الانتهاكات الحديثة والهجمات السيبرانية والتدابير التقنية والإجرائية للحماية

إعداد

د. ياسر الملك احمد سليمان
استاذ مساعد – الجامعة الاسلامية بمنيسوتا
الولايات المتحدة الامريكية – المركز الرئيسي .

الجامعة الإسلامية بمنيسوتا
Islamic University of Minnesota
المركز الرئيسي IUM

الملخص:

تناول البحث مجموعه من المشاكل والاختراقات التي تمت في الفترة الأخيرة وهي من أكبر الهجمات علي مر التاريخ وتسببت في أعطال للأنظمة التقنية حول العالم .

ناقش البحث الهجمات السيبرانية والأعطال وكيفية التعامل مع كل منها و توضيح وفهم الاختلاف بشكل أفضل وتعزيز الأمان السيبراني بشكل عام و من خلال البحث تتم مناقشه مجموعة من الأمثلة لأعطال واختراقات وهجمات سيبرانية لأنظمة عالمية حديثة.

يهدف البحث إلى معرفه الأسباب الأساسية ونقاط الضعف والطرق التي تساهم في إيجاد الحلول سيتم في البحث التركيز على موضوع الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، حيث تهدف إلى تبيان مختلف التحديات والتهديدات السيبرانية التي تهدد أمن الدول.

الكلمات المفتاحية : الأمن السيبراني الاختراقات الإلكترونية ، الفضاء السيبراني.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

Abstract:

The research deals with a group of problems and breakthroughs in the previous period and the largest attacks in history that caused failures in technical systems around the world.
The research discussed cyber attacks and disruptions and how to deal with them, better understand the difference, and enhance cyber security.
Through the research, many examples of malfunctions, hacks, and cyber attacks on modern global systems are discussed.
The research aims to identify the basic causes, weaknesses, and methods that contribute to finding solutions. security and the challenges of espionage and electronic penetration of countries through cyberspace , It aims to clarify the various cyber challenges and risks that threaten the security of countries.

Keywords: CyberSecurity, Electronic hacking, CybersPace.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

المقدمة

الأمن السيبراني من أهم المجالات في عصرنا الحالي، ويهدف إلى حماية الأنظمة الإلكترونية والبيانات من التهديدات الإلكترونية والهجمات السيبرانية و يتضمن مجموعة من التقنيات والممارسات التي تهدف إلى حماية أنظمة المعلومات، والشبكات، والأجهزة الإلكترونية من الهجمات السيبرانية.

إن الأمن السيبراني يلعب دور كبيرًا في عصر التكنولوجيا الحديثة، لكن يتطلب حماية مستمرة واستراتيجيات متطورة لمواجهة التهديدات المتزايدة.

لكن مع ذلك فإنّ هناك العديد من مخاطر الأمن السيبرانيّ التي تواجه الأفراد، والشركات، والمنظمات مع زيادة الاعتماد على التكنولوجيا، شهدت الفترة الأخيرة تحديات كثيرة للأمن السيبراني أكثر من أي فترة مضت، حدثت نتيجة للأعطال والخلل في الانظمة والبرمجيات والتطبيقات المستخدمة تمت من خلالها الهجمات ولهذا يجب التعرف علي الفرق الكبير من وجهة نظر الباحث بين الأعطال والخلل و الهجمات السيبرانية إن الأعطال هي عباره عن مشاكل تقنية تحدث بسبب عيوب في البرمجيات أو التكنولوجيا وتكون نتاج أخطاء برمجية وتحميل وارتفاع علي الأنظمة ، أما الهجمات السيبرانية هي حدوث نشاط متعمد من قبل مهاجمين لأغراض واهداف ، ومن خلال التعريف وتوضيح الفرق تظهر العلاقة في أن للهجوم السيبراني يتم إستغلال الأعطال والخلل والثغرات ونقاط الضعف الموجودة في الشبكات أو أنظمة التشغيل المستخدمة أو البرمجيات من قبل المهاجمين وإلحاق الضرر بالأنظمة والبيانات.

