning/