

تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية
السعودية: استراتيجيات الحماية والتخفيف

إعداد الطالب/ مضاوي محمد المطيري

إشراف/

العام الدراسي:

2024

قائمة المحتويات

3	مقدمة:
5	مشكلة الدراسة:
7	أهمية الدراسة:
12	أهداف الدراسة:
14	تساؤلات الدراسة:
14	فروض الدراسة:
15	الدراسات السابقة:
18	المنطلقات النظرية للدراسة:
20	المنهجية وطرق البحث:
23	أدوات الدراسة:
25	حدود الدراسة:
27	المراجع:

مقدمة:

في ظل التطورات التكنولوجية المتسارعة التي يشهدها العالم اليوم، أصبحت المؤسسات الحكومية أكثر اعتمادًا على الأنظمة الرقمية والتكنولوجيا الحديثة في إدارة عملياتها وتقديم خدماتها. هذا الاعتماد المتزايد على التكنولوجيا يواكبه ارتفاع في مستوى التهديدات السيبرانية التي تستهدف البنية التحتية الحساسة لهذه المؤسسات، مما يجعل الأمن السيبراني قضية محورية تحتاج إلى اهتمام متزايد وإدارة فعالة. في المملكة العربية السعودية، تزايد أهمية هذا الأمر بشكل خاص نظرًا للدور الحيوي الذي تلعبه التكنولوجيا في دعم رؤية 2030، التي تهدف إلى تحقيق تحول رقمي شامل في القطاعات الحكومية والخاصة. ومع هذا التحول، تظهر تحديات جديدة تتعلق بحماية البيانات والمعلومات الحساسة التي تديرها المؤسسات الحكومية، مما يبرز الحاجة إلى استراتيجيات متكاملة لتقييم وإدارة مخاطر الأمن السيبراني (Mishra, 2022).

المؤسسات الحكومية تتعامل يوميًا مع كميات ضخمة من البيانات التي تتضمن معلومات حساسة عن المواطنين، والأمن القومي، والسياسات الحكومية. هذه البيانات ليست فقط قيمة بحد ذاتها، ولكنها أيضًا جزء من بنية تحتية أوسع تضم أنظمة إدارة الهوية، وأنظمة الصحة العامة، والبنية التحتية الحيوية مثل شبكات الطاقة والمياه. تعرض هذه البنية التحتية للخطر يمكن أن يؤدي إلى تداعيات خطيرة على مستوى الدولة ككل، بما في ذلك فقدان الثقة العامة في قدرة الحكومة على حماية مواطنيها وإدارة عملياتها بكفاءة. لذلك، يُعد تقييم المخاطر السيبرانية في هذا السياق أمرًا حيويًا لضمان استمرارية العمل الحكومي وحماية الأمن القومي (Borky, 2018).

تقييم المخاطر السيبرانية هو عملية معقدة تشمل العديد من العناصر، بدءًا من تحديد الأصول القيمة التي تحتاج إلى حماية، وصولًا إلى تحليل التهديدات المحتملة وتحديد نقاط الضعف التي يمكن أن تستغلها هذه التهديدات. في المؤسسات الحكومية، يتطلب هذا التقييم فهمًا دقيقًا للبنية التحتية الرقمية المستخدمة، والتي غالبًا ما تكون معقدة ومتنوعة. تشمل هذه البنية التحتية أنظمة مختلفة تتراوح بين قواعد البيانات الكبيرة إلى تطبيقات الهاتف المحمول التي تُستخدم لتقديم الخدمات العامة. كل مكون من هذه المكونات يمثل نقطة ضعف محتملة يمكن أن تُستغل في حال لم يتم تأمينها بشكل صحيح.

بعد تحديد الأصول ونقاط الضعف، يجب على المؤسسات الحكومية تقدير التأثير المحتمل لأي هجوم سيبراني قد يحدث. هذا يتضمن تحليل السيناريوهات المختلفة التي قد تواجهها المؤسسة، مثل هجمات الحرمان من

الخدمة (DDoS)، أو اختراق البيانات الحساسة، أو هجمات الفدية التي قد تؤدي إلى تعطيل الأنظمة الحيوية. من خلال هذا التحليل، يمكن للمؤسسات تحديد أولوياتها الأمنية والتركيز على حماية الأصول الأكثر أهمية. على سبيل المثال، قد تكون بيانات المواطنين وأنظمة الأمن القومي من بين الأصول التي تتطلب أعلى مستوى من الحماية، وبالتالي يجب توجيه الموارد الأمنية لحمايتها بشكل استباقي (Cremer, 2022).

بمجرد تحديد الأولويات، يأتي دور تطبيق استراتيجيات الحماية التي تهدف إلى تقليل المخاطر إلى أدنى حد ممكن. تعتمد هذه الاستراتيجيات على مزيج من الإجراءات التقنية والتنظيمية التي تعمل معًا لتشكيل دفاعات متعددة الطبقات ضد التهديدات السيبرانية. الإجراءات التقنية تشمل تقنيات مثل التشفير الذي يحمي البيانات أثناء نقلها وتخزينها، وأنظمة مراقبة الشبكات التي تكشف عن الأنشطة المشبوهة في الوقت الفعلي، مما يسمح بالاستجابة السريعة لأي تهديد. بالإضافة إلى ذلك، تأتي الحاجة إلى تطبيق سياسات إدارة الهوية والوصول بصرامة، لضمان أن الأفراد الذين يصلون إلى البيانات الحساسة هم فقط من لديهم التصريح المناسب لذلك، مع استخدام تقنيات متقدمة مثل المصادقة متعددة العوامل لتعزيز الأمان.

فيما يتعلق بالإجراءات التنظيمية، تلعب التوعية والتدريب دورًا محوريًا في حماية المؤسسات الحكومية من المخاطر السيبرانية. العامل البشري غالبًا ما يكون الحلقة الأضعف في سلسلة الأمن السيبراني، حيث يمكن أن تؤدي الأخطاء البشرية إلى فتح الباب أمام الهجمات. لذلك، يجب على المؤسسات الحكومية الاستثمار في تدريب موظفيها بانتظام على أفضل الممارسات الأمنية، وتعريفهم بالتهديدات الشائعة مثل هجمات التصيد الاحتيالي. هذه الجهود التوعوية يجب أن تكون مستمرة، نظرًا لأن طبيعة التهديدات السيبرانية تتطور باستمرار، مما يستدعي تحديث المعلومات والتدابير الأمنية بشكل منتظم (Akter, 2022).

على الرغم من كل التدابير الوقائية، قد تحدث هجمات سيبرانية، ولهذا السبب يجب أن تكون المؤسسات الحكومية مجهزة بخطط استجابة فعالة للحوادث. هذه الخطط تهدف إلى التخفيف من تأثير الهجمات واستعادة العمليات بشكل سريع وفعال. جزء أساسي من هذه الخطط يتضمن تحديد الإجراءات الفورية التي يجب اتخاذها عند اكتشاف تهديد، مثل عزل الأنظمة المتضررة والبدء في عملية التحقيق الجنائي الرقمي لتحديد مصدر الهجوم وكيفية حدوثه. بالإضافة إلى ذلك، يجب أن تتضمن الخطط آليات لاستعادة البيانات والأنظمة المتضررة، بما في ذلك استخدام النسخ الاحتياطية المحمية بشكل جيد لضمان عدم فقدان المعلومات الحيوية.

كما يجب أن تكون خطط الاستجابة ديناميكية، قادرة على التكيف مع التغيرات المستمرة في طبيعة التهديدات. هذا يتطلب من المؤسسات الحكومية إجراء اختبارات دورية لخطط الاستجابة وتحديثها بناءً على نتائج هذه الاختبارات والتغيرات في البيئة الأمنية. كما يجب أن تشمل الخطط تدريبات منتظمة للفرق المتخصصة في الاستجابة للحوادث، لضمان جاهزيتها في مواجهة التهديدات الحقيقية بكفاءة وسرعة.

مع التطور المستمر في تقنيات الهجمات السيبرانية، يجب على المؤسسات الحكومية في المملكة العربية السعودية أن تبقى يقظة ومتقدمة في استخدام أحدث التقنيات الدفاعية. التعاون مع وكالات الأمن السيبراني المحلية والدولية يُعدّ عنصراً أساسياً في مواجهة التهديدات المعقدة. هذا التعاون يمكن أن يشمل تبادل المعلومات حول التهديدات السيبرانية والاكتشافات الجديدة، وكذلك الاستفادة من الخبرات العالمية في تطوير استراتيجيات الدفاع السيبراني. علاوة على ذلك، الابتكار في استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي يمكن أن يعزز قدرة المؤسسات على الكشف عن التهديدات والتعامل معها قبل أن تتسبب في أضرار جسيمة (Giannaros, 2023).

يمثل تقييم وإدارة مخاطر الأمن السيبراني في المؤسسات الحكومية عملية مستمرة ومعقدة تتطلب التزاماً طويل الأمد واستثماراً كبيراً في الموارد والتكنولوجيا. من خلال تطبيق استراتيجيات الحماية الشاملة وتطوير خطط استجابة فعالة، يمكن للمؤسسات الحكومية تعزيز قدراتها الدفاعية بشكل مستمر وتقليل المخاطر السيبرانية، مما يضمن استمرارية العمليات الحكومية وحماية المعلومات الحساسة من أي تهديدات محتملة. هذه الجهود ليست مجرد استجابة للتحديات الحالية، بل هي أيضاً استثمار في المستقبل، حيث يصبح الأمن السيبراني جزءاً لا يتجزأ من البنية التحتية الوطنية واستقرارها (Dawodu, 2023).

مشكلة الدراسة:

• التعقيد والتطور السريع للبنية التحتية الرقمية

تعتمد المؤسسات الحكومية في المملكة العربية السعودية بشكل متزايد على التكنولوجيا الرقمية لإدارة عملياتها وتقديم خدماتها. يشمل هذا الاعتماد العديد من الأنظمة الشبكية المعقدة، والتطبيقات البرمجية المتقدمة، والخدمات السحابية. تتطلب هذه البنية التحتية الرقمية، نظراً لتعقيدها وتنوعها، إجراءات أمنية متقدمة لحمايتها

من التهديدات السيبرانية. المشكلة الأساسية هنا هي القدرة على التقييم الشامل لجميع جوانب هذه البنية التحتية وتحديد نقاط الضعف المحتملة التي يمكن أن تستغلها الجهات المهاجمة. بالإضافة إلى ذلك، يستدعي هذا الأمر تحديثاً مستمراً للبنية التحتية الأمنية لتواكب التطورات التكنولوجية السريعة وتضمن حماية مستدامة للبيانات والأنظمة الحيوية.

• التهديدات السيبرانية المعقدة والمتطورة

تتطور التهديدات السيبرانية بوتيرة سريعة وباستخدام تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي، مما يزيد من تعقيد التحديات التي تواجهها المؤسسات الحكومية. تشمل هذه التهديدات هجمات الحرمان من الخدمة (DDoS)، وهجمات الفدية، واختراق البيانات الحساسة. كل نوع من هذه الهجمات يتطلب استراتيجيات دفاعية مختلفة ومتكاملة لضمان الحماية الشاملة. التحدي الرئيسي هنا يكمن في القدرة على التنبؤ بهذه التهديدات والاستعداد لها بفعالية. تتطلب هذه المهمة تحليلاً دقيقاً لنماذج الهجمات السيبرانية وتطوير حلول مبتكرة تستطيع التعامل مع التهديدات في الوقت الفعلي، مما يضمن حماية الأنظمة الحيوية وتقليل الأضرار المحتملة.

• دور العامل البشري في الأمن السيبراني

يشكل العامل البشري حلقة ضعف رئيسية في سلسلة الأمن السيبراني. غالباً ما يكون الإهمال أو الافتقار إلى الوعي الأمني السبب الرئيسي وراء نجاح العديد من الهجمات السيبرانية. لذا، يتعين على المؤسسات الحكومية في المملكة العربية السعودية التركيز على تدريب الموظفين وتوعيتهم بأهمية الأمن السيبراني. تشمل هذه البرامج التوعوية تدريب الموظفين على كيفية التعرف على التهديدات الشائعة مثل هجمات التصيد الاحتيالي، والتعامل الصحيح مع البيانات الحساسة. بالإضافة إلى ذلك، يجب أن تشمل هذه البرامج تدريبات دورية وتحديثات مستمرة لضمان مواكبة الموظفين للتطورات الجديدة في مجال التهديدات السيبرانية وكيفية التصدي لها.

• السياسات الأمنية والإجراءات الوقائية

تتطلب حماية البيانات الحساسة في المؤسسات الحكومية تطوير سياسات أمنية قوية وإجراءات حماية متعددة الطبقات. تشمل هذه السياسات استخدام تقنيات التشفير لحماية البيانات أثناء نقلها وتخزينها، وتطبيق أنظمة إدارة الهوية والوصول للتحكم في من يمكنه الوصول إلى المعلومات الحساسة. يعتبر وضع خطط استجابة فعالة للحوادث السيبرانية جزءاً أساسياً من هذه السياسات. يجب أن تشمل هذه الخطط تحديد الإجراءات الفورية التي يجب

اتخاذها عند اكتشاف تهديد سيبراني، وتطوير آليات لاستعادة البيانات والأنظمة المتضررة بسرعة لضمان استمرارية العمليات الحيوية. كما يجب أن تكون هذه السياسات ديناميكية وقابلة للتحديث بشكل مستمر لمواكبة التطورات السريعة في مجال التهديدات السيبرانية.

• التعاون والتنسيق بين الجهات المسؤولة

يعتبر التعاون والتنسيق بين مختلف الجهات المسؤولة عن الأمن السيبراني في المؤسسات الحكومية أمراً حيوياً لمواجهة التهديدات السيبرانية بفعالية. يتطلب التصدي للتهديدات السيبرانية تعاوناً وثيقاً بين المؤسسات الحكومية المختلفة، وكذلك التعاون مع القطاع الخاص والوكالات الدولية المتخصصة في الأمن السيبراني. يبرز هنا التحدي في توحيد الجهود وتبادل المعلومات حول التهديدات والتقنيات الدفاعية بين جميع الأطراف المعنية. لذلك، يجب تطوير آليات فعالة للتعاون والتنسيق، بما في ذلك إنشاء مراكز عمليات أمنية مشتركة، وتنظيم تدريبات ومحاكاة دورية للتعامل مع التهديدات السيبرانية، وتبادل المعلومات حول الحوادث والتطورات الجديدة في مجال التهديدات السيبرانية.

• التوازن بين التحول الرقمي والأمن السيبراني

تواجه المؤسسات الحكومية تحدياً كبيراً في تحقيق التوازن بين التحول الرقمي وأمن البنية التحتية الرقمية. التحول الرقمي يعد هدفاً استراتيجياً ضمن رؤية 2030، حيث يسعى إلى تحسين الكفاءة والإنتاجية وتعزيز الابتكار في القطاع الحكومي. ومع ذلك، يجب أن يتم هذا التحول بحذر شديد مع الأخذ في الاعتبار جميع التهديدات الأمنية المحتملة. يتطلب هذا التوازن نهجاً متكاملًا يشمل تقييم المخاطر، وتطبيق استراتيجيات الحماية الفعالة، وضمان استمرارية العمليات حتى في حال حدوث هجمات سيبرانية. يتطلب هذا النهج أيضاً تحديث السياسات والإجراءات الأمنية بشكل دوري لتواكب التغيرات السريعة في البيئة الرقمية وضمان حماية مستدامة للبنية التحتية الرقمية.

أهمية الدراسة:

✓ أهمية الدراسة العلمية

تعتبر الدراسة حول تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية ذات أهمية علمية بالغة لأسباب متعددة تتعلق بأثرها على مجالات متعددة تشمل تطوير المعرفة النظرية، وتحسين الممارسات العملية، وتعزيز السياسات والاستراتيجيات الأمنية.

• تعزيز المعرفة النظرية في مجال الأمن السيبراني

تسهم هذه الدراسة بشكل كبير في إثراء المعرفة النظرية المتعلقة بالأمن السيبراني من خلال تقديم تحليل متعمق وشامل للمخاطر التي تواجه المؤسسات الحكومية. تعتمد هذه الدراسة على نماذج وأساليب علمية لتحليل وتقييم المخاطر، مما يضيف إلى الأدبيات العلمية الحالية في هذا المجال. من خلال توسيع قاعدة المعرفة النظرية، تتيح الدراسة للباحثين والأكاديميين فهمًا أفضل للتهديدات السيبرانية وكيفية تقييمها بطرق علمية دقيقة. كما تسهم في تطوير مفاهيم ونظريات جديدة تتعلق بالأمن السيبراني، مما يمكن أن يكون له تأثير كبير على الأبحاث المستقبلية في هذا المجال الحيوي.

• تطوير استراتيجيات الحماية والتخفيف

تلعب هذه الدراسة دورًا حيويًا في تطوير استراتيجيات فعالة للحماية والتخفيف من المخاطر السيبرانية. من خلال التحليل الدقيق لنقاط الضعف والثغرات في الأنظمة الحكومية، يمكن للدراسة تقديم توصيات علمية مبنية على الأدلة حول كيفية تحسين البنية التحتية الأمنية. تساهم هذه التوصيات في تحسين الإجراءات الوقائية وتطوير سياسات أمنية متقدمة تضمن حماية البيانات الحساسة والمعلومات الحيوية. كما تقدم حلولًا مبتكرة لمواجهة التهديدات المتطورة، مما يعزز من قدرة المؤسسات الحكومية على التصدي للهجمات السيبرانية بشكل فعال. تطبيق هذه الاستراتيجيات المبنية على أسس علمية يساهم في تقليل الخسائر المحتملة وتحقيق أمان معلوماتي أعلى.

• تحسين الممارسات العملية والتطبيقية

تعتبر هذه الدراسة أداة قيمة لتحسين الممارسات العملية والتطبيقية في مجال الأمن السيبراني داخل المؤسسات الحكومية. من خلال تقديم أمثلة عملية ودراسات حالة حول كيفية تطبيق استراتيجيات الحماية والتخفيف بشكل فعال، تساعد الدراسة على ترجمة النظريات العلمية إلى ممارسات فعلية يمكن اعتمادها وتنفيذها. تعزز هذه الدراسة القدرة على تقييم فعالية التدابير الأمنية المتبعة وتحديد المجالات التي تحتاج إلى تحسين. بالتالي، تسهم في رفع مستوى الكفاءة والأمان في العمليات الحكومية اليومية، مما ينعكس بشكل إيجابي على جودة الخدمات المقدمة للمواطنين.

• دعم السياسات والاستراتيجيات الوطنية

تلعب هذه الدراسة دورًا محوريًا في دعم السياسات والاستراتيجيات الوطنية المتعلقة بالأمن السيبراني في المملكة العربية السعودية. تقدم الدراسة بيانات وتحليلات دقيقة يمكن استخدامها من قبل صناع القرار لتطوير سياسات أمنية متكاملة وفعالة. كما تسهم في صياغة استراتيجيات وطنية تأخذ في الاعتبار التهديدات السيبرانية المتزايدة وتعمل على تعزيز القدرة على مواجهتها. هذه الدراسة توفر إطارًا علميًا لصياغة القوانين واللوائح التي تهدف إلى حماية البنية التحتية الحيوية للدولة وضمان استمرارية الأعمال في مواجهة التحديات السيبرانية المتطورة.

• تعزيز التوعية والتعليم في مجال الأمن السيبراني

تساهم الدراسة في تعزيز التوعية والتعليم في مجال الأمن السيبراني من خلال تقديم معلومات قيمة حول المخاطر والإجراءات الوقائية. يمكن استخدام نتائج الدراسة لتطوير برامج تعليمية وتدريبية تهدف إلى رفع مستوى الوعي بين الموظفين الحكوميين وتعزيز فهمهم لأهمية الأمن السيبراني. كما يمكن أن تكون أساسًا لتطوير مناهج دراسية في الجامعات والمؤسسات الأكاديمية، مما يسهم في إعداد جيل جديد من المتخصصين في الأمن السيبراني يتمتعون بالمعرفة والمهارات اللازمة لحماية الأنظمة الرقمية.

• تشجيع البحث والتطوير

تشجع هذه الدراسة على البحث والتطوير المستمر في مجال الأمن السيبراني من خلال تحديد الثغرات والمجالات التي تحتاج إلى مزيد من البحث. تفتح الدراسة آفاقًا جديدة للباحثين لاستكشاف حلول مبتكرة لمشكلات الأمن السيبراني وتطوير تقنيات جديدة لتحسين الحماية والتخفيف. كما تحفز الشركات والمؤسسات التقنية على الاستثمار في تطوير منتجات وخدمات أمنية متقدمة تلبي احتياجات المؤسسات الحكومية وتعزز من قدرتها على التصدي للتهديدات المتزايدة.

تعد هذه الدراسة حول تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية ذات أهمية علمية كبيرة، لما تقدمه من إسهامات في تعزيز المعرفة النظرية، وتطوير استراتيجيات الحماية، وتحسين الممارسات العملية، ودعم السياسات الوطنية، وتعزيز التوعية والتعليم، وتشجيع البحث والتطوير. تساهم هذه الدراسة في بناء منظومة أمنية متكاملة وقادرة على مواجهة التحديات السيبرانية المعقدة، مما يضمن حماية الأنظمة الحكومية واستمرارية الخدمات العامة بكفاءة وأمان.