مشكلة البحث :

تكمن مشكله البحث الأساسية في الأنشطة التي تستهدف الأنظمة الحاسوبية والشبكات الهامة واستغلال نقاط الضعف مما يشكل التهديدات الإلكترونية التي تتم علي البنوك والمصارف

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

ووسائل السغر مطارات وقطارات وحتي قنوات الإعلام و تلحق ضرر كبير وتعطل مصالح أفراد ومؤسسات ودول من خلال الهجمات السيبرانية المدروسة والمستهدفة التي تتم و يمكن تفسيرها علي أنها قرصنة وتخريب وأضرار بمصالح الشعوب.

أهداف البحث :

يهدف البحث الي التعرف علي الخلل (الأعطال) و هي المشاكل التقنية التي تحدث بسبب عيوب في البرمجيات أو التكنولوجيا دون نية متعمدة لإلحاق الضرر. عادة ما تكون الأعطال ناتجة عن أخطاء برمجية أو مشاكل تقنية أو ارتفاع في الحمل على الأنظمة فهم الاختلاف بين الهجمات السيبرانية والأعطال يساعد في التعامل مع كل منها بشكل أفضل وتعزيز الأمان السيبراني بشكل عام.

أهمية البحث :

تتمثل في مجموعة نقاط هامة ظهرت حديثا وهي مجموعة الأعطال والاختراقات في أنظمة الحوسبة حيث شهدت شركات الطيران والمطارات والبنوك وشركات الإعلام ستناولها في البحث والسعي في معرفة الأسباب التي أدت لذلك و الوقاية من الاختراقات، والتهديدات الإلكترونية، وضمان أمن البيانات والمعلومات وتفاديا لها في المستقبل للتأثير العالمي الكبير.

منهجية البحث :

الباحث في منهجية البحث المنهج الوصفي والتحليلي المنهج الوصفي في الشرح و التوصيف ومن ثم التحليلي لشرح المشكلة والمساهمة في كيفية إيجاد طرق عديده تساعد في الحلول والتوصل لنتائج البحث الضرورية.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

تساؤلات البحث:

- ما هي التهديدات في الأمن السيبراني و مخاطر الاختراقات السيبرانية؟
- كيف تتم الانتهاكات والهجمات الإلكترونية علي الأمن السيبراني علي الأنظمة المعلوماتية للوزارات و مؤسسات الدول؟
- هل توجد تدابير تقنية وإجرائية لإيجاد حلول للحد من الانتهاكات الإلكترونية؟
- هل تساهم التدابير التقنية في حماية الأمن السيبراني من الهجمات الإلكترونية ؟

حدود البحث :

أقتصر البحث علي التعرف بالمخاطر السيبرانية والهجمات الإلكترونية علي المؤسسات الحكومية الكبيرة في الدول المتقدمة والثغرات ونقاط الضعف وكيفية إجراء التدابير المناسبة

حدود زمانية: أجريت الدراسة في بداية يونيو ٢٠٢٤ .

حدود مكانية : اهتم البحث بالمؤسسات الحكومية والوزارات المهمة بالدول العظمى .

هيكل البحث :

تقسيم خطة البحث في شكل محاور ونقاط مهمه داخل فصول وتقسيم البحث إلي ثلاث فصول هامه وهي كما يلي :

الفصل الأول محاور البحث المهمة مقدمة للبحث تشتمل علي تعريف الأمن السيبراني ، أهميته والمهددات والمخاطر في الأمن السيبراني ، مشكلة البحث ، أهداف البحث ، أهمية البحث ، المنهجية المتبعة في البحث ، تساؤلات هامة للبحث.

الفصل الثاني يشتمل علي محاور البحث الأساسية مدخل للبحث ، الانتهاكات الحديثة والمهددات الإلكترونية ، الأمثلة الواقعية الحديثة للهجمات الإلكترونية التي تستهدف المؤسسات الحكومية الهامة والوزارات للدول.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

يحتوي تعريف الثغرات ونقاط الضعف ، الأعطال (الخلل) ، مشاكل نظم التشغيل التي تسبب الأعطال ، التدابير التقنية والإجرائية ، طرق الحلول والمساهمة في نهج أساليب حديثة للحماية.
الفصل الثالث يشتمل نتائج البحث ، وخاتمة البحث ، وتوصيات الباحث للتدابير التقنية .

مفهوم الأمن السيبراني

هو ممارسة حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة. تتحمل المؤسسات مسؤولية تأمين البيانات للحفاظ على ثقة العملاء والامتثال للمتطلبات التنظيمية. فهي تعتمد تدابير وأدوات الأمن السيبراني من أجل حماية البيانات الحساسة من الوصول غير المصرّح به، وكذلك منع أي انقطاع للعمليات التجارية بسبب نشاط الشبكة غير المرغوب فيه. تطبّق المؤسسات الأمن السيبراني من خلال تبسيط الدفاع الرقمي بين الأفراد والعمليات والتقنيات ، تنفّذ المؤسسات استراتيجيات الأمن السيبراني من خلال العمل مع متخصّصين يقيّم هؤلاء المتخصصون المخاطر الأمنية لأنظمة الحوسبة الحالية، والشبكات، ومخازن البيانات، والتطبيقات، والأجهزة المتصلة الأخرى. بعد ذلك، ينشئ متخصصو الأمن السيبراني إطار عمل شامل للأمن السيبراني وينفّذون تدابير وقائية في المؤسسة.

نهج الأمن السيبراني:

يحتوي النهج الناجح على طبقات متعددة من الحماية تنتشر عبر أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي يرغب المرء في الحفاظ عليها.
بالنسبة للأشخاص والعمليات والتكنولوجيا، يجب أن يكمل كل منها الآخر داخل المؤسسة لإنشاء دفاع فعال في مواجهة الهجمات السيبرانية ، والتي تهدف عادةً إلى الوصول إلى المعلومات الحساسة

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

أو تغييرها أو تدميرها؛ بغرض الاستيلاء على المال والابتزاز من المستخدمين أو مقاطعة عمليات الأعمال العادية.

مع تغيّر التقنيات، تنشأ أشكال جديدة من الهجمات السيبرانية ، يستخدم المجرمون أدوات جديدة ويبتكرون استراتيجيات جديدة للوصول إلى النظام بدون إذن. تتبنّى المؤسسات تدابير الأمن السيبراني وتحدّثها لمواكبة تقنيات وأدوات الهجوم الرقمي الجديدة والمتطورة.

مع انعدام القدرة على وقف الهجمات السيبرانية ، وفي ظل ارتباط مصالح الدول على نحوٍ متزايد بالفضاء السيبراني الرقمي تتقلص أهمية كافة الآليات الدفاعية بما في ذلك دفاعات الاستكشاف والبحث عن نقاط الضعف والثغرات وكيفية اتخاذ التدابير الحديثة لسد هذه الثغرات لمواجهة المخاطر والإنتهاكات .

الثغرات الأمنية:

تحديد المناطق التي تحتاج إلى تعزيز من الخطوات المهمة التي يرتكز عليها الباحث من خلال إجراء تقييمات الضعف والتدابير التقنية اللازمة سيتم شرح لبعض أنواع الثغرات ونقاط الضعف المهمة في البحث وكيفية المعالجة والحلول المناسبة .

هناك عدة أنواع من نقاط الضعف التي يمكن العثور عليها في أنظمة تكنولوجيا المعلومات.

من أكثر نقاط الضعف هي (البرمجيات، الشبكة، في نظم التشغيل) نقاط الضعف في البرمجيات هي نقاط ضعف موجودة في رمز البرمجيات التي يمكن استغلالها من قبل المتسللين، نقاط الضعف في الشبكة هي نقاط ضعف موجودة في البنية التحتية للشبكة التي يمكن أن يستغلها المهاجمون، نقاط الضعف في نظم التشغيل هي تلك التي تنطوي على خطأ ، سيتم شرح في كل نوع وتحديد الأعطال أو الانتهاك من خلاله.

بعد التعرف على الثغرات ونقاط الضعف التي تتسبب في المخاطر

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

يجب وضع طريقة التقييم لهذه المخاطر السيبرانية من خلال مراحل وضعها الباحث في هذا البحث من خلال مرحلتين .

مراحل إدارة المخاطر والانتهاكات والهجمات الإلكترونية :

1. التقييم والمعالجة .
2. السيطره والتدابير .

التقييم : تُستخدم تقييمات المخاطر السيبرانية لتحديد وتصنيف المخاطر التي تتعرض لها العمليات والأصول التنظيمية الناتجة عن استخدام أنظمة المعلومات ، تُعرَف إدارة مخاطر الأمن السيبراني على أنها مجموعة خطوات تتُخذ بشكل دوري لمواجهة التهديدات الإلكترونية ومعالجتها من خلال رصدها وتحديدها وتقييمها، ومن أجل إدارتها بفاعلية فإن ذلك يتطلب نظرة شاملة لهذه المخاطر وتعاون من كافة أفراد العمل، ليس فقط من أفراد إدارة المخاطر وإنما أفراد الإدارات الأخرى.

وتُعرف إدارة مخاطر الأمن السيبراني أيضًا بأنها عملية مستمرة لتحديد وتحليل وتقييم ومعالجة تهديدات الأمن السيبراني التي تواجهها الم ؤسسة.

تعتمد إدارة مخاطر الأمن السيبراني على استراتيجيات تساعد على ترتيب أولويات المخاطر المطلوب معالجتها؛ لرصد التهديدات الأكثر ضررًا والمطلوب مواجهتها في الوقت المطلوب.

تتعرض مؤسسات وقطاعات الأعمال بكافة انواعها للجريمة السيبرانية وتعتبر القطاعات الاقتصادية الأكثر تعرض للجريمة الالكترونية «السيبرانية» ومن أهمها : «الترتيب حسب تكرارية التعرض للخطر وشدته»:

1. المؤسسات المصرفية.
2. قطاعات الطيران.
3. مؤسسات الرعاية الصحية
4. قطاع البنية التحتية للاتصالات.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

5 قطاع التأمين
6 قطاع الاعلام والإذاعة

الأنتهاكات الحديثة والهجمات السيبرانية :

اهتمام البحث بمشكلة الانتهاكات والهجمات الإلكترونية والتعرف علي نقاط الضعف والثغرات الحديثة والأعطال للتخفيف من مخاطر الانتهاكات ، من خلال خطة علمية وعملية تشرح مشاكل حقيقية وواقعية ومن ثم توضيح إستغلال هذه الثغرات والاعطال والتسبب في الاختراقات والهجمات السيبرانية المستهدفة . .

توضيح امثلة عالمية للأعطال والاختراقات التي حدثت وهي :

- أعطال في مطارات مجموعة دول وهي مطارات (اسبانيا- ألمانيا- اسكتلندا ومطار أمستردام في هولندا- امريكا هجمات سيبرانية.
- قنوات وإذاعات عالمية مثل (انقطاع في إرسال هيئة الإذاعة الاسترالية ومشكلات تقنية ضخمة على مستوى البلاد)، وإيضا من الفتوات العالمية التي حدثت نفس المشكلة (قناة سكاي نيوز البريطانية تعلن توقف بثها) نفس الخلل- التأثيرات التي حدثت بورصة لندن تعلن تأثر خدماتها .
- شركة القطارات البريطانية تعلن عن أعطال في أنظمتها و تلغي جميع رحلات.
- مركز ٩١١ للطوارئ الأمريكي يتلقى عشرات الآلاف من المكالمات ويواجه ضغط شديد من المتصلين.

إن جميع الأعطال والاختراقات والثغرات كانت مرتبطة بالأجهزة التي تعمل على نظام Windows.

تظهر الأمثلة السابقة اتساع نطاق الاستخدامات الهجومية الإلكترونية، وانتشارها على المستوى الدولي، حيث باتت أحد أبرز التهديدات الإلكترونية القادرة على شل حركة الأنظمة الإلكترونية وتعطيل مصالح الدول والحكومات وحتى الأفراد والشركات والبنوك وغيرها من المؤسسات. .

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

المعالجة لمخاطر الأمن السيبراني من تتم من خلال :

1. التخفيف من مخاطر الأمن السيبراني: يتم التخفيف من مخاطر الأمن السيبراني من خلال تطبيق الضوابط الأمنية المطلوبة للحد من احتماليتها أو حجمها / تأثيرها، أو كليهما، والوصول بتقييم تلك المخاطر إلى مستوى يمكن قبوله.
2. تجنّب مخاطر الأمن السيبراني: تجنّب الظروف والأحوال التي تنتج عنها تلك المخاطر.
3. تحويل مخاطر الأمن السيبراني: نقل تلك المخاطر إلى طرف آخر يتمتع بقدرات أفضل للتعامل معها أو التأمين على الأصول المعلوماتية والتقنية ضد تلك المخاطر.
4. تقبّل مخاطر الأمن السيبراني: يكون مستوى تلك المخاطر مقبولًا، لكن يجب مراقبتها باستمرار تحسبًا لأي تغيير.

شكل (I) يوضح الثغرات في الامن السيبراني

الجرائم الإلكترونية الحديثة:

إن تطور الجريمة الإلكترونية بسبب التطور المتسارع للتكنولوجيا والبرمجيات – يقف عائقاً أمام الإلمام بمفهومها, وكذلك أمام الجهود الدولية في مجال مكافحتها لأنها تتسبب في ظهور أنواع جديدة لا يحتويها التعريف وتتطور مع تطور التكنولوجيا وإستخدام الامن

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

السيبراني والمحافظة على المعلومات في المؤسسات والوزارات الحكومية للدول يتعرض اليوم لمخاطر جمة ومن أهمها محاولات الإختراق السيبراني وهو ما يشكل ضررا كبيرا لقواعد البيانات وكشف المعلومات السرية للمؤسسات وتتمثل المشكلة في كيفية التعرف على المشاكل الحقيقية والثغرات ونقاط الضعف التي تمكن من عملية الهجمات الإلكترونية ومن ثم تتم عملية الإختراق.

من خلال الأمثلة التي استند عليها الباحث يجب شرح وتوصيف المشاكل نظم التشغيل ، كيفية التدابير والحلول الممكنة. تتمثل جميع المشاكل التي تسبب الاعطال (الخلل) من خلال نظم التشغيل ممثلة في الاتي :

1. ثغرة برمجية خطرة من نوع « drive-by» في أنظمة «ويندوز-١٠» و «ويندوز-١١» يمكن استغلالها في إختراق تلك الأنظمة والوصول إلى بيانات الأجهزة العاملة.
2. مايكروسوفت كانت قد أطلقت العديد من التحديثات الأمنية لأنظمة ويندوز بعد أن أعلنت عن اكتشاف العديد من الثغرات الخطرة فيها مثل ثغرة PrintNightmare البرمجية في خدمات Windows Print Spooler، حتى أنها أطلقت تحديثات لأنظمة «ويندوز-٧» التي كانت قد توقفت عن دعمها .
3. بإصدار تحديثات برمجية لأنظمة تشغيل، لكن تلك التحديثات لم تعالج الثغرة بالشكل المطلوب تبعا لهم، كما أن مايكروسوفت لم تطلق أي تصريحات رسمية عن هذه الثغرة للمستخدمين، بل حاولت إصلاحها.
4. بسبب عدم تطبيق التحديثات الأمنية الدورية patch التي تصدرها شركات نظم التشغيل بشكل دوري لإغلاق الثغرات الأمنية المستجدة .

الثغرات ونقاط ضعف في البرمجيات والتطبيقات:

اخطر نقاط الضعف في الأمن السيبراني هي البرامج والأنظمة القديمة و عندما لا يتم تحديث البرامج والإجراءات بانتظام ، فإنها

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

تصبح عرضة للهجمات و يمكن للمتسللين إستغلالها للوصول إلى المعلومات الحساسة أو تثبيت برامج ضارة للحماية من هذه الثغرة الأمنية، لهذا يجب التأكد من تحديث جميع البرامج والأنظمة بانتظام بأحدث التحديثات وخصوصا الأمان والترقيات الهامة للبرامج والتطبيقات في الحاسب .

البرامج النصية الآلية تعمل بدون فحص الفيروسات وتتسبب في أعطال .

هناك ثغرة أخرى شائعة في الأمن السيبراني للكمبيوتر أتقنها المهاجمون وهي استخدام اتجاهات معينة لتشغيل البرامج النصية "الموثوقة" أو "الآمنة" تلقائيًا عند القيام بذلك، يتمتع مجرمو الإنترنت بالقدرة على جعل برنامج المتصفح يقوم بتشغيل برامج ضارة دون علم المستخدم.

الثغرات ونقاط ضعف في شبكات المؤسسات :

نقاط الضعف والأعطال في الشبكات لأنظمة المؤسسات تتسبب في الهجمات السيبرانية والانتهاكات تتطرق الباحث لمجموعة هامة من هذه الاعطال ونقاط الضعف في الجانب الشبكي للمؤسسات والشركات والبنوك والمصارف الهامة في الدولة. تشير نقاط الضعف في الشبكة إلى نقاط الضعف أو العيوب في البنية التحتية للشبكة التي يمكن استغلالها من قبل الجهات الفاعلة الضارة للوصول غير المصرح بها أو عمليات تعطيل أو سرقة المعلومات الحساسة. يمكن أن توجد هذه الثغرات الأمنية على مستويات مختلفة داخل الشبكة، بما في ذلك الأجهزة والبرامج .

أنواع نقاط الضعف في الشبكة:

1. نقاط الضعف في الأجهزة: تنشأ هذه الثغرات من نقاط الضعف في المكونات المادية مثل أجهزة التوجيه أو المفاتيح أو الخوادم. على سبيل المثال، قد تحتوي البرامج الثابتة القديمة على جهاز توجيه على عيوب أمان معروفة يمكن استغلالها.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

2 ثغرات التكوين: يمكن لخطأ التكوينات في أجهزة أو أنظمة الشبكة إنشاء فجوات أمان. على سبيل المثال، فإن ترك كلمات المرور الافتراضية دون تغيير على أجهزة الشبكة يجعلها هدفاً سهلًا للمهاجمين.

3 تعطيل الخدمة: يمكن أن تعطل الهجمات التي تستهدف نقاط الضعف في الشبكة الخدمات الهامة، مما يسبب وقت التوقف والتأثير على العمليات المصرفية و لتجارية.

شكل (٢) يوضح نقاط الضعف في الشبكة (٨)

هجمات بروتكول الشبكة يشير الهجوم ا/٥١ إلى نوع معين من هجوم رفض الخدمة الموزع (DDOS) الذي يستغل ثغرة في بروتوكولات الشبكة. إنه يستفيد من الطريقة التي تتعامل بها هذه البروتوكولات التي تتعامل مع الزيارات الواردة، مما يجعل النظام المستهدف مع عدد مفرط من الطلبات، ينبع اسم «ا/٥١» من حقيقة أنه لكل ٥١ حزمة أرسلها المهاجم، لا يلزم سوى استجابة واحدة، مما يجعلها فعالة للغاية من حيث استخدام الموارد، يستغل المهاجم هذه الثغرة الأمنية عن طريق توليد مدخلات متعددة حتى يجدوا تصادماً، مما يسمح لهم بتجاوز التدابير الأمنية.

.

للتخفيف من المخاطر المرتبطة بـ ا/٥١ هجمات، يمكن استخدام العديد من الاستراتيجيات:

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

1. اختيار وظيفة تجزئة التشفير: اختيار وظيفة تجزئة آمنة مع حجم إخراج أكبر يقلل من احتمال الاصطدامات. يتم تبني الخوارزميات مثل SHA-٢٥٦ أو SHA-٣ على نطاق واسع بسبب مقاومتها ضد هجمات الاصطدام.
2. تحديثات الخوارزمية العادية: نظراً لاكتشاف نقاط الضعف في وظائف التجزئة مع مرور الوقت، من الأهمية بمكان البقاء في تحديث مع أحدث معايير التشفير والخوارزميات.

من هنا تبرز أهمية تطبيق أفضل التدابير في أمن الشبكة للتخلص من نقاط الضعف والثغرات التي ستفتح أبواب الحرب السيبرانية على المؤسسة.

تشمل التدابير في الأمن السيبراني :

بناء سياسات وضوابط وأنظمة مثل إنشاء جدران الحماية وبرامج مكافحة الفيروسات أنظمة كشف التسلل والوقاية منها والتشفير وكلمات المرور في عمليات تسجيل الدخول.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

الفصل الثالث

نتائج البحث:

يمكن تلخيص اهم النتائج التي توصل اليها الباحث في مجموعة نقاط وهي :

1. يواجه العصر الحديث عددًا كبيرًا من التهديدات الأمنية التي تتسم بتغيرها وتطورها المستمر، واتساع نطاق تأثيرها بحيث لا يقتصر على الإضرار بأمن فواعل بعينها، وإنما يمتد ليؤثر في الأمن العالمي بشكل عام. ولعل أبرز هذه التهديدات الأمنية المعاصرة وأكثرها حداثة وأوسعها انتشارا هي التهديدات الإلكترونية Cyber threats، فقد أصبحت التهديدات الإلكترونية من تؤثر بشكل مباشر علي حياة الناس ، حيثُ بات من المهم حصرها و تطوير استراتيجيات التدابير التقنية .
2. أصبحت الحاجة إلى الأمن السيبراني أمرًا بالغ الأهمية لحماية البيانات الحساسة، ومن خلال البحث نلاحظ أن هناك تهديدات وإنتهاكات عديده تواجه الأمن السيبراني، واصبح من الضروري مع تصاعد التهديدات السيبرانية حاجة ملحة لتطوير استراتيجيات وأدوات للحماية من هذه التهديدات، وتكون داعم للحماية والمتابعة بصوره دوريه .
3. يجب تعزيز حماية أنظمة التشغيل و التقنيات المستخدمة للحد من الهجمات والإنتهاكات التي تستهدف الأجهزة الحكومية ومؤسسات الدولة.
4. أغلب الهجمات التي تحدث تكون عبر الشبكات الإلكترونية، لذلك يجب وضع أنظمة أمنية تعمل كصمام أمان للشبكة، وتضمن تلك الأنظمة حلول فورية وتحكم كاملٍ في عناصر البيانات والوصول للشبكة، حتى تمنع أي هجمات الكترونية .
5. توجد مشكلة في إستخدامات البرامج والتطبيقات يجب التعامل مع أمن التطبيقات بحماية البرامج والتطبيقات الخاصة بالشركة أو المؤسسة، لهذا يجب ضمان أن البرمجيات المستخدمة في

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

الشركة تتوافق مع معايير الأمان المعتمدة وأنها خالية من الثغرات المعروفة يكون ذلك من خلال إجراء فحوصات أمنية واختبارات الآمن للتأكد من عدم وجود ثغرات قد يستغلها المهاجمون.

التدابير التقنية والإجرائية للحماية:

للتخفيف من المخاطر المرتبطة بـ ٥١/١ هجمات، يوضح البحث مجموعة من الاستراتيجيات التي يمكن استخدامها وهي الاستراتيجيات:

1. اختيار وظيفة تجزئة التشفير: اختيار وظيفة تجزئة آمنة مع حجم إخراج أكبر يقلل من احتمال الاصطدامات. يتم تبني الخوارزميات مثل SHA-٢٥٦ أو SHA-٣ على نطاق واسع بسبب مقاومتها ضد هجمات الاصطدام.
2. تحديثات الخوارزمية العادية: نظراً لاكتشاف نقاط الضعف في وظائف التجزئة مع مرور الوقت، من الأهمية بمكان البقاء في تحديث مع أحدث معايير التشفير والخوارزميات
3. أنظمة الكشف عن التسلل والوقاية (IDPs) تلعب دوراً مهماً في اكتشاف الهجمات وتخفيفها مثل الهجوم ٥١/١. تراقب هذه الأنظمة حركة الشبكة، وتحليل الأنماط، وتحديد الأنشطة المشبوهة أو الحالات الشاذة التي قد تشير إلى هجوم مستمر.

من هنا تبرز أهمية تطبيق أفضل التدابير في أمن الشبكة للتخلص من نقاط الضعف والثغرات التي ستفتح أبواب الحرب السيبرانية على المؤسسة.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

الخاتمة والتوصيات

تناولت البحث موضوع الانتهاكات الإلكترونية باعتبارها ظاهرة تفشت في المجتمعات الحديثة ونالت من المجتمعات النامية مثلما نالت من المتقدمة، مع أن أضرارها وآثارها انحصرت في الدول المتقدمة. أن الأمن السيبراني للدول والمؤسسات يتعرض لمخاطر وهي الانتهاكات والاختراقات مما يتسبب في ضرر لقواعد البيانات وكشف المعلومات السرية للمؤسسات وتعطيل مجموعة من الخدمات وتتمثل المشكلة في كيفية تحديد للثغرات والمخاطر واجراء التدابير التقنية والتعرف علي الحلول والمعالجات تساعد في الحماية .

في خاتمة البحث يجب التوعية بمجموعة من النقاط الهامة المتمثلة في الآتي :

1. التوعية بفوائد الأمن السيبراني بوصفه أداة هامة للحفاظ على خصوصية المعلومات، بالإضافة إلى تحسين أمن المعلومات و طريقة حفظ البيانات والمعلومات خاصة بالنسبة للشركات والبنوك والوزارات.
2. المعرفة بأهمية تخصص الأمن السيبراني؛ خاصة أنه واحد من التخصصات المهتمة بممارسة الدفاع عن أجهزة الحواسيب وأجهزة الهواتف المحمولة، وحماية البيانات من أي تجسس أو هجمات خارجية، لأنّ هذا يُسبب اختراق للخصوصية وضياع للمعلومات وابتزاز للأشخاص و تخصص الأمن السيبراني مهم جدًا إذ إنه يشكل مصدر الأمان لكل وسائل التكنولوجيا.
3. توعية المؤسسات الحكومية والأفراد بأهمية المتابعة والتطوير واستخدامات البرمجيات الاصلية وعملية التحديث بصوره دورية يُساهم في معرفة أساليب الحماية الضرورية لمعلوماتهم والتي عليهم القيام بها.

