تأثير الأمن السيبراني على الأمن القومي

إعداد

د/ أحمد الشوري

أكاديمية ناصر العسكرية

د/ إبراهيم بدوي جابر

ملخص البحث:

في ظل التطور التكنولوجي الهائل الذي يشهده العالم في العصر الحالي، أصبحت تقنية المعلومات جزءًا لا يتجزأ من حياتنا اليومية، سواء على المستوى الفردي أو المؤسسي أو الوطني. ومع ازدياد الاعتماد على الفضاء السيبراني، تنامت المخاطر الأمنية المرتبطة به، مما جعل الأمن السيبراني قضية ذات أولوية كبرى على المستوى العالمي. إن تأثير الأمن السيبراني يتجاوز الجوانب التقنية ليشمل أبعادًا استراتيجية وسياسية واقتصادية، حيث أصبح تهديدًا مباشرًا للأمن القومي للدول.

الكلمات المفتاحية: الأمن السيبراني، الأمن القومي.

مقدمة:

أصبحت تقنية المعلومات جزءًا لا يتجزأ من حياتنا اليومية، سواء على المستوى الفردي أو المؤسسي أو الوطني. ومع ازدياد الاعتماد على الفضاء السيبراني، تنامت المخاطر الأمنية المرتبطة به، مما جعل الأمن السيبراني قضية ذات أولوية كبرى على المستوى العالمي. إن تأثير الأمن السيبراني يتجاوز الجوانب التقنية ليشمل أبعادًا استراتيجية وسياسية واقتصادية، حيث أصبح تهديدًا مباشرًا للأمن القومي للدول.

المشكلة البحثية

مع تزايد الاعتماد على التكنولوجيا في مختلف قطاعات الدولة، أصبحت البنية التحتية الحيوية، مثل الكهرباء والمياه والاتصالات والدفاع، معرضة لهجمات سيبرانية تهدد استقرارها وسلامتها. ومن هنا تبرز المشكلة البحثية: **ما هو تأثير الأمن السيبراني على الأمن القومي للدول؟** هذه المشكلة تتطلب دراسة معمقة لفهم العلاقة بين الأمن السيبراني والأمن القومي، وتحديد التحديات والتهديدات التي تواجه الدول، وكذلك استكشاف الحلول والسياسات المناسبة لتعزيز الأمن القومي في ظل التحديات السيبرانية.

السؤال البحثي

- ✓ كيف يؤثر الأمن السيبراني على الأمن القومي؟
- ✓ ما هي الاستراتيجيات والسياسات التي يمكن اتباعها لتعزيز الأمن القومي من خلال تحسين الأمن السيبراني؟
- ✓ ما هي التحديات الرئيسية التي تواجه الأمن السيبراني في حماية الأمن القومي؟

أهمية البحث

تبرز أهمية هذا البحث من خلال النقاط التالية:

١. الإسهام في فهم العلاقة بين الأمن السيبراني والأمن القومي.

٢. تسليط الضوء على المخاطر السيبرانية التي تهدد الدول والبنية التحتية الحيوية.

٣. تقديم توصيات لتعزيز السياسات الوطنية في مجال الأمن السيبراني.

٤. دعم صناع القرار ببيانات علمية تساعدهم في وضع استراتيجيات فعالة لحماية الأمن القومي.

أهداف الدراسة

١. تحليل تأثير الهجمات السيبرانية على استقرار الأمن القومي.

٢. استكشاف الأبعاد المختلفة للأمن السيبراني وأثرها على القطاعات الحيوية.

٣. تقييم الاستراتيجيات الحالية للدول في مجال الأمن السيبراني.

٤. اقتراح سياسات وتوصيات لتعزيز الأمن السيبراني كجزء من الأمن القومي.

فروض الدراسة

الفرض الرئيسي

- هناك علاقة طردية بين تعزيز الأمن السيبراني واستقرار الأمن القومي.

الفروض الفرعية

١. أبرز التهديدات السيبرانية التي تواجه الدول الكبرى في الوقت الراهن والمحتملة خلال ٢٠ عامًا قادمًا.

٢. ضعف الأمن السيبراني يزيد من احتمالية تعرض البنية التحتية الحيوية لهجمات سيبرانية تؤثر على الأمن القومي.

٣. تطبيق استراتيجيات وسياسات شاملة للأمن السيبراني يقلل من التهديدات الموجهة للأمن القومي.

٤. الدول التي تستثمر بشكل كافٍ في مجال الأمن السيبراني تكون أقل عرضة للتأثيرات السلبية للهجمات السيبرانية.

مفاهيم الدراسة

الأمن القومي

يشير الأمن القومي إلى قدرة الدولة على حماية سيادتها واستقرارها من التهديدات الداخلية والخارجية، بما يشمل الجوانب العسكرية، الاقتصادية، السياسية، والاجتماعية.

الأمن السيبراني

الأمن السيبراني هو مجموعة من التدابير والإجراءات التقنية والتنظيمية التي تهدف إلى حماية الأنظمة والشبكات والمعلومات الرقمية من التهديدات والهجمات الإلكترونية.

التهديدات السيبرانية

تشمل التهديدات السيبرانية الأنشطة الخبيثة التي تستهدف الأنظمة والشبكات والبنية التحتية الحيوية، مثل البرمجيات الضارة، الهجمات الموجهة، والهجمات على البيانات.

البنية التحتية الحيوية

تشير البنية التحتية الحيوية إلى الأنظمة والمرافق الأساسية التي تعتمد عليها الدول لضمان استمرارية الحياة والخدمات، مثل الطاقة، المياه، النقل، والاتصالات.

WormGPT وFraudGPT

هما أدوات مدعومة بالذكاء الاصطناعي تمثلان الجانب المظلم من تطبيقات الذكاء الاصطناعي، حيث تستخدمان في تسهيل الأنشطة الإجرامية عبر الإنترنت. فيما يلي ملخص حول كل منهما:

WormGPT

التعريف: تم اكتشافWormGPT في يوليو ٢٠٢٣، وهو نموذج ذكاء اصطناعي يستخدم تقنيات معالجة اللغة الطبيعية (NLP) لإنشاء محتوى ضار مثل رسائل التصيد الاحتيالي.

الوظائف: يمكن لـ WormGPT كتابة رسائل إلكترونية مزيفة، وإنشاء محتوى يهدف إلى خداع المستخدمين للنقر على روابط ضارة أو تحميل ملفات مصابة. كما يمكنه تحديد الثغرات في الشبكات واستغلالها لنشر البرمجيات الضارة.

سهولة الاستخدام: تم تصميم هذه الأداة لتكون سهلة الاستخدام حتى للمهاجمين ذوي المهارات المحدودة، مما يزيد من انتشارها بين مجرمي الإنترنت.

FraudGPT

التعريف: ظهر FraudGPT كبديل لويرمGPT، ويُباع على الويب المظلم وتطبيقات مثل .Telegram يبدأ اشتراكه من ٢٠٠ دولار شهريًا ويصل إلى ١٧٠٠ دولار سنويًا.

الوظائف: يقوم **FraudGPT** بإنشاء محتوى يساعد في تنفيذ الهجمات الإلكترونية، مثل رسائل البريد الإلكتروني الاحتيالية وصفحات الويب المزيفة. يمكنه أيضًا إنشاء هويات مزيفة والتلاعب بالمعاملات المالية.

التقنيات المتقدمة: يستخدم **FraudGPT** خوارزميات ذكاء اصطناعي متقدمة لتوليد رسائل مقنعة، مما يسهل على المهاجمين تنفيذ عمليات الاحتيال المالي وسرقة الهوية.

استخدامات مشتركة

** -إنشاء المحتوى الضار**: كلا الأداة تمكن المهاجمين من إنتاج محتوى ضار بشكل آلي، مما يسمح لهم بتوسيع نطاق عملياتهم الإجرامية بسهولة.

** -تجنب الكشف**: يمكن لكل من WormGPT و FraudGPTتعديل استراتيجياتهما في الوقت الحقيقي لتجاوز تدابير الأمان التقليدية، مما يزيد من معدل نجاح الهجمات.

تظهر هذه الأدوات كيف يمكن أن يُستغل الذكاء الاصطناعي في الأنشطة الإجرامية، مما يستدعي الحاجة إلى تعزيز الأمن السيبراني لمواجهة هذه التهديدات المتزايدة.

Citations:
[1] Certera – Modern and Affordable Website Security Services Provider
https://certera.com/blog/wormgpt-fraudgpt-the-dark-side-of-generative-ai/
[2] https://secureops.com/blog/ai-attacks-fraudgpt/
[3] https://abnormalsecurity.com/blog/what-happened-to-wormgpt-cybercriminal-tools
[4] https://arxiv.org/abs/2310.05595
[5]https://www.researchgate.net/publication/374536568_Decoding_the_Threat_Landscape_ChatGPT_FraudGPT_and_WormGPT_in_Social_Engineering_Attacks

الدراسات السابقة

في مجال الأمن السيبراني مجموعة متنوعة من المواضيع التي تعكس أهمية هذا المجال في مواجهة التهديدات الإلكترونية المتزايدة. فيما يلي تلخيص لأهم هذه الدراسات:

تطور التهديدات السيبرانية

تتناول الأبحاث تطور **التهديدات السيبرانية** وأساليب الحماية الرقمية، حيث تركز على كيفية تطور أساليب الاختراق والهجمات المتقدمة، بالإضافة إلى تحليل الجرائم السيبرانية ووسائل التصدي لها.

استراتيجيات الحماية

تشمل الدراسات أيضًا **استراتيجيات الحماية** الحالية، حيث يتم تقييم فعالية التقنيات المستخدمة وتطوير استراتيجيات جديدة لمواجهة التهديدات. كما تركز بعض الأبحاث على **تقنيات اختبار الاختراق** لتقييم قوة الأنظمة وتحديد الثغرات الأمنية.

تأثير الأمن السيبراني على العلاقات الدولية

أحد الأبحاث البارزة يدرس تأثير **التهديدات السيبرانية على العلاقات الأمريكية الروسية**، حيث يستعرض كيف تؤثر هذه التهديدات على الأمن القومي والتنافس الدولي.

تشير النتائج إلى أن الفضاء السيبراني أصبح ساحة جديدة للصراعات، مما يتطلب استراتيجيات فعالة لحماية البنية التحتية المعلوماتية للدول.

الابتكارات التكنولوجية

تسلط الأبحاث الضوء على **الابتكارات التكنولوجية** في مجال الأمن السيبراني، مثل تطوير أدوات جديدة لكشف التهديدات وتحليل البرمجيات الخبيثة. هذا يتضمن دراسة حالات معينة من الهجمات وكيفية التعامل معها، مما يوفر رؤى قيمة لتعزيز الأمان الرقمي.

أهمية التدريب والتطوير

تؤكد الدراسات أيضًا على ضرورة **التدريب والتطوير** للفرق العاملة في مجال الأمن السيبراني، حيث أن الفجوات في المعرفة والمهارات تمثل تحديًا كبيرًا في مواجهة التهديدات المتطورة.

هذه الدراسات تمثل خطوة مهمة نحو فهم أفضل لتهديدات الأمن السيبراني وكيفية التصدي لها، مما يسهم في تعزيز الأمان الرقمي للأفراد والمؤسسات.

مناهج الدراسة

المنهج الوصفي التحليلي:

- ✓ مناسب لـ :تحليل الظاهرة وتوصيفها بشكل دقيق لفهم العلاقة بين الأمن السيبراني والأمن القومي.

المنهج التاريخي:

- ✓ مناسب لـ :دراسة تطور الهجمات السيبرانية وتأثيرها على الأمن القومي عبر الزمن.
- ✓ آلية التطبيق:
  - تحليل الحوادث السيبرانية السابقة وتأثيرها على الأمن القومي.

.أدوات جمع البيانات:

- **تحليل وثائق وأدبيات:**
  - ✓ جمع البيانات من الدراسات السابقة والتقارير الأمنية.
  - ✓ مراجعة القوانين والتشريعات المرتبطة بالأمن السيبراني.

Citations:

[1]المجلة العربية للعلوم و نشر الأبحاث

https://blog.ajsrp.com/%d8%ae%d8%af%d9%85%d8%a7%d8%aa-%d9%85%d9%85%d9%8a%d8%b2%d8%a9/
https://blog.ajsrp.com/%D8%B9%D9%86%D8%A7%D9%88%D9%8A%D9%86-%D8%A8%D8%AD%D9%88%D8%AB-%D9%81%D9%8A-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A/
[2] https://www.injazatpapers.com/%D8%B1%D8%B3%D8%A7%D8%A6%D9%84-%D9%85%D8%A7%D8%AC%D8%B3%D8%AA%D9%8A%D8%B1-%D9%88%D8%AF%D9%83%D8%AA%D9%88%D8%B1%D8%A7%D9%87-%D9%81%D9%8A-%D8%A7%D9%84%D8%A7%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8/
[3]https://uni2pia.com/blog/%D8%AF%D8%B1%D8%A7%D8%B3%D8%A9_%D8%A7%D9%84%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A
[4] https://democraticac.de/?p=99583
[5] https://www.mobt3ath.com/dets.php?page=1051
[6] https://www.sis.gov.eg/Story/258293/%D9%85%D8%B5%D8%B1-%D9%88%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%89?lang=ar

الفصل الأول

أبرز التهديدات السيبرانية التي تواجه الدول الكبرى في الوقت الراهن والمحتملة خلال ٢٠ عامًا قادمًا

التهديدات الحالية

**** .1الهجمات السيبرانية المنظمة****

تتزايد **الهجمات السيبرانية المنظمة** التي تنفذها مجموعات مدعومة من دول، حيث تستخدم هذه المجموعات تكتيكات متعددة لتحقيق أهدافها، مثل الهجمات المتسلسلة التي تجمع بين أساليب مختلفة لتعظيم التأثير.

**** .2 استغلال الذكاء الاصطناعي****

يستخدم مجرمو الإنترنت **تقنيات الذكاء الاصطناعي** بشكل متزايد لتطوير أدوات مثل WormGPT وFraudGPT، التي تساعدهم في تنفيذ هجمات معقدة واستهداف البيانات الحساسة.

**** .3 التصيد الاحتيالي المتقدم****

تشهد عمليات **التصيد الاحتيالي** تطورًا كبيرًا، بما في ذلك استخدام تقنيات **التزييف العميق** لإنشاء محتوى مزيف، مثل مقاطع الفيديو والصوت، مما يزيد من صعوبة اكتشاف الاحتيال.

**** .4 الهجمات على البنية التحتية الحيوية****

تستهدف الهجمات السيبرانية بشكل متزايد **البنية التحتية الحيوية** للدول، مثل شبكات الطاقة والمياه، مما يشكل تهديدًا للأمن القومي ويؤثر على الخدمات الأساسية.

التهديدات المحتملة خلال ٢٠ عامًا

**** .1 تزايد الاعتماد على الذكاء الاصطناعي****

من المتوقع أن يؤدي الاعتماد المتزايد على الذكاء الاصطناعي في جميع مجالات الحياة إلى ظهور **تهديدات جديدة**، حيث يمكن أن يتم استغلال هذه التكنولوجيا من قبل المهاجمين لشن هجمات أكثر تعقيدًا.

**** .2 تصاعد الهجمات السحابية****

مع تزايد استخدام الخدمات السحابية، ستصبح **الهجمات السحابية** أكثر شيوعًا، مما يتطلب تطوير استراتيجيات جديدة لحماية البيانات المخزنة في هذه البيئة.

**** .3 التحديات المتعلقة بالخصوصية****

ستظل قضايا **الخصوصية وحماية البيانات** تشكل تحديًا كبيرًا، خاصة مع تزايد استخدام الأجهزة المتصلة بالإنترنت (IoT) وزيادة كمية البيانات المتاحة عبر الإنترنت.

**** .4 الهجمات الإلكترونية على الانتخابات****

من المتوقع أن تستمر **الهجمات الإلكترونية على العمليات الانتخابية** كتهديد رئيسي، حيث يمكن أن تستخدم التقنيات الحديثة للتأثير على نتائج الانتخابات وزعزعة الاستقرار السياسي.

تتطلب هذه التهديدات استجابة فعالة من الدول الكبرى لتعزيز الأمن السيبراني وتطوير استراتيجيات جديدة لمواجهة المخاطر المتزايدة.

Citations:
[1] https://www.mc-doualiya.com/%D8%A8%D8%B1%D8%A7%D9%85%D8%AC/%D8%A7%D9%84%D9%86%D8%B4%D8%B1%D8%A9-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9/20240109-%D8%A3%D8%A8%D8%B1%D8%B2-%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF%D8%A7%D

8%AA-%D8%A7%D9%84%D8%A3%D9%85%D9%86-
%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9
%8A-%D9%88-%D8%A7%D9%85%D9%86-
%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%
AA-%D8%A7%D9%84%D9%85%D8%AA%D9%88%D9%82%D8%B9%D8%A9-
%D8%B9%D8%A7%D9%85-2024
[2]
https://www.ssl.com/ar/%D8%A8%D9%84%D9%88%D9%82/%D8%AA%D9%82%
D8%B1%D9%8A%D8%B1-%D8%A7%D9%84%D8%A3%D9%85%D9%86-
%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9
%8A-%D8%A3%D8%A8%D8%B1%D9%8A%D9%84-2024/
[3] https://www.skyhighsecurity.com/ar/industry-perspectives/eight-cybersecurity-predictions-for-2024-and-beyond.html

الفصل الثاني

أمثلة هامة لهجمات سيبرانية خلاي عام ٢٠٢٤

سلاسل الهجمات على مغاسل المطبخ: التهديد السيبراني الأساسي لانتخابات عام ٢٠٢٤

حذر خبراء الأمن السيبراني من أن التهديد الأكثر أهمية للعملية الديمقراطية سيكون على الأرجح مزيجًا من الهجمات السيبرانية المختلفة، وليس حادثة واحدة معزولة. تتضمن سلاسل الهجوم "المغرقة في المطبخ"، كما يطلق عليها، قراصنة يستخدمون تكتيكات متعددة جنبًا إلى جنب لتحقيق أهدافهم الخبيثة، مما يزيد من صعوبة اكتشافها والدفاع ضدها. وفقًا لتقرير حديث صادر عن شركة**Mandiant** ، وهي جزء من**Google Cloud** ، فإن أقوى التهديدات التي تواجه الانتخابات هي الهجمات المتسلسلة، حيث تقوم الجهات الفاعلة في مجال التهديد بوضع تكتيكات متعددة عمدًا في عمليات هجينة لتضخيم تأثير كل مكون. وقد تم استخدام هذا النهج في الانتخابات السابقة، مثل الانتخابات الرئاسية الأوكرانية عام ٢٠١٤، حيث شنت الجهات الروسية هجماتDDoS ، وحذفت الملفات من أجهزة الكمبيوتر الخاصة بالانتخابات المركزية في البلاد، وتسريب رسائل البريد الإلكتروني والوثائق، وحاولت تقديم نتائج مزيفة لصالح مرشح معين. في الانتخابات الأمريكية لعام ٢٠٢٠، نفذ مواطنان إيرانيان حملة ضد مواقع الويب المتعلقة بالتصويت في عدة ولايات، وحصلوا على معلومات سرية للناخبين، وأرسلوا رسائل بريد إلكتروني مخيفة ومضللة، ونشروا معلومات مضللة حول نقاط ضعف البنية التحتية للانتخابات. كما قاموا باختراق شركة إعلامية كان من الممكن أن توفر قناة أخرى لنشر الادعاءات الكاذبة. وبصرف النظر عن الجهات الفاعلة التي ترعاها الدولة، فإن المطلعين على بواطن الأمور، ونشطاء القرصنة، ومجرمي الإنترنت يشكلون أيضًا تهديدًا للعملية الديمقراطية. يمكن استخدام حسابات وسائل التواصل الاجتماعي والمواقع الإلكترونية المزيفة التابعة للمرشحين الرئاسيين لنشر

عمليات الاحتيال أو البرامج الضارة أو سرقة الأموال أو التأثير على آراء الناخبين من خلال توزيع أخبار مزيفة. يمكن أيضًا استخدام عمليات انتحال الشخصية هذه للتفاعل مع أشخاص حقيقيين من الحملات والتسلل إلى أنظمتهم. ومع تزايد إمكانية الوصول إلى ساحة المعركة الرقمية، فمن الأهمية بمكان أن يظل مسؤولو الانتخابات والحملات الانتخابية والناخبون يقظين واستباقيين في حماية نزاهة العملية الديمقراطية ضد هذه التهديدات السيبرانية المتطورة.

قراصنة ترعاهم الدولة يخترقون شبكة MITRE للبحث والتطوير عبر ثغراتIvanti Zero-Day

كشفتMITRE ، وهي شركة غير ربحية تمولها الحكومة الفيدرالية، مؤخرًا عن اختراق لبيئة التجارب والأبحاث والمحاكاة الافتراضية (NERVE) الخاصة بها من قبل جهة تهديد أجنبية ترعاها دولة في أوائل شهر يناير. استغل المهاجمون اثنتين من ثغرات يوم الصفر، CVE-2023-46805وCVE-2024-21887، في أجهزة Ivanti Connect Secure VPN للوصول الأولي. تم الإبلاغ عن هذه الثغرات الأمنية لأول مرة بواسطة Volexity في ١٠ يناير، ونسبت استغلالها إلى المتسللين المدعومين من الحكومة الصينية. بعد الوصول، أجرى المهاجمون استطلاعًا وتجاوزوا المصادقة متعددة العوامل باستخدام اختطاف الجلسة، وتحركوا أفقيًا داخل شبكة .MITRE لقد استخدموا أبوابًا خلفية وشبكات ويب متطورة للحفاظ على الثبات وجمع بيانات الاعتماد، واستهداف البنية التحتية لبرنامج VMware الخاص بالمؤسسة باستخدام حساب مسؤول مخترق. في حين أن MITRE لم تقدم تفاصيل الإسناد بخلاف تحديد المهاجمين باعتبارهم ممثل تهديد لدولة قومية أجنبية، فإن Google Cloud's Mandiantعلى علم بالعديد من الجهات الفاعلة المرتبطة بالتهديد المرتبطة بالصين والتي تستغل ثغرات Ivanti VPN في هجماتها. لم يجد التحقيق المستمر الذي تجريه MITRE أي دليل على التأثير على شبكة المؤسسة الأساسية أو أنظمة الشركاء. قامت المنظمة بمشاركة المعلومات حول تقنيات ATT&CK المرصودة، وأفضل الممارسات للكشف عن مثل هذه الهجمات،

والتوصيات المتعلقة بتقوية الشبكات. كما تم استخدام نفس ثغرات Ivanti لاختراق الأنظمة التابعة لوكالة الأمن السيبراني وأمن البنية التحتية الأمريكية(CISA) ، مما قد يؤثر على ١٠٠ ,٠٠٠ فرد. افتتحتMITRE ، المعروفة على نطاق واسع بقاعدة معارفها الخاصة بـ ATT&CK لتكتيكات وتقنيات الخصم، مؤخرًا مختبرًا جديدًا للتأمين والاكتشاف للذكاء الاصطناعي لاكتشاف وإدارة المخاطر في الأنظمة التي تدعم الذكاء الاصطناعي.

إطلاق ممثل التهديد CoralRaider حملة هجوم عالمية باستخدام العديد من سارقي المعلومات

كشفت وحدة أبحاث الأمان Talos التابعة لشركة Cisco عن حملة هجوم واسعة النطاق قام بها جهة تهديد تُعرف باسمCoralRaider ، والتي تستخدم مجموعة من سارقي المعلومات لجمع بيانات الاعتماد والبيانات المالية من المستخدمين في جميع أنحاء العالم. كان ممثل التهديد، الذي يُعتقد أنه من أصل فيتنامي، يستهدف الأفراد عبر مختلف قطاعات الأعمال والمناطق الجغرافية منذ عام ٢٠٢٣ على الأقل. تطورت حملة هجوم CoralRaider بمرور الوقت، حيث استخدم ممثل التهديد سابقًا متغير QuasarRAT مخصصًا يسمى RotBot و XClientsteerلاستهداف المعلومات المالية ومعلومات تسجيل الدخول وسرقة حسابات وسائل التواصل الاجتماعي. منذ فبراير ٢٠٢٤، قام ممثل التهديد بتوسيع ترسانته لتشمل ثلاثة سارقي معلومات Cryptbot :و LummaC2 و .Radamanthysاستهدفت الهجمات مستخدمين في الإكوادور، ومصر، وألمانيا، واليابان، ونيجيريا، والنرويج، وباكستان، والفلبين، وبولندا، وسوريا، وتركيا، والمملكة المتحدة، والولايات المتحدة، وتم تحديد بعض الضحايا على أنهم موظفون في مؤسسات مراكز اتصال خدمات الكمبيوتر في اليابان. ومنظمات خدمة الدفاع المدني في سوريا. يستخدم CoralRaider رسائل البريد الإلكتروني التصيدية التي تحتوي على روابط ضارة لتسليم أرشيفات ZIP مع ملفات مختصرة معدة، مما يؤدي إلى إطلاق سلسلة عدوى متعددة المراحل تؤدي في النهاية إلى تنفيذ سارقي

المعلومات على الأنظمة المستهدفة. تعد CryptBot و LummaC2و Radamanthysمن أدوات سرقة المعلومات المعروفة بقدرات متنوعة، بما في ذلك جمع بيانات الاعتماد من المتصفحات، وسرقة الملفات الحساسة، وتصفية البيانات من محافظ العملات المشفرة والتطبيقات الأخرى. إن استخدام أدوات السرقة هذه معًا يسمح لـ CoralRaider بتعظيم تأثير هجماتها وجمع نطاق واسع من المعلومات القيمة من ضحاياها. مع استمرار CoralRaider في التطور وتوسيع نطاق انتشارها العالمي، يجب على المنظمات والأفراد أن يظلوا يقظين وأن يعتمدوا تدابير قوية للأمن السيبراني للحماية من هذه التهديدات المتطورة بشكل متزايد. يعد تحديث البرامج بانتظام، واستخدام كلمات مرور قوية وفريدة من نوعها، وتمكين المصادقة متعددة العوامل، وتثقيف المستخدمين حول مخاطر رسائل البريد الإلكتروني التصيدية، خطوات أساسية في التخفيف من مخاطر الوقوع ضحية لمثل هذه الهجمات.

منظمة Change Healthcare تتعرض لهجوم ثانٍ من برامج الفدية بواسطةRansomHub

وبحسب ما ورد تعرضت شركةChange Healthcare ، وهي شركة تابعة لشركة United Healthcare، لهجوم آخر من برامج الفدية، هذه المرة من قبل عصابةRansomHub ، بعد أسابيع فقط من استهداف .ALPHV/BlackCat تدعي RansomHub أنها سرقت ٤ تيرابايت من البيانات الحساسة، بما في ذلك معلومات حول الأفراد العسكريين الأمريكيين والمرضى والسجلات الطبية والمعلومات المالية. تطالب العصابة بدفع مبلغ ابتزازي وتهدد ببيع البيانات لمن يدفع أعلى سعر إذا لم يتم دفع الفدية خلال ١٢ يومًا. يأتي هذا الهجوم الثاني في وقت مليء بالتحديات بالنسبة لشركة Change Healthcare، التي تعافت مؤخرًا فقط من الهجوم الإلكتروني السابق .ALPHV/BlackCat تواجه الشركة الآن قرارًا صعبًا فيما يتعلق بدفع الفدية أم لا لحماية المعلومات الحساسة لعملائها. ويشير ملاخي ووكر، المستشار الأمني فيDomainTools ، إلى أنه حتى لو لم تكن RansomHub

مرتبطة مباشرة بـALPHV/BlackCat ، فمن الممكن أن تدعي المجموعة وجود علاقات مع ضحاياها لترهيبهم ودفعهم. كما يسلط الضوء أيضًا على الاقتصاد السري المزدهر المحيط بمشهد برامج الفدية، حيث تتعاون جهات فاعلة مختلفة لتبادل المعلومات. في حين أن هناك تكهنات حول وجود اتصال محتمل بين ALPHV/BlackCat وRansomHub، أو إذا تم إعادة تسمية ALPHV إلى RansomHub، إلا أن ووكر ذكر أنه من السابق لأوانه تأكيد أي رابط مباشر بين المجموعتين. يسلط هذا الحادث الضوء على التهديد المستمر الذي تشكله عصابات برامج الفدية وأهمية اتخاذ تدابير قوية للأمن السيبراني لحماية البيانات الحساسة في قطاع الرعاية الصحية. بينما تتنقل شركة Change Healthcareفي هجوم برنامج الفدية الثاني هذا، فإنها تواجه موقفًا صعبًا في ضمان سلامة معلومات عملائها.

