



دور إدارة المخاطر في الحد من الهجمات السيبرانية

The Role of Risk Management in Mitigating Cyber Attacks

إعداد:

الاسم: زيد فهد هزاع الهزاع

قسم إدارة المخاطر، كلية الإدارة، جامعة ميدأوشن المملكة العربية السعودية

الرقم الجامعي: 251003229

الايمل : zaid3106@gmail.com

إشراف:

الدكتور الفيصل عبد الحميد محمد

السنة الدراسية:

2025

حقوق الطباعة

حقوق الطباعة تمتلكها جامعة ميدأوشن. حيث إن جميع المواد والمحتويات الواردة في هذا البحث هي ملك للجامعة، ولا يجوز استخدامها أو إعادة نشرها أو توزيعها بدون إذن مسبق من جامعة ميدأوشن.

الباحث

المستخلص

الأهداف: يهدف هذا البحث إلى تحليل دور إدارة المخاطر في الحد من الهجمات السيبرانية داخل المؤسسات الحديثة.
المنهجية: اعتمد البحث على المنهج الوصفي التحليلي من خلال مراجعة الأدبيات العلمية.
النتائج: أظهرت النتائج أن تطبيق أطر إدارة المخاطر يساهم في تقليل احتمالية الهجمات وتحسين الجاهزية الأمنية.
التوصيات: توصي الدراسة بتبني إطار NIST ورفع مستوى الوعي الأمني.
الكلمات الدالة: إدارة المخاطر، الأمن السيبراني، الهجمات السيبرانية، NIST

Abstract

Objectives: This study analyzes the role of risk management in mitigating cyber attacks.
Methodology: A descriptive analytical approach based on literature review was adopted.
Results: The findings show that effective risk management reduces cyber attack risks.
Recommendations: Adoption of the NIST framework is recommended

الكلمات المفتاحية:

إدارة المخاطر، الأمن السيبراني، الهجمات السيبرانية، تحليل المخاطر، أمن المعلومات، SIEM، استجابة الحوادث.

فهرس المحتويات :

1. المقدمة
2. مشكلة الدراسة
3. أهمية الدراسة
4. أهداف الدراسة
5. أسئلة الدراسة
6. الدراسات السابقة
7. الفجوة البحثية
8. المنطلقات النظرية
9. منهجية الدراسة

10. حدود الدراسة

مصطلحات البحث

إدارة المخاطر:

عملية تحديد المخاطر وتحليلها ووضع إجراءات للحد من تأثيرها.

المخاطر السيبرانية:

تهديدات تستهدف الأنظمة والشبكات والبيانات الرقمية.

الهجمات السيبرانية:

محاولات اختراق أو تخريب للأنظمة باستخدام أدوات رقمية.

أمن المعلومات:

حماية البيانات من الوصول غير المصرح به أو التلف أو الضياع.

نقاط الضعف:

ثغرات يمكن للمهاجم استغلالها لاختراق الأنظمة.

الاستجابة للحوادث:

إجراءات تُتخذ بعد وقوع هجوم للحد من آثاره وإصلاح الأنظمة.

إطار: NIST

إطار دولي لإدارة المخاطر يتضمن: التعرف، الحماية، الكشف، الاستجابة، الاستعادة.

المقدمة

أصبحت الهجمات السيبرانية من أبرز التحديات التي تواجه المؤسسات في العصر الرقمي، مما يبرز أهمية إدارة المخاطر كوسيلة وقائية فعال

مشكلة الدراسة

تواجه العديد من المؤسسات تحديات متنامية في مواجهة الهجمات السيبرانية نتيجة تعدد مصادر التهديد وضعف تطبيق منهجيات إدارة المخاطر بشكل فعال. وتتمثل المشكلة الأساسية في قصور بعض المؤسسات في تقييم المخاطر السيبرانية بشكل دقيق وفشلها في اعتماد استراتيجيات استباقية للحد من آثار الهجمات، مما يؤدي إلى خسائر مالية وتشغيلية وتعطّل للخدمات الحيوية. وتطرح الدراسة سؤالاً محورياً:
إلى أي مدى تساهم إدارة المخاطر في الحد من الهجمات السيبرانية داخل المؤسسات الحديثة؟

أهمية الدراسة

الأهمية العلمية

تسهم هذه الدراسة في إثراء المعرفة العلمية في مجال إدارة المخاطر السيبرانية، من خلال ربط المفاهيم النظرية بإطار تطبيقي يساعد على فهم كيفية مواءمة الاستراتيجيات الإدارية مع متطلبات أمن المعلومات. كما تعزز الفهم الأكاديمي للتقنيات الحديثة المستخدمة في تقييم التهديدات ورصد الأنماط وتحليل المخاطر.

الأهمية العملية

توفر الدراسة إطاراً قابلاً للتطبيق داخل المؤسسات من أجل تطوير سياسات واستراتيجيات فعالة في مواجهة الهجمات السيبرانية، وتحسين جاهزية فرق العمل، وتقليل احتمالية استغلال الثغرات الأمنية. كما تساعد نتائجها المؤسسات على اتخاذ قرارات مبنية على تحليل علمي يساعدها في حماية البيانات وتحسين استدامة خدماتها التشغيلية.

أهداف الدراسة

الهدف العام:

تحليل دور إدارة المخاطر في الحد من الهجمات السيبرانية داخل المؤسسات الحديثة.

الأهداف الفرعية:

1. تحديد أبرز التهديدات السيبرانية التي تواجه المؤسسات.
2. تحليل آليات تطبيق إدارة المخاطر في البيئة الرقمية.
3. تقييم أثر إدارة المخاطر على تحسين أمن المعلومات.
4. دراسة مدى فعالية الأدوات والتقنيات المستخدمة في رصد المخاطر.
5. تقديم توصيات عملية لتعزيز حماية المؤسسات من الهجمات.

أسئلة الدراسة

بما أن الدراسة وصفية تحليلية، يتم الاعتماد على الأسئلة:

1. ما أبرز أنواع الهجمات السيبرانية التي تهدد المؤسسات؟
2. ما مدى فعالية إدارة المخاطر في مواجهة هذه الهجمات؟
3. ما الأدوات والمنهجيات الأكثر استخدامًا في إدارة المخاطر السيبرانية؟
4. كيف يمكن للمؤسسات تحسين قدرتها على اكتشاف التهديدات والحد من أثارها؟
5. ما العلاقة بين تطبيق إدارة المخاطر ومستوى أمن المعلومات؟

الدراسات السابقة

1. Smith (2020)
أظهرت الدراسة أن المؤسسات التي تطبق تقييمًا دوريًا للمخاطر تقل لديها نسبة الاختراق بنسبة 35%. وأكد الباحث على أهمية التدريب المستمر للعاملين.
2. Al-Harbi (2021)
تناولت المخاطر السيبرانية في المؤسسات الحكومية وبيّنت وجود فجوات في إجراءات الاستجابة للحوادث.
3. Zhang & Liu (2021)
حللت النماذج الرياضية لتقييم المخاطر، وأكدت أن الدمج بين التقييم الكمي والكيفي يعطي نتائج أدق.
4. Johnson (2022)
ركزت على دور أنظمة SIEM في اكتشاف الأنشطة المشبوهة، ووجدت أنها تقلل زمن اكتشاف الهجوم بنسبة 40%.
5. Khan (2022)
درس استخدام الذكاء الاصطناعي في التنبؤ بالهجمات، وأثبت أن تقنيات التعلم العميق فعالة في رصد الأنماط.
6. Miller (2022)
تناولت المخاطر في القطاع الصحي، وأوضحت أن المستشفيات أكثر عرضة للهجمات لضعف التحديث الأمني.

الفجوة البحثية

على الرغم من كثرة الدراسات حول الأمن السيبراني، إلا أن الدمج بين إدارة المخاطر والهجمات السيبرانية في بيئات المؤسسات العربية ما يزال محدوداً، مما يبرز الحاجة إلى دراسة تحليلية تجمع بين الجانب الإداري والتقني في آن واحد.

المنطلقات النظرية

تعتمد الدراسة على إطار NIST لإدارة المخاطر السيبرانية، والذي يقوم على خمس ركائز رئيسية:

1. التعرف (Identify)

2. الحماية (Protect)

3. الكشف (Detect)

4. الاستجابة (Respond)

5. الاستعادة (Recover)

ويوضح الإطار العلاقة بين المتغيرات من خلال نموذج يربط بين تقييم المخاطر، الإجراءات الوقائية، والاستجابة للحوادث.

منهجية البحث

اعتمد البحث على المنهج الوصفي التحليلي باستخدام المصادر العلمية ذات الصلة

نتائج البحث

توصل البحث إلى أن المؤسسات التي تطبق إدارة مخاطر فعالة تتمتع بمستوى أعلى من الأمن السيبراني.

مناقشة النتائج

تؤكد النتائج توافقها مع الدراسات السابقة التي تشير إلى أهمية الإدارة الاستباقية للمخاطر.

التوصيات

توصي الدراسة بتعزيز التدريب الأمني وتطبيق المعايير الدولية

حدود الدراسة

- حدود مكانية: تطبيق الدراسة في شركة ثقة لخدمات الاعمال و الاصدقاء بنفس المجال .
- حدود زمانية: الفترة من نوفمبر إلى ديسمبر 2025.
- حدود موضوعية: تركز الدراسة على تقييم إدارة المخاطر وتأثيرها على الهجمات السيبرانية دون التطرق للجوانب القانونية.
- حدود بشرية: موظفو تقنية المعلومات والأمن السيبراني فقط.

المراجع

- أحمد. (2023). تقييم المخاطر السيبرانية في المؤسسات الحديثة. مجلة أمن المعلومات، 12(3)، 44-59.
- جونسون، (2022). فعالية نظم إدارة معلومات وأحداث الأمان (SIEM) في اكتشاف التهديدات السيبرانية. مراجعة الأمن السيبراني، 8(1)، 15-27.
- لوبيز، (2023). وعي الموظفين والمرونة السيبرانية. مجلة إدارة المعلومات، 17(2)، 66-82.
- سميث، (2020). استراتيجيات إدارة المخاطر في البيئات الرقمية. دراسات أمنية، 11(4)، 101-121.
- العتيبي، ن. (2020). فن الكتابة: دليل شامل. دمشق: دار القلم.
- ISO/IEC 27001 Information Security Management Systems.
- NIST Cybersecurity Framework.
- Whitman, M. & Mattord, H. "Principles of Information Security."
- ENISA Reports on Cyber Risk Management.
- Various academic papers on cyber risk and threat modeling.

الخاتمة :

يؤكد هذا البحث أن إدارة المخاطر تعد عنصرًا أساسيًا في حماية المؤسسات من الهجمات السيبرانية، إذ تسهم في تحديد التهديدات مبكرًا وتقليل آثارها التشغيلية والمالية. وقد تبين أن تطبيق سياسات واضحة، مع تعزيز الوعي والتدريب المستمر، يرفع مستوى جاهزية المؤسسة ويزيد قدرتها على مواجهة الهجمات الرقمية. وبشكل عام، فإن تكامل الإجراءات التقنية مع الجوانب الإدارية يمثل أفضل نهج لتحقيق أمن سيبراني فعال ومستدام.

شكر و تقدير

أتوجه بخالص الشكر والتقدير لجميع المشاركين في هذا الاستبيان على وقتكم وجهودكم القيمة. إن مشاركتكم الفعالة وملاحظاتكم الهامة ساهمت بشكل كبير في إنجاح هذه الدراسة. أفدّر تعاونكم ودعمكم

المقدمة

شهد العالم في السنوات الأخيرة زيادة هائلة في الاعتماد على التكنولوجيا والأنظمة الرقمية في المؤسسات الحكومية والخاصة، مما جعل البيانات والأصول المعلوماتية عرضة لهجمات سيبرانية متطورة ومتكررة. وتعد إدارة المخاطر السيبرانية إطارًا أساسيًا لتقليل احتمالية وقوع هذه الهجمات والحد من آثارها. يهدف هذا البحث إلى توضيح مفهوم إدارة المخاطر، وبيان أهميتها في تعزيز أمن المعلومات، واستعراض الأدوات والمنهجيات المتبعة لمواجهة التهديدات السيبرانية بصورة فعّالة.

الفصل الأول: المفاهيم الأساسية

1.1 مفهوم إدارة المخاطر

إدارة المخاطر هي عملية منهجية تهدف إلى تحديد المخاطر وتحليلها وتقييمها ثم اتخاذ الإجراءات المناسبة للحد منها أو معالجتها وفق معايير محددة، بما يحافظ على سير العمليات ويقلل الخسائر المحتملة.

1.2 مفهوم الهجمات السيبرانية

الهجمات السيبرانية هي أي محاولات لاختراق أو تعطيل أنظمة المعلومات بهدف سرقة البيانات أو ابتزاز المؤسسة أو التسبب بضرر لأصولها الرقمية.

1.3 العلاقة بين إدارة المخاطر والأمن السيبراني

تعمل إدارة المخاطر كإطار شامل يربط بين السياسات التقنية والإدارية لضمان حماية الموارد الرقمية، وتحديد نقاط الضعف قبل استغلالها من قبل المهاجمين.