يوصي الباحث بمجموعة من التوصيات لمواجهة التحديات في الأمن

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

السيبراني والانتهاكات بصوره مستقبلية تتبني أفضل المهارات لرفع مستوي الامن للفضاء السيبراني المعلوماتي للدول .

توصيات الباحث تتلخص في الآتي:

1. إقامة مؤسسات بحثية داخل وحدات مكافحة الجريمة الإلكترونية تهتم بالأمن الدولي الإلكتروني، والتعامل مع التطورات التقنية التي تؤدي إلى تطور وسائل الجريمة الإلكترونية.
2. توظيف الكوادر ذوي الخبرات التقنية الفائقة في مجال الحاسوب في المؤسسات الحكومية المنوط لها التعامل مع الجرائم الإلكترونية سواء في مراكز الضبط أو في جهات التحقيق والقضاء السيبراني.
3. يجب تأمين الأنظمة التي تمكن من الوصول عن بعد والشبكات .
4. عدم إستخدام البرامج والتطبيقات مجهولة المصدر والمجانية التعامل مع التطبيقات والبرامج الاصلية والعمل علي تحديثها بصوره دورية ومستثمره التفادي لمشاكل الاعطال. .
5. المشاركة الجماعية للجهات الحكومية, والمنظمات ومراكز الأبحاث والجامعات, في رسم السياسات لمنع الحروب الإلكترونية المستترة والظاهرة, و وضع قوانين وتدابير اجرائية.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

المصادر و المراجع

المراجع العربية:

- د. إسلام مصطفي (٢٠٢٣) ، جريمة إختراق الامن السيبراني وحماية البيانات والمعلومات ، دراسة منشوره ، القاهرة .
- د. فرح يحي زعاترة (٢٠٢٣) ، التهديدات السيبرانية علي الامن القومي الامريكي ، رسالة منشوره .
- د.نوران شفيق (٢٠٢٢) ، اثر التهديدات الإلكترونية علي العلاقات الدولية ، دراسة في ابعاد الامن الالكتروني ، الكويت .
- نور سليمان يوسف يعقوب البالول (٢٠٢١): الأحكام الموضوعية لجرائم المعلوماتية , رسالة دكتوراه , غير منشورة , كلية الحقوق , قسم القانون الخاص , جامعة عين شمس.
- منصور ناصر الكعبي(٢٠٢١): أثر تكنولوجيا المعلومات علي ظهور الجرائم الالكترونية , دراسة ميدانية بإمارة أبو ظبي , رسالة دكتوراه , غير منشورة , كلية الآداب , قسم علم اجتماع , جامعة المنصورة.
- عيسي عبد الله الحبسي (٢٠٢٠): جرائم البريد الالكتروني «دراسة مقارنة» , رسالة دكتوراه , غير منشورة , كلية الحقوق , قسم القانون الجنائي , جامعة المنصورة.
- جلال الدين عبد الخالق (٢٠٢٠): الجريمة والانحراف من منظور الخدمة الاجتماعية , المكتب الجامعي الحديث , الازاريطة , ص ١٨٣.
- حسين عباس حميد (٢٠٢٠): نحو اختصاص محكمة الكترونية خاصة بالجرائم المعلوماتية ,رسالة ماجستير , غير منشورة , كلية الحقوق , قسم القانون الجنائي , جامعة الاسكندرية.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

Refernce:

- Source:MunichRe,Cyberresilience-Thecyberriskchallenge and the role of insurance-December 2014 Emarah,S. (2007) : The Control of Firewalls using nd national security Conference, Riyadhks, Information Technology and .
- Emarah,S.(2007): The Control of Firewalls using Active Networks, Information Technology and national security Conference,Riyadh.

ium.usa.online@gmail.com www.ium.edu.so
+ 967 730053135 http://ium.usa.online

الجامعة الإسلامية بمنيسوتا

Islamic University of Minnesota

المركز الرئيسي IUM