Citations:

١-تقرير-الأمن-السيبراني-أبريل- --SSl
https://www.ssl.com/ar/%D8%A8%D9%84%D9%88%D9%82/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A3%D8%A8%D8%B1%D9%8A%D9%84-2024/#ftoc-heading-1

الفصل الثالث

ضعف الأمن السيبراني يزيد من احتمالية تعرض البنية التحتية الحيوية لهجمات سيبرانية تؤثر على الأمن القومي

ويمكن تأييد هذا الفرض بالنماذج ودراسات الحالة التالية

توجد تجارب واقعية تدعم الفرض العلمي القائل بأن ضعف الأمن السيبراني يزيد من احتمالية تعرض البنية التحتية الحيوية لهجمات سيبرانية تؤثر على الأمن القومي. فيما يلي بعض هذه التجارب:

**** .1 الهجوم السيبراني على أستونيا (٢٠٠٧)** .**

كان الهجوم على أستونيا في عام ٢٠٠٧ نقطة تحول في فهم تأثير الهجمات السيبرانية على البنية التحتية الحيوية. استهدف الهجوم المواقع الحكومية والمالية والإعلامية، مما أدى إلى تعطيل الخدمات الأساسية لأسابيع. هذا الهجوم، الذي نسب إلى قراصنة روس، أبرز كيف يمكن أن تؤدي الثغرات في الأمن السيبراني إلى تأثيرات سلبية على الأمن القومي.

**** .2 فيروس ستوكسنت (٢٠١٠)** .**

يعتبر فيروس ستوكسنت مثالًا آخر على كيفية تأثير ضعف الأمن السيبراني على البنية التحتية الحيوية. استهدف هذا الفيروس المنشآت النووية الإيرانية، مما تسبب في أضرار مادية لأجهزة الطرد المركزي. أظهر ستوكسنت أن الهجمات السيبرانية يمكن أن تتجاوز الفضاء الرقمي لتؤثر بشكل مباشر على العمليات الفيزيائية، مما يعكس المخاطر الكبيرة التي تواجهها الدول بسبب ضعف الأمن السيبراني.

**** .3 الهجمات على البنية التحتية الصحية (٢٠٢٠)٢٠٢٠****

خلال جائحة كوفيد-١٩، تعرضت العديد من المؤسسات الصحية لهجمات سيبرانية متزايدة، بما في ذلك هجمات ransomware التي استهدفت المستشفيات. هذه الهجمات أدت إلى

تعطيل الخدمات الطبية الحيوية وأثرت على قدرة الدول على الاستجابة للأزمات الصحية، مما يبرز العلاقة بين ضعف الأمن السيبراني والأثر السلبي على الأمن القومي.

**** .4 الهجمات المدعومة من الدول****

تشير العديد من التقارير إلى أن الدول الكبرى، مثل روسيا والصين وكوريا الشمالية، تنفذ هجمات سيبرانية تستهدف البنية التحتية الحيوية للدول الأخرى لأغراض التجسس والتخريب. هذه الأنشطة تعكس كيف يمكن أن يؤدي ضعف الأمن السيبراني إلى تهديدات مباشرة للأمن القومي، حيث يتم استغلال الثغرات لتحقيق أهداف سياسية أو اقتصادية.

هذه التجارب تؤكد أهمية تعزيز الأمن السيبراني لحماية البنية التحتية الحيوية وضمان استقرار الأمن القومي للدول.

Citations:
[1]
https://www.youm7.com/story/2024/7/21/%D9%87%D8%A7%D9%83%D8%B1%D8%B2-%D8%A8%D8%AF%D8%B1%D8%AC%D8%A9-%D8%AC%D9%86%D9%88%D8%AF-%D8%A7%D9%84%D8%AD%D8%B1%D9%88%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%88%D8%B3%D9%8A%D9%86%D8%A7%D8%B1%D9%8A%D9%88%D9%87%D8%A7%D8%AA-%D9%85%D8%B3%D8%AA%D9%82%D8%A8%D9%84%D9%87%D8%A7-%D8%A7%D9%84%D8%A3%D9%83%D8%AB%D8%B1-%D8%B1%D8%B9%D8%A8%D8%A7%D9%8B/6646735
[2] https://unidir.org/files/2022-02/UNIDIR_International_Cooperation_Mitigate_Cyber_Operations_Critical_Infrastructure_AR.pdf
[3]
https://jlr.journals.ekb.eg/article_140263_cb94f0a290f06e186c872c0b46fc66cc.pdf
[4] https://asjp.cerist.dz/en/downArticle/535/7/2/208054

الفصل الرابع

تطبيق استراتيجيات وسياسات شاملة للأمن السيبراني يقلل من التهديدات الموجهة للأمن القومي

تدعم العديد من التجارب الواقعية الفرض العلمي القائل بأن تطبيق استراتيجيات وسياسات شاملة للأمن السيبراني يقلل من التهديدات الموجهة للأمن القومي. فيما يلي بعض هذه التجارب:

**** .1الهجوم السيبراني على شركة**(2021) Colonial Pipeline**

في مايو ٢٠٢١، تعرضت شركةColonial Pipeline ، التي تدير أكبر شبكة لأنابيب الوقود في الولايات المتحدة، لهجوم سيبراني أدى إلى تعطيل عملياتها بشكل كبير. بعد الهجوم، قامت الشركة بتطبيق استراتيجيات أمنية شاملة، بما في ذلك تحديث الأنظمة وتعزيز تدابير الأمان، مما ساعد على استعادة العمليات بسرعة وتقليل التأثير على إمدادات الوقود في البلاد. هذه الاستجابة السريعة تعكس أهمية وجود استراتيجيات أمن سيبراني فعالة للتقليل من الأضرار الناتجة عن الهجمات.

**** .2 استراتيجيات الأمن السيبراني في المؤسسات المالية****

تعتبر المؤسسات المالية من أكثر القطاعات تعرضًا للهجمات السيبرانية. على سبيل المثال، قامت العديد من البنوك بتطبيق استراتيجيات شاملة تشمل استخدام تقنيات مثل **الكشف عن التهديدات والاستجابة للنقاط النهائية**(EDR) ، وتقنيات الخداع لجذب المهاجمين وتحليل أساليبهم. هذه الاستراتيجيات ساعدت في تقليل عدد الهجمات الناجحة وحماية البيانات الحساسة للعملاء.

