International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (2)

IJCI

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (2)

February 2025

Cyber security Crimes, weaknesses, and modern practical applications in solution

Yasser Elmalik Ahmed Seleman
Assistant Professor, Department of Computer Science and Information Systems, University of Technology, Sudan
dr.yaserking359@hotmail.com

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: Cyber Security, Electronic hacking, Cyber Space.

International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (2)

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (2)

IJCI
February 2025

جرائم الأمن السيبراني ونقاط الضعف والثغرات والتطبيقات العملية الحديثة في الحلول

ياسر الملك أحمد سليمان
أستاذ مساعد، قسم علوم الحاسوب نظم المعلومات، الجامعة التكنولوجية، السودان
dr.yaserking359@hotmail.com

الملخص

تناول البحث مجموعة من المشاكل والاختراقات التي تمت في الفترة الأخيرة وهي من أكبر الهجمات على مر التاريخ وتسببت في أعطال للأنظمة التقنية حول العالم. ناقش البحث الهجمات السيبرانية والأعطال وكيفية التعامل مع كل منها وتوضيح وفهم الاختلاف بشكل أفضل وتعزيز الأمان السيبراني بشكل عام. من خلال البحث تتم مناقشه مجموعة من الأمثلة لأعطال واختراقات وهجمات سيبرانية لأنظمة عالمية حديثة. يهدف البحث إلى معرفة 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.

كلمات مفتاحية: الأمن السيبراني، الاختراقات الإلكترونية، الفضاء السيبراني.

1. مقدّمة

الأمن السيبراني من أهم المجالات في عصرنا الحالي، ويهدف إلى حماية الأنظمة الإلكترونية والبيانات من التهديدات الإلكترونية والهجمات السيبرانية ويتضمن 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. 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 والهجمات السيبرانية إن الأعطال هي عبارة 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 وأهداف، ومن خلال التعريف وتوضيح الفرق تظهر العلاقة في أن للهجوم السيبراني يتم استغلال الأعطال والخلل والثغرات ونقاط الضعف الموجودة في الشبكات أو أنظمة التشغيل المستخدمة أو البرمجيات من قبل المهاجمين وإلحاق الضرر بالأنظمة والبيانات.

2. مشكلة البحث

تكمن مشكلة البحث الأساسية في الأنشطة التي تستهدف الأنظمة الحاسوبية والشبكات الهامة واستغلال نقاط الضعف مما يشكل التهديدات الإلكترونية التي تتم على البنوك والمصارف ووسائل السغر مطارات وقطارات وحتى قنوات الإعلام وتلحق ضرر كبير وتعطل مصالح أفراد ومؤسسات ودول من خلال الهجمات السيبرانية المدروسة والمستهدفة التي تتم ويمكن تفسيرها على أنها قرصنة وتخريب وإضرار بمصالح الشعوب.

3. تساؤلات البحث

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

4. الهدف من البحث

يهدف البحث إلى التعرف على الخلل (الأعطال) وهي 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.

5. أهمية البحث

تتمثل في مجموعة نقاط هامة ظهرت حديثاً 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 والوقاية من الاختراقات، والتهديدات الإلكترونية، وضمان أمن البيانات والمعلومات وتفادياً لها في المستقبل للتأثير العالمي الكبير.

6. منهجية البحث

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

7. حدود البحث

اقتصر البحث على التعرف بالمخاطر السيبرانية والهجمات الإلكترونية على المؤسسات الحكومية الكبيرة في الدول المتقدمة والثغرات ونقاط الضعف وكيفية إجراء التدابير المناسبة.

- **حدود زمانية:** أجريت الدراسة في بداية يناير 2025.
- **حدود مكانية:** اهتم البحث بالمؤسسات الحكومية والوزارات المهمة بالدول العظمي.

المحور الأول: الجانب النظري للبحث

أولاً: مفهوم الأمن السيبراني:

1. تعريف الأمن السيبراني: (مصطفي، 2023)

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.

2. 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. (حميد، 2020)

International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (2)
IJCI
February 2025
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (2)

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 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 والانتهاكات.

3. الثغرات الأمنية: (البالول، 2021)

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 وتحديد الأعطال أو الانتهاك من خلاله.

ثانياً: الانتهاكات والهجمات الإلكترونية: (حميد، 2020)

1. التقييم والمعالجة.

2. السيطرة 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 المؤسسة.

3. إدارة المخاطر:

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 الإلكترونية "السيبرانية" ومن أهمها: "الترتيب حسب تكرارية التعرض للخطر وشدته: (جلال الدين، 2020)

- المؤسسات المصرفية.
- قطاعات الطيران.
- مؤسسات الرعاية الصحية.
- قطاع البنية التحتية للاتصالات.
- قطاع التأمين.
- قطاع الإعلام والإذاعة.

4. الانتهاكات الحديثة والهجمات السيبرانية:

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

توضيح أمثلة عالمية للأعطال والاختراقات التي حدثت وهي: (الكعبي، 2021)

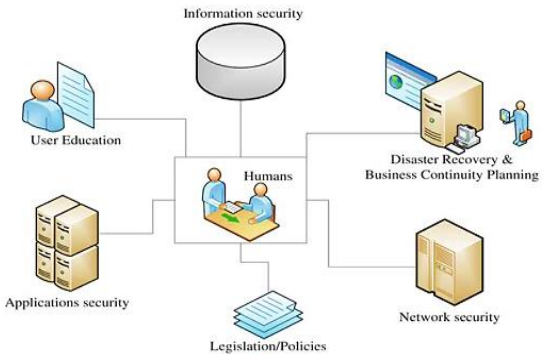
- أعطال في مطارات مجموعة دول وهي مطارات (إسبانيا-ألمانيا-اسكتلندا ومطار أمستردام في هولندا-أمريكا) هجمات سيبرانية.
- قنوات وإذاعات عالمية مثل (انقطاع في إرسال هيئة الإذاعة الأسترالية ومشكلات تقنية ضخمة على مستوى البلاد)، وأيضاً من الفتوات العالمية التي حدثت نفس المشكلة (قناة سكاي نيوز البريطانية تعلن توقف بثها) نفس الخلل.

- التأثيرات التي حدثت بورصة لندن تعلن تأثر خدماتها.
- شركة القطارات البريطانية تعلن عن أعطال في أنظمتها وتلغي جميع رحلات.
- مركز 911 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.

المعالجة لمخاطر الأمن السيبراني تتم من خلال: (الحبسي، 2020)

- 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.
- تجنّب مخاطر الأمن السيبراني: تجنّب الظروف والأحوال التي تنتج عنها تلك المخاطر.
- تحويل مخاطر الأمن السيبراني: نقل تلك المخاطر إلى طرف آخر يتمتع بقدرات أفضل للتعامل معها أو التأمين على الأصول المعلوماتية والتقنية ضد تلك المخاطر.
- تقبّل مخاطر الأمن السيبراني: يكون مستوى تلك المخاطر مقبولاً، لكن يجب مراقبتها باستمرار تحسبًا لأي تغيير.



الشكل (1): يوضح المكونات في الأمن السيبراني - المصدر: (حميد، 2020)

5. 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، واستخدام الأمن السيبراني والمحافظة علي المعلومات في المؤسسات والوزارات الحكومية للدول يتعرض اليوم لمخاطر جمة ومن أهمها محاولات الاختراق السيبراني وهو ما يشكل ضرراً كبيراً 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 الاختراق. (شفيق، 2022)

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

- برمجية خطرة من نوع "drive-by" في أنظمة "ويندوز-10" و"ويندوز-11" يمكن استغلالها في اختراق تلك الأنظمة والوصول إلى بيانات الأجهزة العاملة.
- 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-7" والتي توقفت عن دعمها.
- 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.
- بسبب عدم تطبيق التحديثات الأمنية الدورية patch التي تصدرها شركات نظم التشغيل بشكل دوري لإغلاق الثغرات الأمنية المستجدة.

6. الثغرات ونقاط ضعف في البرمجيات والتطبيقات: (زعاترة، 2023)

أخطر نقاط الضعف في الأمن السيبراني هي البرامج والأنظمة القديمة وعندما لا يتم تحديث البرامج والإجراءات بانتظام، فإنها تصبح عرضة للهجمات ويمكن للمتسللين استغلالها للوصول إلى المعلومات الحساسة أو تثبيت برامج ضارة للحماية من هذه الثغرة الأمنية، لهذا يجب التأكد من تحديث جميع البرامج والأنظمة بانتظام بأحدث التحديثات وخصوصاً الأمان والترقيات الهامة للبرامج والتطبيقات في الحاسب، والبرامج النصية الآلية التي 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.

7. الثغرات ونقاط ضعف في شبكات المؤسسات:

نقاط الضعف والأعطال في الشبكات لأنظمة المؤسسات تتسبب في الهجمات السيبرانية والانتهاكات تتطرق الباحث لمجموعة هامة من هذه الأعطال 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. (Munich, 2014)

8. أنواع نقاط الضعف في الشبكة:

- **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.
- **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 سهلاً للمهاجمين.
- **تعطيل الخدمة:** يمكن أن تعطل الهجمات التي تستهدف نقاط الضعف في الشبكة الخدمات الهامة، مما يسبب وقت التوقف والتأثير على العمليات المصرفية والتجارية. (Emarah, 2007)

International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (2)
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (2)
IJCI
February 2025

شكل (2): يوضح نقاط الضعف في الشبكة - المصدر: (حميد، 2020)

9. هجمات بروتكول الشبكة:

يشير الهجوم 51/1 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 "51/1" من حقيقة أنه لكل 51 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 51/1 هجمات، يمكن استخدام العديد من الاستراتيجيات: (حميد، 2020)

- **اختيار وظيفة تجزئة التشفير:** اختيار وظيفة تجزئة آمنة مع حجم إخراج أكبر يقلل من احتمال الاصطدامات. يتم تبني الخوارزميات مثل SHA-256 أو SHA-3 على نطاق واسع بسبب مقاومتها ضد هجمات الاصطدام.
- **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.

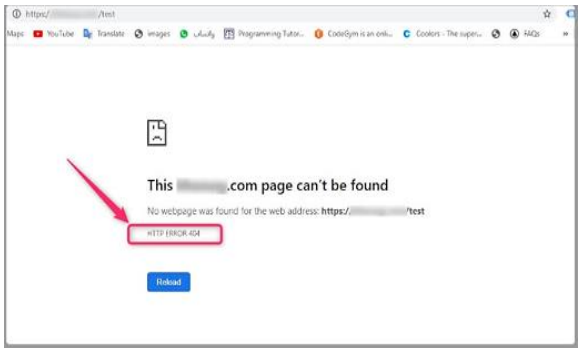
المحور الثاني: محور تطبيقي

يناقش الباحث في هذا المحور نقاط عملية في الجرائم والانتهاكات الإلكترونية والتقنيات والبرامج المساعدة، وتم شرح نقاط الضعف والثغرات ومن ثم الاستفادة من لغات البرمجة في سد هذه الثغرات وإنشاء تطبيق يمنع ويحد من الجريمة الإلكترونية.

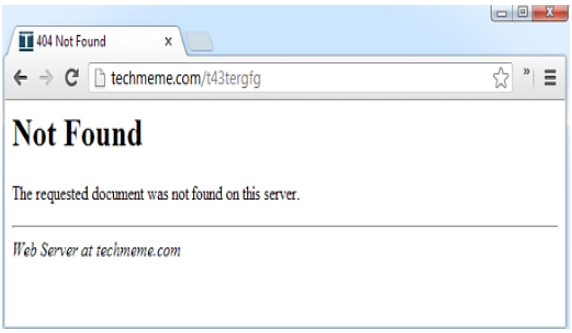
التقنيات والبرامج التي يستخدمها المخترقين أكثر تقدمًا، ومن الضروري التطوير في أشكال دفاعية أكثر قوة، وإن وجود دفاعات تتفاعل مع التهديدات أمرًا غير كافيًا -بل يجب أن تكون تلك الدفاعات استباقية وقادرة على تحديد الهجمات الإلكترونية قبل أن تتسبب في حدوث مشكلات. ومن ملاحظة الباحث أن هناك العديد من نقاط الضعف عند إنشاء التطبيقات وخصوصا "في JavaScript، مثل Cross-Site Scripting (XSS) وCross-Site Request Forgery (CSRF) وإلغاء التسلسل غير الآمن.

تحدث ثغرات برمجة المواقع المتقاطعة عادةً في أجزاء من موقع الويب أو تطبيق الويب حيث يمكن للمستخدمين نشر أو تحميل بياناتهم الخاصة، يتطرق الباحث لعدة نقاط ضعف برمجية في التطبيقات ويوضح حلول وتدابير عملية للتغلب على هذه الثغرات والمشاكل:

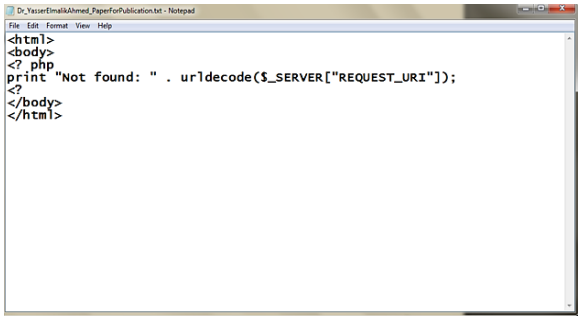
- مشكلة صفحة الخطأ:



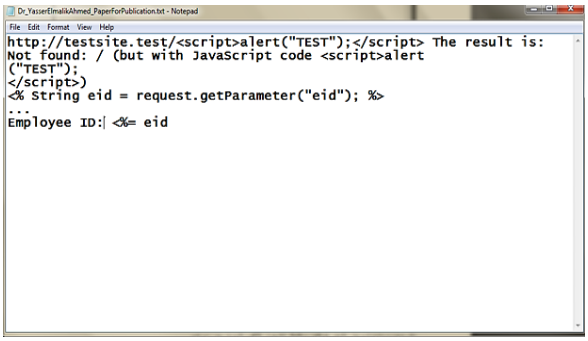
International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (2)
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (2)
IJCI
February 2025



صفحة خطأ 404 التقليدية التي تعرض عنوان URL الذي يحاول المستخدم الوصول إليه وتبلغه بأنه غير موجود.



نظرًا لأن الكود لا يقوم بالتحقق من صحة هذه البيانات REQUEST_URI، فيمكن للمهاجم التلاعب بقيمة هذه البيانات لتنفيذ برنامج نصي ضار ويمكن للمهاجمين الاستخدام على سبيل المثال، لاختطاف ملف تعريف ارتباط الجلسة.



International Journal of Computers and Informatics (IJCI)
Vol. (4), No. (2)
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (4)، العدد (2)
IJCI
February 2025

تكمن خطورة هذه الثغرة في أن المهاجمين قد يقومون بإرسال عنوان URL بالبريد الإلكتروني مع الكود الضار إلى المستخدم وإجباره على النقر فوقه، وبالتالي تشغيل الكود الضار على جهازه.

- الكشف عن XSS واختباره باستخدام Bright:

على الرغم من أن أدوات اختبار أمان التطبيقات الديناميكية (DAST) قادرة على اختبار بعض ثغرات XSS، إلا أنها غالبًا ما تكون محدودة وتنتج نسبة عالية من الإيجابيات الخاطئة.

يمكن لـ Bright فحص التطبيقات تلقائيًا لاختبار نقاط ضعف XSS المنعكسة والمخزنة والمستندة إلى DOM، مما يمنح أقصى قدر من التغطية، ومتكامل بسلاسة عبر خطوط أنابيب التطوير.
يمكن لفرق الهندسة والأمن أن تثق في نتائج Bright، مع التحقق التلقائي من كل اكتشاف XSS تم إجراؤه، دون نتائج إيجابية خاطئة، حتى أن Bright يولد لقطة شاشة لإثبات المفهوم إلى جانب نصائح شاملة صديقة للمطورين لإصلاح المشكلة بسرعة وفي وقت مبكر.
كيفية تعمل Nessus وأدوات الأمان الأخرى الخاصة بفحص المنافذ، من الضروري فهم الخدمات المختلفة (مثل خادم الويب، خادم SMTP، خادم FTP) التي يتم الوصول إليها على خادم بعيد. معظم حركة مرور الشبكة عالية المستوى، مثل البريد الإلكتروني وصفحات الويب وغيرها تصل إلى الخادم عبر بروتوكول عالي المستوى يتم نقله بشكل موثوق عبر دفق TCP، لمنع التدفقات المختلفة من التداخل مع بعضها البعض، يقسم الكمبيوتر اتصاله الفعلي بالشبكة إلى آلاف المسارات المنطقية، التي تسمى المنافذ. لذلك إذا كنت ترغب في التحدث إلى خادم ويب على جهاز معين، فسوف تتصل بالمنفذ رقم 80 (منفذ HTTP القياسي)، ولكن إذا كنت ترغب في الاتصال بخادم SMTP على نفس الجهاز، فستقوم بدلاً من ذلك بالاتصال بالمنفذ #25 مدخلات المستخدم والتحقق من صحته.

- منع مخاطر ثغرات الـ XSS:

1. **Input Validation:** تتمثل الخطوة الأولى لمنع XSS في التحقق من صحة كل مدخلات المستخدم قبل معالجتها بواسطة الخادم.
2. **Output Encoding**: يجب تشفير جميع البيانات التي يوفرها المستخدم قبل عرضها في الـ Browser. سيؤدي هذا إلى منع تنفيذ أي نصوص تم إدخالها.
3. **Content Security Policy:** عبارة عن مجموعة من القواعد التي تحدد المحتوى الذي يُسمح بتحميله بواسطة صفحة ويب. من خلال تنفيذ CSP، يمكنك منع تنفيذ أي نصوص تم حقنها. تشكل

هجمات XSS تهديدًا أمنيًا خطيرًا يمكن أن يؤدي إلى سرقة معلومات حساسة وإجراءات غير مصرح بها نيابة عن الضحية. من المهم فهم الأنواع المختلفة لهجمات XSS التي يمكن استخدامها لاستغلالها. باتباع أفضل الممارسات لمنع ثغرات XSS، يمكن للمطورين المساعدة في حماية تطبيقاتهم والمستخدمين من هذه الأنواع من الهجمات. يوفر Nessus مجموعة متنوعة من أنظمة تحديد درجة الثغرات الأمنية مثل CVSS v4 وEPSS وVPR من Tenable لمساعدتك في تحديد أولوية الثغرات الأمنية الفعالة لجهود الإصلاح. يمكن
استخدام هذه الأداة في أي مكان وتوفر تقارير قابلة للتكوين يمكن لفرق الأمن استخدامها لفهم نقاط الضعف ومعالجتها. الميزات الرئيسية لبرنامج Nessus Professional هي في إنه يوفر الوصول إلى مكتبة تحتوي على أكثر من 185000 مكون إضافي لتحديد الثغرات الأمنية الناشئة وإصلاحها والتحقق من الحماية منها.

يجب تفعيل الوصول إلى المواقع الإلكترونية التي تستخدم HTTP Only التي تقوم بتنبيه المتصفح لمنع كود سكربت من قراءة Cookies بالتالي منع سرقتها.

يوجد في برتوكول HTTP خاصية تسمى قانون المحتوى الأمني CSP[22] الذي يعمل على تحديد الأجزاء التي يُسمَح فيها تنفيذ أوامر كود الجافاسكربت في صفحة الويب، من المهم تفعيل بروتوكول HTTPS هو يعمل على تشفير قنوات الاتصال في الشبكة ويضمن الحماية من هجمات التجسس، ويمكن للمخترق على نفس الشبكة المحلية أن يتعرف على المعلومات الحساسة التي لا يحميها بروتوكول HTTPS يتوجب على جميع المستخدمين التأكد من الروابط قبل الولوج اليها، لمنع واجتناب عمليات اختراق محتملة بطرق احترافية، يكون من الصعب اكتشافها من قبل الضحية.

خاتمة البحث

تناول 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 وإجراء التدابير التقنية والتعرف على الحلول والمعالجات تساعد في الحماية.

يمكن تلخيص أهم النتائج التي توصل إليها الباحث في مجموعة نقاط وهي:

- 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 انتشاراً هي التهديدات الإلكترونية Cyber threats، فقد أصبحت التهديدات الإلكترونية من تؤثر بشكل مباشر علي حياة الناس، حيثُ بات من المهم حصرها وتطوير استراتيجيات التدابير التقنية.
- أصبحت الحاجة إلى الأمن السيبراني أمرًا بالغ الأهمية لحماية البيانات الحساسة، ومن خلال البحث نلاحظ أن هناك تهديدات وانتهاكات عديدة تواجه الأمن السيبراني، وأصبح من الضروري مع تصاعد التهديدات السيبرانية حاجة ملحة لتطوير استراتيجيات وأدوات للحماية من هذه التهديدات، وتكون داعم للحماية والمتابعة بصورة دورية.
- يجب تعزيز حماية أنظمة التشغيل والتقنيات المستخدمة للحد من الهجمات والانتهاكات التي تستهدف الأجهزة الحكومية ومؤسسات الدولة.
- 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 إلكترونية.
- توجد مشكلة في استخدامات البرامج والتطبيقات يجب التعامل مع أمن التطبيقات بحماية البرامج والتطبيقات الخاصة بالشركة أو المؤسسة، لهذا يجب ضمان أن البرمجيات المستخدمة في 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.

وللتخفيف من المخاطر المرتبطة بـ 51/1 هجمات، يوضح البحث مجموعة من الاستراتيجيات (التدابير التقنية والإجرائية للحماية) التي يمكن استخدامها وهي الاستراتيجيات:

- اختيار وظيفة تجزئة التشفير: اختيار وظيفة تجزئة آمنة مع حجم إخراج أكبر يقلل من احتمال الاصطدامات. يتم تبني الخوارزميات مثل SHA-256 أو SHA-3 على نطاق واسع بسبب مقاومتها ضد هجمات الاصطدام.

- تحديثات الخوارزمية العادية: نظراً لاكتشاف نقاط الضعف في وظائف التجزئة مع مرور الوقت، من الأهمية بمكان البقاء في تحديث مع أحدث معايير التشفير والخوارزميات.
- أنظمة الكشف عن التسلل والوقاية (IDPs) تلعب دوراً مهماً في اكتشاف الهجمات وتخفيفها مثل الهجوم 51/1. 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.

كما يجب التوعية بمجموعة من النقاط الهامة المتمثلة في الآتي:

- التوعية بفوائد الأمن السيبراني بوصفه أداة هامة للحفاظ على خصوصية المعلومات، بالإضافة إلى تحسين أمن المعلومات وطريقة حفظ البيانات والمعلومات خاصة بالنسبة للشركات والبنوك والوزارات.
- 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 وتخصص الأمن السيبراني مهم جدًا إذ إنه يشكل مصدر الأمان لكل وسائل التكنولوجيا.
- توعية المؤسسات الحكومية والأفراد بأهمية المتابعة والتطوير واستخدامات البرمجيات الأصلية وعملية التحديث بصورة دورية يُساهم في معرفة أساليب الحماية الضرورية لمعلوماتهم والتي عليهم القيام بها.

يوصي الباحث بمجموعة من التوصيات لمواجهة التحديات في الأمن السيبراني والانتهاكات بصورة مستقبلية تتبني أفضل المهارات لرفع مستوي الأمن للفضاء السيبراني المعلوماتي للدول.

تتلخص توصيات الباحث في الآتي:

- إقامة مؤسسات بحثية داخل وحدات مكافحة الجريمة الإلكترونية تهتم بالأمن الدولي الإلكتروني، والتعامل مع التطورات التقنية التي تؤدي إلى تطور وسائل الجريمة الإلكترونية.
- 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.
- يجب تأمين الأنظمة التي تمكن من الوصول عن بعد والشبكات.