✓ أهمية الدراسة العملية

تتجلى الأهمية العملية لدراسة "تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية: استراتيجيات الحماية والتخفيف" من خلال تأثيرها المباشر والملموس على الواقع العملي والإجراءات التنفيذية في مجال الأمن السيبراني. تغطي هذه الأهمية عدة جوانب حيوية تشمل تحسين مستوى الأمان المعلوماتي، تعزيز الجاهزية والاستجابة للحوادث السيبرانية، تحسين الكفاءة التشغيلية، وتعزيز التعاون بين المؤسسات المختلفة.

• تحسين مستوى الأمان المعلوماتي

تُعتبر هذه الدراسة أداة أساسية لتحسين مستوى الأمان المعلوماتي في المؤسسات الحكومية. من خلال التقييم الشامل للمخاطر السيبرانية وتحديد نقاط الضعف والثغرات في الأنظمة الحالية، يمكن لهذه الدراسة أن تساهم في وضع استراتيجيات حماية فعالة تستند إلى البيانات والتحليلات الدقيقة. يعد تطوير بروتوكولات أمان مخصصة لكل مؤسسة حكومية جزءاً من هذا التحسين، حيث تأخذ هذه البروتوكولات في الاعتبار الاحتياجات الفريدة لكل مؤسسة وتساعد على حماية بياناتها الحيوية من التهديدات المتزايدة. كما أن تنفيذ التوصيات الواردة في الدراسة يمكن أن يقلل من احتمالية حدوث اختراقات أمنية كبيرة، مما يعزز الثقة في البنية التحتية الرقمية للحكومة.

• تعزيز الجاهزية والاستجابة للحوادث السيبرانية

تساهم هذه الدراسة بشكل كبير في تعزيز الجاهزية والاستجابة للحوادث السيبرانية. من خلال تحليل سيناريوهات الهجوم المحتملة ووضع خطط استجابة تفصيلية، تُمكن هذه الدراسة المؤسسات الحكومية من التصرف بسرعة وفعالية عند وقوع هجمات سيبرانية. تتضمن هذه الخطط إجراءات محددة يجب اتباعها في حال اكتشاف تهديد، مما يقلل من الوقت المستغرق للتعافي ويحد من الأضرار المحتملة. بالإضافة إلى ذلك، يمكن استخدام نتائج الدراسة لتطوير تدريبات دورية ومحاكاة لحوادث سيبرانية، مما يساهم في تحسين كفاءة الفرق الأمنية وزيادة وعي الموظفين بكيفية التعامل مع المواقف الطارئة.

• تحسين الكفاءة التشغيلية

يمكن أن تؤدي استراتيجيات الحماية والتخفيف المستمدة من هذه الدراسة إلى تحسين الكفاءة التشغيلية للمؤسسات الحكومية. من خلال تطبيق إجراءات أمان أكثر فعالية وتجنب الانقطاعات الناتجة عن الهجمات السيبرانية، يمكن للمؤسسات الحفاظ على استمرارية الأعمال وتقديم الخدمات العامة بشكل سلس ودون تأخير. بالإضافة إلى ذلك، يؤدي تقليل عدد الحوادث السيبرانية إلى تقليل النفقات المرتبطة بإصلاح الأضرار واستعادة

البيانات، مما يتيح توجيه الموارد بشكل أكثر كفاءة نحو المبادرات الأخرى. كما أن الكفاءة التشغيلية المعززة تساهم في تحقيق أهداف رؤية 2030 التي تسعى إلى تحسين جودة الخدمات الحكومية وتعزيز الاعتماد على التكنولوجيا الرقمية.

• تعزيز التعاون بين المؤسسات المختلفة

تلعب هذه الدراسة دورًا مهمًا في تعزيز التعاون بين المؤسسات الحكومية المختلفة وكذلك بين الحكومة والقطاع الخاص. من خلال توفير إطار عمل مشترك لتقييم المخاطر وتطوير استراتيجيات الحماية، يمكن للمؤسسات تبادل المعلومات والخبرات بشكل أكثر فعالية. يعزز هذا التعاون من القدرة على التصدي للتهديدات السيبرانية المشتركة ويخلق بيئة أكثر أمانًا لجميع الأطراف المعنية. كما يمكن أن تساهم هذه الدراسة في إنشاء شبكات تعاون محلية ودولية لمشاركة أفضل الممارسات وأحدث التقنيات في مجال الأمن السيبراني، مما يعزز من مستوى الأمان العام ويقلل من التهديدات التي قد تواجه المؤسسات الحكومية.

• المساهمة في وضع سياسات وتشريعات أكثر فعالية

من الجوانب العملية الهامة لهذه الدراسة هي مساهمتها في وضع سياسات وتشريعات أكثر فعالية في مجال الأمن السيبراني. توفر الدراسة بيانات وتحليلات يمكن استخدامها كأدلة لتطوير أو تحديث السياسات الأمنية. تساهم هذه السياسات في إنشاء بيئة تنظيمية تضمن الامتثال لمعايير الأمن السيبراني وتحفز على تطبيق أفضل الممارسات. كما تساهم في تحديد الأدوار والمسؤوليات بوضوح بين مختلف الجهات المعنية، مما يعزز من الفعالية والانسجام في تنفيذ الإجراءات الأمنية.

• تعزيز الوعي والتدريب المستمر

تلعب الدراسة دورًا حيويًا في تعزيز الوعي بأهمية الأمن السيبراني وتوفير التدريب المستمر للموظفين في المؤسسات الحكومية. من خلال تسليط الضوء على المخاطر المحتملة والإجراءات الوقائية، تساعد الدراسة على رفع مستوى الوعي بين الموظفين بأهمية حماية البيانات والتصرف بشكل صحيح عند مواجهة تهديدات سيبرانية. كما يمكن أن تكون نتائج الدراسة أساسًا لتطوير برامج تدريبية متقدمة تهدف إلى تعزيز مهارات الموظفين وتحديث معارفهم بانتظام لمواكبة التغيرات السريعة في مجال التهديدات السيبرانية.

• دعم الاقتصاد الرقمي

تساهم هذه الدراسة بشكل غير مباشر في دعم الاقتصاد الرقمي بالمملكة العربية السعودية. من خلال تعزيز الأمان المعلوماتي، تزيد الثقة في الخدمات الحكومية الرقمية، مما يشجع على تبني التكنولوجيا الرقمية بشكل أوسع. هذا الدعم يساهم في تحقيق أهداف رؤية 2030 التي تسعى إلى تنويع الاقتصاد وزيادة الاعتماد على الاقتصاد الرقمي. كما أن حماية البيانات والمعلومات الحكومية بشكل فعال يعزز من جاذبية المملكة للاستثمارات الأجنبية، حيث يشكل الأمان السيبراني عاملاً حاسماً في قرارات المستثمرين.