**** .3 نموذج NIST للأمن السيبراني****

اعتمدت العديد من المؤسسات الحكومية والخاصة على **إطار العمل الأمني **NIST كجزء من استراتيجياتها للأمن السيبراني. هذا النموذج يوفر توجيهات شاملة لتقييم المخاطر وتطوير استراتيجيات فعالة للتخفيف منها. المؤسسات التي اتبعت هذا النموذج شهدت انخفاضًا ملحوظًا في الحوادث الأمنية، مما يبرز فعالية تطبيق سياسات شاملة للأمن السيبراني.

**** .4 استجابة الحكومة الأمريكية للهجمات السيبرانية****

بعد سلسلة من الهجمات السيبرانية الكبيرة، بما في ذلك هجومSolarWinds ، قامت الحكومة الأمريكية بتعزيز استراتيجيات الأمن السيبراني على مستوى الفيدرالية. تم تنفيذ سياسات جديدة تتضمن تحسين التعاون بين الوكالات وتبادل المعلومات حول التهديدات، مما أدى إلى تحسين القدرة على التصدي للهجمات وتقليل تأثيرها على الأمن القومي.

**** .5تجربة الدول الاسكندنافية****

استثمرت الدول الاسكندنافية في تطوير استراتيجيات شاملة للأمن السيبراني تشمل التدريب المستمر للموظفين وتحديث الأنظمة بشكل دوري. أدت هذه الجهود إلى تقليل عدد الهجمات الناجحة وزيادة الوعي بالأمن السيبراني بين المواطنين، مما يعكس كيف يمكن لاستراتيجيات الأمن الشاملة أن تحسن من الوضع الأمني العام.

هذه التجارب تؤكد أن تطبيق استراتيجيات وسياسات شاملة للأمن السيبراني يمكن أن يكون له تأثير كبير في تقليل التهديدات الموجهة للأمن القومي وتعزيز القدرة على التصدي للهجمات الإلكترونية.

Citation

[1] https://www.rmg-sa.com/%D8%A3%D9%87%D9%85-%D8%A7%D9%84%D9%86%D9%85%D8%A7%D8%B0%D8%AC-%D9%84%D8%AA%D8%AD%D9%82%D9%8A%D9%82-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84/

[2] https://www.azeusconvene.com/ar-sa/articles/cybersecurity-in-fi

[3] https://maed.journals.ekb.eg/article_269212_78babb976e961a2679a4b0befdedb087.pdf

[4]https://insight.oceanx.sa/%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A7%D8%AA-%D8%AA%D8%B9%D8%B2%D8%B2-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%81%D9%8

الفصل الخامس

الدول التي تستثمر بشكل كافٍ في مجال الأمن السيبراني تكون أقل عرضة للتأثيرات السلبية للهجمات السيبرانية.

تدعم عدة تجارب واقعية الفرض القائل بأن الدول التي تستثمر بشكل كافٍ في مجال الأمن السيبراني تكون أقل عرضة للتأثيرات السلبية للهجمات السيبرانية. فيما يلي بعض هذه التجارب:

**** .1 تجربة الإمارات العربية المتحدة****

استثمرت الإمارات بشكل كبير في تطوير **مجلس الأمن السيبراني**، الذي يهدف إلى تعزيز القدرات الدفاعية في مواجهة التهديدات السيبرانية. من خلال تنفيذ استراتيجيات شاملة، تمكنت الإمارات من تقليل عدد الهجمات الناجحة بشكل ملحوظ. على سبيل المثال، خلال "الأسبوع الإقليمي للأمن السيبراني"، تم تسليط الضوء على نجاح الإمارات في التصدي لمهددات الأمن السيبراني، مما يعكس فعالية استثماراتها في هذا المجال.

**** .2 تجربة إسرائيل****

تعتبر إسرائيل من الدول الرائدة في مجال الأمن السيبراني، حيث تستثمر الحكومة الإسرائيلية بشكل كبير في البحث والتطوير. وقد أدى هذا الاستثمار إلى إنشاء بيئة آمنة تقلل من تأثير الهجمات السيبرانية. على سبيل المثال، بعد الهجوم على شركة "سايبر إكسبو" في عام ٢٠٢٠، أظهرت إسرائيل قدرة عالية على استعادة الأنظمة بسرعة وتقليل الأضرار، مما يدل على فعالية استراتيجياتها الأمنية.

**** .3 استثمار كاسبرسكي في التعليم****

أجرت شركة كاسبرسكي دراسة تشير إلى أن نقص مهارات الأمن السيبراني يمكن أن يؤثر سلبًا على قدرة الدول والشركات على مواجهة التهديدات. لذا، قامت كاسبرسكي بتطوير برامج تعليمية بالتعاون مع الجامعات لتعزيز مهارات الطلاب في هذا المجال. هذه المبادرات ساعدت في تحسين جاهزية القوى العاملة لمواجهة التهديدات المتزايدة، مما يعكس أهمية الاستثمار في التعليم والتدريب.

**** .4 تجربة سنغافورة****

استثمرت سنغافورة بشكل كبير في تطوير استراتيجيات الأمن السيبراني الوطنية، بما في ذلك إنشاء هيئة الأمن السيبراني الوطنية .(CSA) هذه الهيئة تعمل على تعزيز التعاون بين القطاعين العام والخاص وتطوير برامج تدريب متخصصة. نتيجة لهذه الاستثمارات، تمكنت سنغافورة من تقليل عدد الحوادث الأمنية وزيادة مستوى الوعي بالأمن السيبراني بين المواطنين والشركات.

**** .5 الولايات المتحدة الأمريكية****

بعد سلسلة من الهجمات الكبيرة مثل هجومSolarWinds ، قامت الولايات المتحدة بتعزيز استثماراتها في الأمن السيبراني من خلال تنفيذ سياسات جديدة وتخصيص ميزانيات أكبر للأمن السيبراني. هذه الجهود أدت إلى تحسين الدفاعات الإلكترونية وتقليل عدد الهجمات الناجحة ضد البنية التحتية الحيوية.