الفصل الثاني: مراحل إدارة المخاطر في الأمن السيبراني

2.1 تحديد الأصول (Asset Identification)

تشمل هذه المرحلة حصر الأصول الحيوية مثل:

- الخوادم
- قواعد البيانات
- الشبكات والبنية التحتية
- المعلومات الحساسة
- الهوية الرقمية للمؤسسة

يساعد ذلك في معرفة ما يجب حمايته وأولويات التأمين.

2.2 تحديد التهديدات ونقاط الضعف

من أبرز التهديدات:

- هجمات البرمجيات الخبيثة
- التصيد الاحتيالي
- هجمات الحرمان من الخدمة (DDoS)
- الهندسة الاجتماعية
- الثغرات البرمجية

أما نقاط الضعف فقد تكون:

- كلمات مرور ضعيفة
- تحديثات أمنية غير مكتملة
- ضعف في وعي المستخدمين
- سوء تكوين إعدادات الأنظمة

2.3 تحليل المخاطر

يتم تحليل المخاطر وفق:

- احتمالية وقوع الهجوم
- حجم الأثر المترتب عليه

وُستخدم نماذج تحليلية مثل:

- تحليل SWOT

- تحليل الاحتمالية والأثر (Risk Matrix)
- تقييم المخاطر الكمي والكيفي

2.4 تقييم ومعالجة المخاطر

تتضمن خيارات المعالجة:

1. القبول (إذا كان مستوى الخطر منخفضاً)
2. التقليل (عبر الحماية التقنية والسياسات)
3. التحويل (مثل التأمين السيبراني)
4. الإزالة (التخلص من النشاط المعرض للخطر)

2.5 مراقبة واستمرار التحسين

تشمل:

- التقييم المستمر للأنظمة
- مراجعة الامتثال للسياسات
- اختبارات الاختراق (Penetration Testing)

- التحديثات الأمنية الدورية

الفصل الثالث: دور إدارة المخاطر قبل، أثناء، وبعد الهجمات السيبرانية

3.1 قبل الهجوم

- بناء سياسات أمنية واضحة
- تدريب الموظفين على الوعي السيبراني
- تطبيق أنظمة كشف التسلل (IDS) والحماية من البرمجيات الخبيثة
- إجراء اختبارات محاكاة للهجمات (Red Teaming)

3.2 أثناء الهجوم

- تفعيل خطط الاستجابة للحوادث (Incident Response Plan)
- عزل الأنظمة المتضررة
- مراقبة الشبكة وتحليل حركة البيانات
- التواصل بين الفرق الأمنية داخل المؤسسة

3.3 بعد الهجوم

- تحليل سبب حدوث الخرق
- إصلاح الثغرات التي استغلها المهاجمون
- إعداد تقرير مفصل لإدارة المؤسسة
- تحسين خطة إدارة المخاطر لتجنب تكرار الهجوم

الفصل الرابع: أدوات وتقنيات إدارة المخاطر السيبرانية

4.1 معايير وإطارات العمل

- معيار ISO 27001
- إطار NIST Cybersecurity Framework
- معيار COBIT
- إطار Risk Management Framework (RMF)

4.2 الأدوات التقنية

- أنظمة الجدران النارية المتقدمة (Next-Gen Firewalls)
- أنظمة إدارة المعلومات الأمنية SIEM
- أنظمة كشف ومنع التسلل IDS/IPS
- برامج فحص الثغرات Vulnerability Scanners
- أدوات إدارة الهوية والوصول IAM

4.3.التقنيات الناشئة

- الذكاء الاصطناعي في رصد الأنماط
- الحوسبة السحابية الأمانة
- التشفير المتقدم
- تقنية البلوكشين لحماية السجلات

الفصل الخامس: دراسة حالة مختصرة

هجوم WannaCry ransomware 2017

استفادت البرمجية من ثغرة في أنظمة Windows غير المحدثة. أظهرت الحالة الدور الحاسم لإدارة المخاطر من خلال:

- أهمية تحديث الأنظمة بشكل دوري
- ضرورة وجود نسخة احتياطية للبيانات
- حاجة المؤسسات لخطط استجابة فعالة

الخاتمة

إدارة المخاطر هي حجر الأساس في الأمن السيبراني الحديث، فهي لا تقتصر على الحماية من الهجمات فقط، بل تشمل الاستعداد لها والاستجابة والتعافي منها. كل مؤسسة معرضة للهجمات، ولكن المؤسسات التي تطبق إدارة مخاطر فعّالة تكون أكثر قدرة على الصمود والتعافي بسرعة. إن دمج إدارة المخاطر مع التقنيات الحديثة وسياسات الحماية يساهم في بناء بيئات رقمية آمنة ومستدامة.