أهداف الدراسة:

تهدف هذه الدراسة إلى معالجة واحدة من أهم القضايا المعاصرة التي تواجه المؤسسات الحكومية في المملكة العربية السعودية، وهي تقييم مخاطر الأمن السيبراني ووضع استراتيجيات فعالة للحماية والتخفيف. يتطلب تحقيق هذا الهدف الرئيسي تحليلاً دقيقاً للمخاطر الحالية، وتحديد الثغرات الأمنية، ووضع خطط شاملة لمواجهتها. يتفرع من هذا الهدف الرئيسي مجموعة من الأهداف الفرعية التي تساعد في تحقيق رؤية متكاملة وشاملة للأمن السيبراني في القطاع الحكومي.

✓ الهدف الرئيسي

- تقييم شامل لمخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية وتطوير استراتيجيات فعالة للحماية والتخفيف من هذه المخاطر.

✓ الأهداف الفرعية

- تحليل الوضع الحالي للأمن السيبراني في المؤسسات الحكومية.
- تهدف هذه الدراسة إلى إجراء تحليل دقيق للوضع الحالي للأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. يتضمن ذلك تقييم البنية التحتية الأمنية الموجودة، وفحص السياسات والإجراءات المتبعة، وتحديد مستوى الوعي بأهمية الأمن السيبراني بين الموظفين. من خلال هذا التحليل، يمكن تحديد نقاط القوة والضعف في الأنظمة الحالية وتوجيه الجهود نحو المجالات التي تحتاج إلى تحسين.
- تحديد التهديدات السيبرانية الرئيسية التي تواجه المؤسسات الحكومية.

يركز هذا الهدف الفرعي على تحديد التهديدات السيبرانية الأكثر شيوعًا وخطورة التي تواجه المؤسسات الحكومية. يشمل ذلك تحليل أنواع الهجمات الشائعة مثل الهجمات بالبرمجيات الخبيثة، وهجمات التصيد، وهجمات الفدية، وتحديد مصادر هذه التهديدات سواء كانت من جهات داخلية أو خارجية. يساعد تحديد هذه التهديدات على توجيه الجهود الأمنية بشكل أكثر فعالية وتركيز الموارد على الحماية من التهديدات الأكثر احتمالاً.

— تقييم تأثير الهجمات السيبرانية على العمليات الحكومية.

يتضمن هذا الهدف الفرعي دراسة تأثير الهجمات السيبرانية على العمليات الحكومية المختلفة، بما في ذلك تأثيرها على تقديم الخدمات العامة، والحفاظ على سرية البيانات، واستمرارية الأعمال. من خلال فهم تأثير هذه الهجمات، يمكن تطوير استراتيجيات للحد من الأضرار والتأكد من استمرارية العمليات الحيوية حتى في حالة وقوع هجوم سيبراني. يتطلب ذلك تحليلاً دقيقاً للحوادث السابقة ودراسة الأضرار التي تسببت فيها هذه الهجمات.

— تطوير إطار عمل شامل لإدارة المخاطر السيبرانية.

تهدف هذا الهدف الفرعي إلى تطوير إطار عمل شامل لإدارة المخاطر السيبرانية يشمل تحديد المخاطر، وتقييمها، وإدارة الاستجابة لها. يتضمن ذلك وضع سياسات وإجراءات موحدة لمواجهة التهديدات السيبرانية، وتحديد الأدوار والمسؤوليات بوضوح، وتطوير خطط استجابة للحوادث. يساعد إطار العمل هذا في تنظيم الجهود وتحسين التنسيق بين مختلف الجهات المعنية بالأمن السيبراني داخل المؤسسات الحكومية.

— تطوير وتنفيذ برامج تدريبية لزيادة الوعي بالأمن السيبراني.

يركز هذا الهدف الفرعي على تطوير برامج تدريبية وتوعوية تستهدف جميع مستويات الموظفين في المؤسسات الحكومية. تهدف هذه البرامج إلى زيادة الوعي بأهمية الأمن السيبراني، وتعزيز فهم الموظفين للتهديدات السيبرانية وكيفية التعامل معها، وتشجيع الممارسات الأمنية الجيدة. يشمل ذلك تنظيم ورش عمل، ودورات تدريبية، وحملات توعية مستمرة لضمان بقاء الموظفين على اطلاع دائم بأحدث التهديدات وأساليب الحماية.

تساؤلات الدراسة:

✓ السؤال الرئيسي

- كيف يمكن تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية وتطوير استراتيجيات فعالة للحماية والتخفيف من هذه المخاطر؟

✓ الأسئلة الفرعية:

- ما هي التهديدات السيبرانية الرئيسية التي تواجه المؤسسات الحكومية في المملكة العربية السعودية؟
- ما هو الوضع الحالي للأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية؟
- كيف يمكن قياس فعالية الاستراتيجيات الحالية للحماية من المخاطر السيبرانية في المؤسسات الحكومية؟
- ما هي التحديات الرئيسية التي تواجه المؤسسات الحكومية في تطبيق استراتيجيات الأمن السيبراني؟
- ما هي أفضل الممارسات والتوصيات لتطوير استراتيجيات حماية فعالة للمؤسسات الحكومية في المملكة؟
- كيف يمكن تعزيز التعاون بين المؤسسات الحكومية المختلفة في مجال الأمن السيبراني؟
- ما هي الخطوات المطلوبة لتطوير إطار عمل شامل لإدارة المخاطر السيبرانية في المؤسسات الحكومية؟

فروض الدراسة:

✓ الفرضية الرئيسية

- تطبيق استراتيجيات فعالة لتقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية يساهم بشكل كبير في تحسين مستوى الحماية والتخفيف من المخاطر السيبرانية.

✓ الفرضيات الفرعية

- التهديدات السيبرانية المحددة تؤثر بشكل مباشر على مستوى الأمان السيبراني في المؤسسات الحكومية.
- وجود إطار عمل شامل لإدارة المخاطر السيبرانية يساهم في تحسين فعالية استراتيجيات الحماية والتخفيف.
- تدريب الموظفين وزيادة الوعي بالأمن السيبراني يساهمان في تعزيز الحماية وتقليل المخاطر.
- فعالية استراتيجيات الحماية والتخفيف تتأثر بالتحديات التقنية والتنظيمية التي تواجه المؤسسات.

— التعاون بين المؤسسات الحكومية المختلفة يعزز من فعالية الاستراتيجيات الأمنية ضد المخاطر السيبرانية.

الدراسات السابقة:

تعاني العديد من المنظمات في جميع أنحاء العالم من خسائر فادحة بسبب المخاطر غير المتوقعة التي يمكن أن يكون لها تأثير عميق على بقائها. تقدم هذه الورقة إطارًا آمنًا جديدًا لتلبية الاحتياجات الأمنية للمنظمات السعودية. هناك أربع مراحل في إطار الأمن: تقييم المخاطر وإدارتها، والاستخبارات الأمنية والتحليلات، وسياسات وإجراءات الأمن، ومراقبة الأمن. تم توفير حل أمني شامل من خلال الجمع بين أطر الأمن المشتركة، على سبيل المثال ISO / IEC 27001: 2013، وإطار الأمن السيبراني NIST، و COBIT. تم تصميم الإطار المتطور لمساعدة المنظمات السعودية على تحديد المخاطر وتقييمها والسيطرة عليها والاستجابة للأحداث غير المتوقعة في الوقت المناسب وبطريقة فعالة. ومن المتوقع أن يساعد المنظمات على تطوير وتنفيذ تدابير أمنية فعالة لحماية أصولها وعملياتها الحيوية من التهديدات الأمنية. الإطار المقترح شامل ويمكن أن يغطي متطلبات معظم المنظمات (Alshammari, 2023).