- عدم استخدام البرامج والتطبيقات مجهولة المصدر والمجانية التعامل مع التطبيقات والبرامج الأصلية والعمل على تحديثها بصورة دورية ومستثمرة التفادي لمشاكل الأعطال.
- المشاركة الجماعية للجهات الحكومية، والمنظمات ومراكز الأبحاث والجامعات، في رسم السياسات لمنع الحروب الإلكترونية المستترة والظاهرة، ووضع قوانين وتدابير إجرائية.

جدول (1): قائمة الاختصارات

قائمة الاختصارات ICD / ITKE		
File Transfer Protocol	(FTP)	برتوكول نقل الملفات
Hyper Text Transfer Protocol	(HTTP)	برتوكول نقل النص الفائق
Simple Mail Transfer Protocol	(SMTP)	برتوكول نقل البريد البسيط
Cross-Site Scripting	(XSS)	الثغرات الأمنية
Secure Hash Algorithm	(SHA)	خوارزمية التجزئة الأمنة

المصادر والمراجع

1. إسلام مصطفي. (2023). جريمة إختراق الأمن السيبراني وحماية البيانات والمعلومات. دراسة منشورة.
2. حسين عباس حميد. (2020). نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية. رسالة ماجستير غير منشورة. جامعة الاسكندرية، كلية الحقوق قسم القانون الجنائي، الإسكندرية.
3. عبد الخالق جلال الدين. (2020). الجريمة والانحراف من منظور الخدمة الاجتماعية. الأزاريطة: المكتب الجامعي الحديث.
4. عيسي عبد الله الحبسي. (2020). جرائم البريد الإلكتروني "دراسة مقارنة". رسالة دكتوراه غير منشورة. جامعة المنصورة، كلية الحقوق قسم القانون الجنائي.
5. فرح يحي زعاترة. (2023). التهديدات السيبرانية علي الأمن القومي الأمريكي. رسالة منشورة.
6. منصور ناصر الكعبي. (2021). أثر تكنولوجيا المعلومات علي ظهور الجرائم الإلكترونية، دراسة ميدانية بإمارة أبو ظبي. رسالة دكتوراه غير منشورة. جامعة المنصورة، كلية الآداب قسم علم اجتماع.
7. نور سليمان يوسف يعقوب البالول. (2021). الأحكام الموضوعية لجرائم المعلوماتية. رسالة دكتوراه غير منشورة. جامعة عين شمس، كلية الحقوق قسم القانون الخاص.

8. نوران شفيق. (2022). أثر التهديدات الإلكترونية علي العلاقات الدولية، دراسة في أبعاد الأمن الإلكتروني. الكويت.

المقالات

- بوفاس الشريف وفاطمة الزهراء طلحي، نحو بناء نظم لإدارة حماية المعلومات ايزو 27001 في المؤسسات الجزائرية، المؤتمر الدولي الثاني للذكاء الاقتصادي حول "اليقظة الاستراتيجية ونظم المعلومات في المؤسسة الاقتصادية"، أيام 30/29افريل 2014، جامعة عنابة.
- سمير قلاع ضروسو، الأمن السيبراني الوطني – قراءة في أهم الاستراتيجيات الأمنية لمواجهة الجريمة الإلكترونية بالجزائر، مجلة الرواق للدراسات الاجتماعية والسياسية، مجلد 8، ع 2، سنة 2022.
- سامي محمد بونيف، دور الاستراتيجيات الاستباقية في واجهة الهجمات السيبرانية –الردع السيبراني نموذجاً، المجلة الجزائرية للحقوق والعلوم السياسية، المركز الجامعي أحمد بن يحي الونشريسي، تيسمسيلت، الجزائر، المجلد 4، ع7، جوان 2019.

مواقع إلكترونية

- microsoft.com/ar/security/business/zerotrust/maturity-model-assissment-cool ly/account/1
- http://portal.aridmy/ar-ly/account/ ly/account