

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية مسح التعليم الجامعي: المملكة العربية السعودية

إسم الطالبة: جنان حسين المحيسن

مشروع التخرج-1

كلية الإدارة-جامعة ميداوون

إشراف:

د. منى مصطفى العشري

عضو هيئة التدريس - كلية الإدارة - جامعة ميداوون

الفصل الدراسي الأول- 2024



المحتويات

1	المقدمة.....
3	مشكلة البحث.....
4	أهمية البحث.....
5	اهداف البحث.....
6	فرضيات البحث.....
7	نموذج البحث.....
8	منهجية البحث.....
9	الدراسة الميدانية.....
13	هيكل المشروع.....
14	المراجع.....

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية

المقدمة:

العالم الرقمي :

يشهد العالم اليوم ثورة رقمية هائلة، حيث أصبحت تقنيات المعلومات والاتصالات جزءًا لا يتجزأ من جميع جوانب الحياة، بما في ذلك التعليم. ونتيجة لذلك، أصبحت المؤسسات التعليمية عرضة لمخاطر الأمن السيبراني بشكل متزايد.

مخاطر متزايدة :

تشمل مخاطر الأمن السيبراني التي تواجهها المؤسسات التعليمية ما يلي:

- **الاختراقات الإلكترونية:** يمكن للقراصنة اختراق أنظمة المؤسسات التعليمية وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.
- **البرامج الضارة:** يمكن لنشر البرامج الضارة على أجهزة الكمبيوتر التابعة للمؤسسات التعليمية أن يؤدي إلى تلف البيانات أو تعطيل الخدمات.
- **هجمات الحرمان من الخدمة:** يمكن استخدام هجمات الحرمان من الخدمة لتعطيل مواقع المؤسسات التعليمية على الإنترنت مما يمنع الطلاب والموظفين من الوصول إلى المعلومات والخدمات.
- **التنمر الإلكتروني:** يمكن استخدام الإنترنت لتنمر الطلاب على بعضهم البعض، مما قد يؤدي إلى مشاكل نفسية واجتماعية.

تأثيرات واسعة:

لا تقتصر مخاطر الأمن السيبراني على المؤسسات التعليمية فقط، بل يمكن أن تؤثر أيضًا على :

- **الطلاب :** قد تسرق بياناتهم الشخصية أو تُستخدم لارتكاب جرائم.
- **الموظفون :** قد تُسرق بياناتهم الشخصية أو تستخدم لابتزازهم.
- **المؤسسات التعليمية:** قد تلحق الضرر بسمعتها أو تُجبر على دفع غرامات كبيرة

حاجة ملحة للحلول :

في ظل هذه التحديات، هناك حاجة ملحة لتطوير حلول فعالة لضمان الأمن السيبراني في المؤسسات التعليمية تتضمن بعض الحلول :

- **رفع مستوى الوعي :** نشر الوعي بمخاطر الأمن السيبراني بين الطلاب والموظفين.
- **تطوير البنية التحتية:** الاستثمار في تطوير البنية التحتية لتقنية المعلومات والاتصالات لجعلها أكثر أمانًا.
- **تطبيق تدابير الأمن السيبراني:** تطبيق تدابير الأمن السيبراني الفعالة، مثل جدران الحماية وبرامج مكافحة الفيروسات.
- **التعاون مع الجهات الخارجية:** التعاون مع الجهات الخارجية مثل الشركات الخاصة والحكومة، لتحسين الأمن السيبراني.

المسؤولية المشتركة:

يقع ضمان الأمن السيبراني في المؤسسات التعليمية على عاتق جميع الأطراف المعنية، بما في ذلك :

- **الطلاب:** يجب على الطلاب أن يكونوا على دراية بمخاطر الأمن السيبراني وأن يتخذوا خطوات لحماية أنفسهم.
- **الموظفون:** يجب على الموظفين اتباع ممارسات الأمن السيبراني الجيدة وحماية البيانات الحساسة.
- **المؤسسات التعليمية:** يجب على المؤسسات التعليمية الاستثمار في تطوير حلول الأمن السيبراني وتطبيقها بشكل فعال.

مستقبل التعليم:

يعتمد مستقبل التعليم على قدرة المؤسسات التعليمية على ضمان أمن أنظمتها وبياناتها من خلال العمل معاً، يمكن لجميع الأطراف المعنية خلق بيئة تعليمية آمنة وفعالة للجميع.

مشكلة البحث :

تعد مخاطر الأمن السيبراني من أهم التحديات التي تواجهها المؤسسات التعليمية في المملكة العربية السعودية تشمل هذه المخاطر:

- الاختراقات الإلكترونية :

يمكن للقراصنة اختراق أنظمة المؤسسات التعليمية وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.

- البرامج الضارة:

يمكن لنشر البرامج الضارة على أجهزة الكمبيوتر التابعة للمؤسسات التعليمية أن يؤدي إلى تلف البيانات أو تعطيل الخدمات.

- هجمات الحرمان من الخدمة :

يمكن استخدام هجمات الحرمان من الخدمة لتعطيل مواقع المؤسسات التعليمية على الإنترنت، مما يمنع الطلاب والموظفين من الوصول إلى المعلومات والخدمات.

- التنمر الإلكتروني :

يمكن استخدام الإنترنت لتنمر الطلاب على بعضهم البعض، مما قد يؤدي إلى مشاكل نفسية واجتماعية.

أهمية البحث:

- سيساعد هذا البحث في فهم مخاطر الأمن السيبراني التي تواجهها الجامعات السعودية بشكل أفضل.
- سيساعد هذا البحث في تحديد تدابير الأمن السيبراني التي يجب على الجامعات السعودية تطبيقها.
- سيساعد هذا البحث في التغلب على التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.
- سيساعد هذا البحث في تحسين الأمن السيبراني في الجامعات السعودية، مما سيحمي البيانات الحساسة للطلاب والموظفين.

أسئلة البحث :

- ما هي أهم مخاطر الأمن السيبراني التي تواجهها الجامعات السعودية؟
- ما ما هي تدابير الأمن السيبراني التي تتخذها الجامعات السعودية لحماية أنظمتها وبياناتها ؟
- ما هي التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني ؟
- ما هي أفضل الممارسات لتحسين الأمن السيبراني في الجامعات السعودية؟

اهداف البحث:

- لتحديد مخاطر الامن السيبراني التي يواجهها المؤسسات التعليمية بالمملكة العربية السعودية.
- لتحديد اهم التحديات التي يواجهها المؤسسات التعليمية في المملكة العربية السعودية.
- لاكتشاف الحلول التطويرية لضمان الامن السيبراني المؤسسات التعليمية في المملكة العربية السعودية.

صياغة فرضيات البحث:

١. . فرضيات رئيسية:

- الفرضية الأولى: تواجه الجامعات السعودية مخاطر عالية من الأمن السيبراني.
- الفرضية الثانية: لا تتخذ الجامعات السعودية تدابير كافية لحماية أنظمتها وبياناتها من مخاطر الأمن السيبراني.
- الفرضية الثالثة: هناك العديد من التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.

٢. فرضيات فرعية:

- الفرضية الفرعية الأولى: أكثر مخاطر الأمن السيبراني شيوعاً التي تواجهها الجامعات السعودية هي الاختراقات الإلكترونية.
- الفرضية الفرعية الثانية: لا تمتلك الجامعات السعودية الموارد المالية أو البشرية الكافية لتطبيق تدابير الأمن السيبراني الفعالة.
- الفرضية الفرعية الثالثة: نقص الوعي بمخاطر الأمن السيبراني هو أحد أهم التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.

نموذج البحث:

١. المتغيرات:

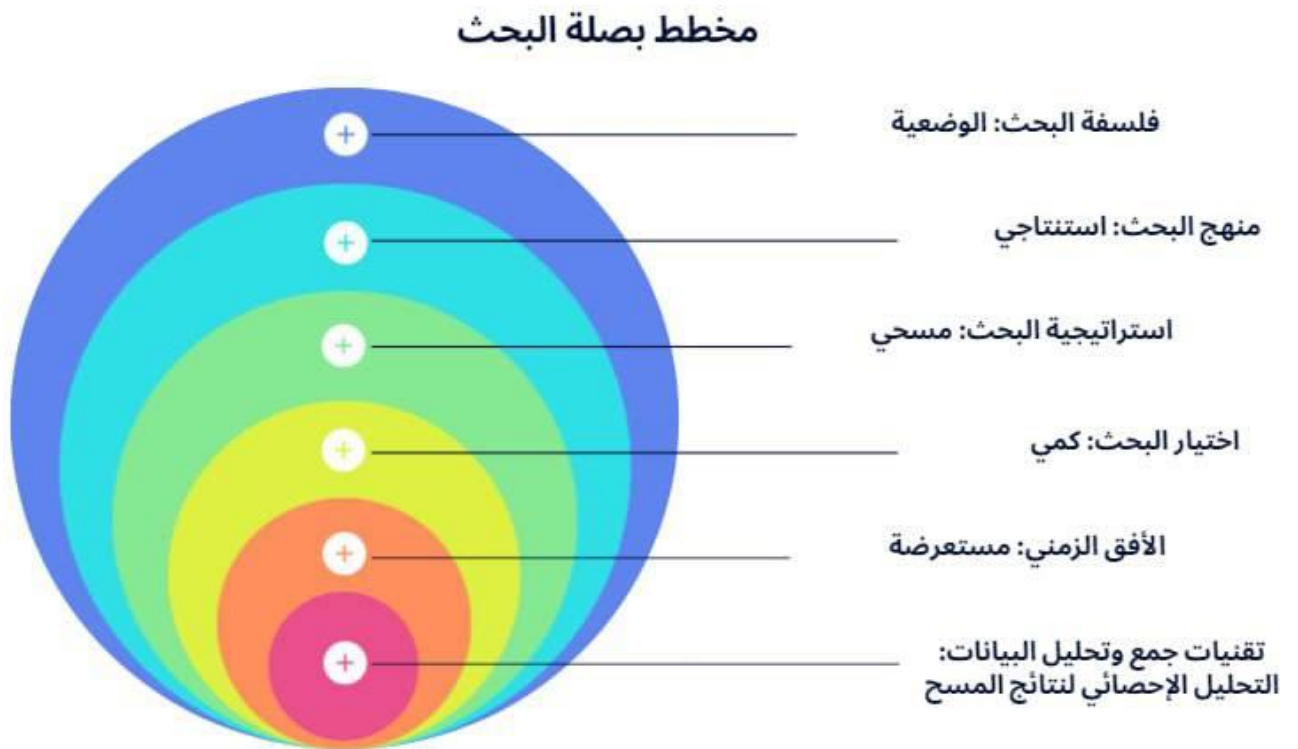
- المتغير المستقل: مخاطر الأمن السيبراني.
- المتغير التابع: تدابير الأمن السيبراني التي تتخذها الجامعات السعودية.
- المتغيرات المتداخلة الموارد المالية والبشرية الوعي بمخاطر الأمن السيبراني، البنية التحتية لتقنية المعلومات والاتصالات.