حققت المملكة العربية السعودية إنجازات كبيرة في مجال الأمن السيبراني. فقد حافظت المملكة العربية السعودية على آليات تنظيمية قوية لمنع وتتبع ومعاينة المخالفين لحماية مصالح المستخدمين الأفراد والمنظمات من التهديدات عبر الإنترنت المتمثلة في سرقة البيانات. كما يعزز الاستخدام الواسع النطاق لتكنولوجيا المعلومات وخدمات تمكين تكنولوجيا المعلومات تدابير الأمن. وتعتبر التهديدات السيبرانية المتطورة باستمرار موضوعًا يثير الكثير من المناقشات. وفي هذا الصدد، تسلط هذه المقالة الضوء على منظور واسع النطاق حول كيفية تطور الجرائم الإلكترونية في المملكة العربية السعودية في الوقت الحاضر، كما تلقي نظرة على بعض أهم الهجمات التي وقعت في المنطقة. وتهدف الأطر التشريعية والتدابير الحالية في المملكة العربية السعودية إلى ردع النشاط الإجرامي عبر الإنترنت. وقد تم ابتكار نماذج كفاءة مختلفة لمعالجة الكفاءات اللازمة لمكافحة الجرائم الإلكترونية في هذا السياق. ويمكن للمتخصصين في البحث في هذا المجال الاستفادة بشكل أكبر من خلال تطوير مستوى كفاءة رئيسي لتحقيق أقصى قدر من الأمن. لمعالجة هذا السؤال البحثي، يستخدم التقييم الحالي مختبر تجربة وتقييم صنع القرار الضبابي (Fuzzy-DMTAEI)، وعملية التسلسل الهرمي التحليلي الضبابي (F.AHP)، ومنهجية Fuzzy TOPSIS لتحقيق تطوير

الكفاءة على مستوى القطاعات في سياسة الأمن السيبراني. كما تمت مناقشة أوجه التشابه والاختلاف بين الطرق الثلاث. حدد تحليل الأمن السيبراني هذا أن المركز الوطني للأمن السيبراني حصل على أعلى أولوية. وتختتم الدراسة بدراسة التحديات التي لا تزال بحاجة إلى الفحص والحل في إحداث آليات أمان عبر الإنترنت أكثر مصداقية وفعالية لتقديم اقتصاد أكثر تمكينًا مدفوعًا بخدمات تكنولوجيا المعلومات للمملكة العربية السعودية. علاوة على ذلك، يحتاج المتخصصون في الأمن السيبراني وصناع السياسات إلى جمع جهودهم لحماية الأصول الرقمية للبلاد في عصر الحرب السيبرانية العلنية والسرية (Alhakami, 2024).

اقترحت حكومة المملكة العربية السعودية أطر عمل مختلفة مثل إطار تنظيم الأمن السيبراني لهيئة الاتصالات وتقنية المعلومات وضوابط الأمن السيبراني الأساسية للهيئة الوطنية للأمن السيبراني لضمان أمن البيانات والبنية الأساسية في جميع الأنظمة القائمة على تكنولوجيا المعلومات. ومع ذلك، تفتقر هذه الأطر إلى آلية عملية منشورة تقيم باستمرار مستوى أمن المنظمات، وخاصة في أنظمة مؤسسات التعليم العالي. تقترح هذه الورقة إطار عمل لتقييم نضج الأمن السيبراني لمؤسسات التعليم العالي في المملكة العربية السعودية. SCMAF هو إطار عمل شامل ومخصص لتقييم نضج الأمن للمؤسسات السعودية يتماشى مع معايير الأمن المحلية والدولية. يمكن استخدام الإطار كطريقة تقييم ذاتي لتحديد مستوى الأمان وتبسيط الضوء على نقاط الضعف وخطط التخفيف التي يجب تنفيذها. SCMAF هو نموذج رسم وترميز لجميع اللوائح التي يجب على المؤسسات السعودية الامتثال لها. يستخدم الإطار مستويات مختلفة من النضج يمكن من خلالها قياس أداء الأمن لكل مؤسسة. تم تنفيذ SCMAF كأداة تقييم خفيفة الوزن يمكن توفيرها عبر الإنترنت من خلال خدمة تعتمد على الويب أو دون اتصال بالإنترنت من خلال تنزيل الأداة لضمان خصوصية بيانات المنظمات. يمكن للمنظمات التي تطبق هذا الإطار تقييم مستوى أمان أنظمتها وإجراء تحليل للفجوات وإنشاء خطة للتخفيف. يتم توصيل نتائج التقييم إلى المنظمة باستخدام مخططات النتائج المرئية لكل متطلب أمني لكل مستوى مرفقة بتقرير تقييم (Almomani, 2021).

لقد تصاعد تطور أنظمة المعلومات بشكل كبير خلال العقد الماضي حيث كشفت الأبحاث عن مفاهيم جديدة. إن التوجه العام لتوفير حلول للمشاكل المعقدة لا يزال يلهم الإبداع والتقدم الجديد. يبرز الأمن السيبراني كعامل حاسم للنظر فيه ضمن النموذج الناتج حيث أصبحت أنظمة المعلومات متكاملة بشكل كبير. تقدم هذه الورقة تحليلًا متعمقًا للأمن السيبراني في سياق أنظمة المعلومات. تدرس الورقة بعض الجوانب الأكثر أهمية للأمن

السيبراني من منظور مشروع الحكومة الإلكترونية في المملكة العربية السعودية. يتم اقتراح نظام شامل ضمن إطار البحث لدمج المبادئ التوجيهية العلمية المختلفة. يعتمد التوجه العام لهذا البحث على الطموح لتصميم وتنفيذ إطار معقد وقوي يمكن لنظام الحكومة الإلكترونية من خلاله أن يزدهر في سياق المملكة العربية السعودية. يتم أيضًا النظر في البيئة المادية التي سيعمل فيها المشروع، مع التركيز على الأمن. يعكس تقييم بيئة الأمن السيبراني في المملكة العربية السعودية التقدم الكبير الذي حدث في مجالات أنظمة المعلومات خلال السنوات القليلة الماضية (Alrubaiq, 2021).