تظهر هذه التجارب كيف أن الاستثمار الكافي في الأمن السيبراني يمكن أن يقلل بشكل كبير من التأثيرات السلبية للهجمات السيبرانية ويعزز الأمان القومي للدول.

Citations:

[1] https://gcforum.org/GCF-2022-Book-Arabic.pdf
[2] https://almalnews.com/%D9%85%D8%AA%D8%AE%D8%B5%D8%B5%D9%88-%D8%A7%D9%84%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7-%D9%8A%D8%A4%D9%83%D8%AF%D9%88%D9%86-%D8%A3%D9%87%D9%85%D9%8A%D8%A9-%D8%A7%D9%84%D8%A7%D8%AA/
[3] https://www.aletihad.ae/opinion/4434704/%D8%A7%D9%84%D8%A3%D8%B3%D8%A8%D9%88%D8%B9-%D8%A7%D9%84%D8%A5%D9%82%D9%84%D9%8A%D9%85%D9%8A-%D9%84%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A
[4] https://cert.gov.om/sp/investment

الخاتمة

يمثل هذا البحث خطوة نحو فهم أعمق لتأثير الأمن السيبراني على الأمن القومي، كما يساهم في توجيه الجهود لتحسين السياسات والإجراءات لحماية الدول من المخاطر المتزايدة في الفضاء السيبراني. النتائج المتوقعة من هذا البحث ستكون ذات أهمية كبيرة لصناع القرار والباحثين والمهتمين بمجال الأمن السيبراني والأمن القومي على حد سواء.

نتناول في هذه الجزئية أهم التوصيات التي تؤكد علي أهمية الأمن السيبراني في تعزيز الأمن القومي، وتقدم استراتيجيات فعالة يمكن أن تعتمدها الدول لتقليل المخاطر المرتبطة بالتهديدات السيبرانية.

فيما يلي بعض التوصيات التي يمكن تنفيذها بصورة أو بأخري:

**** .1 تطوير استراتيجيات وطنية شاملة للأمن السيبراني****

** -وصف**: يجب على الدول تطوير استراتيجيات وطنية متكاملة للأمن السيبراني تشمل جميع القطاعات الحيوية، مثل الطاقة، الصحة، والنقل. هذه الاستراتيجيات يجب أن تتضمن تقييم المخاطر، وتحديد الأصول الحيوية، ووضع خطط استجابة فعالة.

** -التطبيق**: يمكن استخدام نماذج مثل الاستراتيجية الوطنية للأمن السيبراني التي أطلقتها مصر (٢٠١٧-٢٠٢١) كمرجع لتطوير استراتيجيات مشابهة في دول أخرى.

**** .2 تعزيز التعاون الدولي****

** -وصف**: يجب تعزيز التعاون بين الدول لمواجهة التهديدات السيبرانية العابرة للحدود. يشمل ذلك تبادل المعلومات حول التهديدات، وتطوير بروتوكولات مشتركة للاستجابة للهجمات.

** -التطبيق**: يمكن للدول الانضمام إلى مبادرات دولية مثل مركز الأمن السيبراني الأوروبي أو التعاون مع منظمات مثل الاتحاد الدولي للاتصالات لتعزيز القدرات الأمنية.

**** .3 استثمار في التعليم والتدريب****

** -وصف**: ينبغي على الدول الاستثمار في برامج التعليم والتدريب المتخصص في الأمن السيبراني لرفع مستوى الوعي والمهارات لدى الأفراد العاملين في هذا المجال.

** -التطبيق**: يمكن إنشاء شراكات مع الجامعات والمؤسسات التعليمية لتطوير مناهج دراسية تركز على الأمن السيبراني، كما فعلت بعض الدول التي أطلقت مبادرات تعليمية لتعزيز المهارات الرقمية.

**** .4 استخدام الذكاء الاصطناعي لتحسين الدفاعات السيبرانية****

** -وصف**: ينبغي استخدام تقنيات الذكاء الاصطناعي لتحليل البيانات والتنبؤ بالتهديدات وتعزيز الدفاعات الأمنية. يمكن للذكاء الاصطناعي أن يسهم في تحسين سرعة وكفاءة الاستجابة للحوادث.

** -التطبيق**: يجب على الدول دمج أدوات الذكاء الاصطناعي في أنظمة الأمن السيبراني الخاصة بها، كما تم الإشارة إليه في الأبحاث حول دور الذكاء الاصطناعي في تعزيز الأمن السيبراني.

**** .5 تطوير إطار عمل قانوني وتنظيمي****

** -وصف**: يتطلب تعزيز الأمن السيبراني وجود إطار قانوني وتنظيمي واضح يحدد المسؤوليات والعقوبات المتعلقة بالجرائم السيبرانية.

** -التطبيق**: ينبغي وضع قوانين تحمي البيانات الشخصية وتعزز من الشفافية والمساءلة، مما يسهم في بناء ثقة الجمهور في الأنظمة الرقمية.

**** .6 إجراء تقييمات دورية للأمن السيبراني****

** -وصف**: يجب على الدول إجراء تقييمات دورية لمستوى الأمن السيبراني لديها لتحديد الثغرات وتحسين الاستجابة.

** -التطبيق**: يمكن الاستفادة من تقارير الأمن السيبراني العالمية ومؤشرات الأداء لتقييم الفعالية والقدرة على مواجهة التهديدات.

**** .7 تعزيز الوعي العام حول الأمن السيبراني****

** -وصف**: يجب تنفيذ حملات توعية للمواطنين حول أهمية الأمن السيبراني وكيفية حماية أنفسهم من التهديدات.

** -التطبيق**: يمكن تنظيم ورش عمل وندوات تعليمية تهدف إلى رفع مستوى الوعي حول المخاطر وكيفية التصدي لها.

هذه التوصيات تمثل خطوات عملية يمكن أن تتخذها الدول لتعزيز أمنها السيبراني ودعم أمنها القومي بشكل فعال.