٢. العلاقات بين المتغيرات:

- العلاقة بين المتغير المستقل والمتغير التابع: تؤثر مخاطر الأمن السيبراني بشكل مباشر على تدابير الأمن السيبراني التي تتخذها الجامعات السعودية.
- العلاقة بين المتغيرات المتداخلة والمتغير التابع: تؤثر المتغيرات المتداخلة على قدرة الجامعات السعودية على تطبيق تدابير الأمن السيبراني.

منهجية البحث:

في هذي الدراسة، سيعتمد الباحث على منهجية البحث التحليلي الوصفي.



الدراسة الميدانية:

١. عنوان المشروع:

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية دراسة حالة التعليم الجامعي في المملكة العربية السعودية

• مدة المشروع:

٦ أشهر

٢. خطوات المشروع:

أ. المرحلة التحضيرية:

- مراجعة الأدبيات ذات الصلة بمخاطر الأمن السيبراني في المؤسسات التعليمية.
- تحديد الجامعات السعودية التي سيتم دراستها.
- تصميم أدوات جمع البيانات.

ب. مرحلة جمع البيانات:

- إجراء مقابلات مع خبراء الأمن السيبراني في الجامعات السعودية.
- تحليل وثائق الجامعات السعودية المتعلقة بالأمن السيبراني.

ت. مرحلة تحليل البيانات:

- تحليل البيانات التي تم جمعها باستخدام التحليل الإحصائي.
- تفسير نتائج التحليل.

ث. مرحلة كتابة التقرير:

- كتابة تقرير نهائي يتضمن نتائج البحث وتوصياته.

٣. المخاطر والتحديات:

- نقص التعاون من قبل الجامعات السعودية.
- صعوبة الحصول على البيانات.
- نقص الموارد المالية والبشرية.

٤. خطة لإدارة المخاطر والتحديات:

- التواصل الفعال مع الجامعات السعودية.
- استخدام أدوات جمع البيانات المختلفة.
- البحث عن مصادر تمويل إضافية.

٥. نتائج المشروع المتوقعة:

- فهم أفضل لمخاطر الأمن السيبراني التي تواجهها الجامعات السعودية.
- توصيات لتحسين الأمن السيبراني في الجامعات السعودية.

٦. الفوائد المتوقعة من المشروع:

- تحسين الأمن السيبراني في الجامعات السعودية.
- حماية البيانات الحساسة للطلاب والموظفين.
- تعزيز الثقة في المؤسسات التعليمية.

٧. خطة لنشر نتائج المشروع:

- نشر التقرير النهائي في مجلات علمية محكمة.
- تقديم نتائج البحث في مؤتمرات علمية.
- مشاركة نتائج البحث مع الجامعات السعودية والجهات الحكومية والقطاع الخاص.

الجدول الزمني للمشروع:

النشاط	المدة
مراجعة الأدبيات	1 شهر
تحديد الجامعات السعودية	1 شهر
تصميم أدوات جمع البيانات	1 شهر
جمع البيانات	2 شهر
تحليل البيانات	1 شهر
كتابة التقرير	1 شهر

هيكل المشروع:

الفصل الأول: الإطار العام للدراسة

الفصل الثاني: الإطار النظري

الفصل الثالث: منهجية البحث

الفصل الرابع: التحليل الإحصائي

الفصل الخامس: المناقشة والخاتمة

المراجع:

كتب:

- إدارة الامن السيبراني في مؤسسات التعليم العالي، فاطمة عبدالله الشبانات، 2021.
- الامن السيبراني وتحدياته في ظل التطورات التقنية، عبدالله بن محمد الحربي، 2022.

مقالات:

- التحديات التي تواجه الامن السيبراني في الجامعات السعودية، مجلة جامعة الملك عبد العزيز، 2023.

تقارير:

- تقييم المخاطر السيبرانية في قطاع التعليم العالي، مركز الامن السيبراني الوطني، 2023.