إن المملكة العربية السعودية لديها هدف يتمثل في ضمان وجود مدينتين على الأقل ضمن أفضل 100 مدينة ذكية في المستقبل. ومع ذلك، فإن زيادة الاتصال ودمج الحلول الذكية في المدن لا يزال يثير المخاوف بشأن الأمن السيبراني مع التهديدات التي تنشأ يوميًا بما في ذلك رفض الخدمات والتصيد الاحتيالي كأحد أهم التهديدات. وبالتالي، تحتاج المملكة العربية السعودية إلى إطار عمل لسياسة الأمن السيبراني يضمن الحماية الفعالة لجميع أصحاب المصلحة في المدينة الذكية من هذه التهديدات السيبرانية. يعد قبول المستخدم هو الأهم في أي تقنية جديدة، بما في ذلك المدن الذكية. وبسبب التهديدات السيبرانية المستمرة وفي غياب سياسات سيبرانية فعّالة، فإن مجتمع المستخدم النهائي السعودي ليس حريصًا على قبول التقنيات الأحدث حيث يتطلب تفاعله مع الوسائط عبر الإنترنت. يتيح انتشار المدن الذكية عالميًا الفرصة لتحليل ومقارنة الجهود المبذولة في المملكة العربية السعودية مع دول أخرى مثل الولايات المتحدة الأمريكية والهند وسنغافورة التي تعد نموذج المدينة الذكية الرائد في العالم حاليًا. تتناول هذه المراجعة أوجه التشابه والاختلاف بين إطار سياسة الأمن السيبراني في المملكة العربية السعودية مع هذه الدول الثلاث. ستتناول المراجعة بعض الخصائص والأساليب المحددة للأمن السيبراني في المدن الذكية في الولايات المتحدة الأمريكية والهند وسنغافورة. وبعد مراجعة الإطار الحالي في المملكة العربية السعودية، ستقدم هذه الورقة اقتراحات مثل تحديث تشريعات الجرائم الإلكترونية في المملكة العربية السعودية كما هو الحال في الولايات المتحدة أو صياغة خطة رئيسية للأمن السيبراني كما هو الحال في سنغافورة والتي من شأنها تحسين إطار المملكة العربية السعودية من خلال إنشاء أفضل نموذج إيطاري للأمن السيبراني في مدنها الذكية (Alhalafi, 2021).

المنطلقات النظرية للدراسة:

في عصر التكنولوجيا الرقمية، أصبحت المخاطر السيبرانية واحدة من أبرز التهديدات التي تواجه المؤسسات الحكومية في المملكة العربية السعودية. يشكل تقييم مخاطر الأمن السيبراني في هذه المؤسسات موضوعاً بالغ الأهمية، إذ يلعب دوراً حيوياً في ضمان استمرارية العمل وحماية المعلومات الحساسة والأنظمة الحيوية. من خلال فهم المنطلقات النظرية التي تقوم عليها دراسة هذا الموضوع، يمكن تسليط الضوء على الأسس التي تعتمد عليها استراتيجيات الحماية والتخفيف، مما يساهم في تعزيز الأمان السيبراني وحماية البنية التحتية المعلوماتية.

• مفهوم الأمن السيبراني وأهمية تقييم المخاطر

الأمن السيبراني يشير إلى مجموعة التدابير والتقنيات والسياسات التي تهدف إلى حماية الأنظمة الحاسوبية والشبكات والمعلومات من التهديدات والاختراقات السيبرانية. يشمل ذلك تأمين البيانات من السرقة أو التعديل غير المصرح به، وضمان استمرارية التشغيل، وحماية الخصوصية. في المؤسسات الحكومية، يعتبر الأمن السيبراني أكثر أهمية نظراً لحساسية المعلومات التي تديرها والتي قد تشمل بيانات شخصية، معلومات حساسة تتعلق بالأمن الوطني، والبيانات المالية.

تقييم مخاطر الأمن السيبراني هو عملية منهجية تهدف إلى تحديد وتحليل المخاطر التي قد تؤثر على الأمان السيبراني للمؤسسات. يتضمن ذلك دراسة التهديدات المحتملة، وتحديد نقاط الضعف في الأنظمة، وتقدير الأثر المحتمل لهذه التهديدات. يُعد هذا التقييم خطوة أساسية في تطوير استراتيجيات فعالة للحماية والتخفيف من المخاطر، حيث يساعد في تحديد أولويات الأمان وتركيز الموارد على التهديدات الأكثر خطورة (Pryimenko, 2024).

• الأسس النظرية لنموذج تقييم المخاطر

نموذج تقييم المخاطر هو إطار عمل يساعد في تحديد وتقدير وتحليل المخاطر السيبرانية. يتألف النموذج من عدة خطوات رئيسية تبدأ بتحديد الأصول التي تحتاج إلى حماية. هذه الأصول قد تشمل البيانات الحساسة، الأنظمة الحيوية، والبنية التحتية التقنية. يتطلب تحديد الأصول فهماً عميقاً لمحتويات المعلومات وقيمتها بالنسبة للمؤسسة. بعد ذلك، يتم تحديد التهديدات المحتملة التي قد تستهدف هذه الأصول. يشمل ذلك التعرف على الهجمات الإلكترونية الشائعة مثل البرمجيات الخبيثة، وهجمات الفدية، وهجمات التصيد.

الخطوة التالية هي تقييم الثغرات في الأنظمة والإجراءات الأمنية. هذا يتضمن فحص نقاط الضعف المحتملة التي يمكن أن يستغلها المهاجمون، مثل ضعف الأمان في البرمجيات، أو نقص في تحديث الأنظمة. بعد تحديد الثغرات، يتم تقدير الأثر المحتمل لكل تهديد على المؤسسة، بما في ذلك التأثير على العمليات التشغيلية، وسرية المعلومات، وسمعة المؤسسة. أخيراً، يتم دمج نتائج تحليل التهديدات والثغرات والأثر لتحديد مستوى المخاطر وإيجاد استراتيجيات لتخفيف هذه المخاطر (Kure, 2021).

• استراتيجيات الحماية والتخفيف من المخاطر السيبرانية

تستند استراتيجيات الحماية والتخفيف إلى مجموعة من المبادئ والأسس النظرية التي تهدف إلى تعزيز الأمان السيبراني. تعتمد هذه الاستراتيجيات على مفهوم الدفاع المتعدد الطبقات، الذي يتضمن استخدام مجموعة من التدابير الأمنية المختلفة لتوفير حماية شاملة. يشمل ذلك استخدام الجدران النارية، وبرامج مكافحة الفيروسات، وأنظمة الكشف عن التسلل، وأنظمة التحكم بالوصول. الفكرة هي أن كل طبقة من هذه الطبقات تعزز الأمان وتضيف حماية إضافية ضد التهديدات (Obi, 2024).

استراتيجية أخرى هي إدارة الثغرات، التي تركز على التعرف على نقاط الضعف في الأنظمة والعمل على إصلاحها. يشمل ذلك تحديث البرمجيات بانتظام، وتطبيق التصحيحات الأمنية، وإجراء اختبارات اختراق دورية لتحديد الثغرات قبل أن يستغلها المهاجمون. بالإضافة إلى ذلك، تكتسب استراتيجيات الاستجابة للحوادث أهمية كبيرة، حيث تشمل إنشاء خطط للاستجابة السريعة والفعالة للحوادث الأمنية، وتحديد الفرق المسؤولة عن التعامل مع هذه الحوادث، وتحليل أسبابها، وتطوير استراتيجيات لاستعادة الأنظمة والبيانات.

• التدريب والتوعية كعنصر أساسي في تعزيز الأمان

أحد الأسس النظرية الهامة في استراتيجيات الحماية والتخفيف هو أهمية التدريب والتوعية. برامج التدريب والتوعية تلعب دوراً حاسماً في زيادة وعي الموظفين بالمخاطر السيبرانية وكيفية التعامل معها. إن تحسين الوعي حول الأمن السيبراني وتعليم الموظفين كيفية التعرف على التهديدات وكيفية التعامل معها يمكن أن يساهم بشكل كبير في تقليل الأخطاء البشرية التي قد تؤدي إلى خروقات أمنية. تتضمن هذه البرامج التدريبية دورات تعليمية، وورش عمل، وحملات توعية منتظمة (Olabode, 2023).

• التعاون والتنسيق بين المؤسسات

استراتيجية التعاون والتنسيق تعد من العوامل الهامة في تعزيز الأمن السيبراني. يشمل التعاون بين المؤسسات الحكومية تبادل المعلومات حول التهديدات والحوادث السيبرانية، وتطوير استراتيجيات حماية مشتركة. يعزز التعاون المشترك من قدرة المؤسسات على التصدي للتهديدات بشكل جماعي، ويحقق حماية أفضل. يشمل هذا التعاون تطوير قنوات للتواصل، وتنسيق الجهود لمواجهة التهديدات المشتركة، وإنشاء فرق عمل مشتركة لتحليل الحوادث وتطوير حلول فعالة (Lostri, 2022).

تشكل المنطلقات النظرية أساساً لفهم الأبعاد المختلفة للأمن السيبراني وتقييم المخاطر في المؤسسات الحكومية. من خلال دراسة مفاهيم الأمن السيبراني، ونموذج تقييم المخاطر، واستراتيجيات الحماية والتخفيف، والتدريب والتوعية، والتعاون بين المؤسسات، يمكن تطوير استراتيجيات فعالة لتعزيز الأمن السيبراني وحماية الأنظمة والبيانات في المؤسسات الحكومية بالمملكة العربية السعودية. هذه المنطلقات توفر إطاراً متكاملاً يساعد في فهم التحديات وتقديم حلول مبتكرة لضمان أمان المعلومات واستمرارية العمل في ظل التهديدات المتزايدة.

المنهجية وطرق البحث:

تعد المنهجية الكمية أداة رئيسية في دراسة تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، حيث تتيح تحليل البيانات بطريقة علمية وموضوعية لدعم الفرضيات وتقديم رؤى دقيقة حول الاستراتيجيات الأكثر فعالية للحماية والتخفيف. تعنى المنهجية الكمية بجمع وتحليل البيانات الرقمية من خلال أدوات وأساليب إحصائية، مما يوفر قاعدة قوية لفهم العلاقات بين المتغيرات وتقييم فعالية الاستراتيجيات الأمنية. في هذا السياق، تتضمن المنهجية الكمية عدة مراحل وخطوات أساسية تشمل تصميم الدراسة، جمع البيانات، تحليل البيانات، وتفسير النتائج.

تصميم الدراسة هو المرحلة الأولى والأكثر أهمية في المنهجية الكمية، حيث يتعين تحديد الأهداف البحثية، وصياغة الفرضيات، واختيار الأدوات المناسبة لجمع البيانات. في دراسة تقييم مخاطر الأمن السيبراني، يبدأ التصميم

بتحديد الأهداف البحثية المحددة التي تسعى الدراسة إلى تحقيقها، مثل تقييم فعالية استراتيجيات الحماية الحالية، أو تحليل مدى استعداد المؤسسات الحكومية للتعامل مع المخاطر السيبرانية.

بعد تحديد الأهداف، يتم صياغة الفرضيات التي ستختبر خلال البحث. الفرضيات قد تشمل مثلاً: "تطبيق استراتيجيات الحماية السيبرانية المتقدمة يقلل بشكل كبير من المخاطر السيبرانية في المؤسسات الحكومية"، أو "التدريب والتوعية المستمرة للموظفين يعزز من فعالية استراتيجيات الأمن السيبراني". تستند هذه الفرضيات إلى الأدبيات السابقة والمعرفة النظرية حول الأمن السيبراني.

اختيار أدوات جمع البيانات هو خطوة حاسمة في التصميم. تشمل الأدوات الشائعة في المنهجية الكمية الاستبيانات، والمقاييس الرقمية، والبيانات الثانوية. في هذا السياق، يمكن استخدام الاستبيانات لتجميع بيانات من موظفي المؤسسات الحكومية حول ممارسات الأمن السيبراني والإجراءات المتبعة، بينما توفر البيانات الثانوية تحليلات سابقة أو تقارير تتعلق بالحوادث السيبرانية وأداء استراتيجيات الحماية.

جمع البيانات هو المرحلة الثانية في المنهجية الكمية، ويشمل تنفيذ الأدوات التي تم تحديدها في مرحلة التصميم. يمكن أن يتم جمع البيانات من خلال عدة طرق، مثل إرسال الاستبيانات إلى موظفي المؤسسات الحكومية، أو إجراء مقابلات structured مع المسؤولين عن الأمن السيبراني في هذه المؤسسات. الهدف من جمع البيانات هو الحصول على معلومات دقيقة وشاملة حول المخاطر السيبرانية والتدابير المتخذة لتخفيفها.

تتضمن عملية جمع البيانات في دراسة تقييم مخاطر الأمن السيبراني تنظيم الاستبيانات بحيث تتناول جميع جوانب الأمان السيبراني، مثل الأساليب المستخدمة للحماية، والتدريب، والاستجابة للحوادث. قد تشمل الاستبيانات أسئلة متعددة الخيارات، وأسئلة تقييم، وأسئلة مفتوحة للحصول على معلومات نوعية. من الضروري التأكد من أن الاستبيانات مصممة بطريقة تمكن من الحصول على بيانات قابلة للتحليل الإحصائي.

تحليل البيانات هو المرحلة التي يتم فيها تحويل البيانات الخام إلى معلومات ذات معنى وقيمة. في المنهجية الكمية، يتضمن التحليل استخدام أدوات إحصائية لفحص العلاقات بين المتغيرات واختبار الفرضيات. يمكن استخدام برامج التحليل الإحصائي مثل SPSS، أو R، أو Python لتحليل البيانات.

تبدأ عملية التحليل بتقييم جودة البيانات وتنظيفها، وهو خطوة ضرورية لضمان دقة النتائج. يشمل التنظيف إزالة البيانات غير الصحيحة أو المفقودة، وضمان تطابق البيانات مع معايير البحث. بعد التنظيف، يتم تطبيق الأساليب الإحصائية مثل التحليل الوصفي لتلخيص البيانات واختبار الفرضيات باستخدام التحليل الاستدلالي.

تشمل الأساليب الإحصائية الشائعة في تحليل بيانات الأمن السيبراني تحليل الانحدار لتحديد مدى تأثير المتغيرات المستقلة مثل استراتيجيات الحماية على المتغير التابع مثل مستوى المخاطر، وتحليل التباين لتحديد الفروقات بين مجموعات مختلفة مثل المؤسسات التي تطبق استراتيجيات حماية متقدمة مقابل تلك التي لا تطبقها. تفسير النتائج هو المرحلة التي يتم فيها استخدام نتائج التحليل للإجابة على الأسئلة البحثية وتقييم الفرضيات. في دراسة تقييم مخاطر الأمن السيبراني، يتطلب تفسير النتائج ربط البيانات التي تم تحليلها بالسياق النظري والعملي للبحث. يتضمن ذلك فهم كيف تعكس النتائج فعالية استراتيجيات الحماية والتخفيف المستخدمة في المؤسسات الحكومية، ومدى استعدادها للتعامل مع التهديدات السيبرانية.

يتضمن تفسير النتائج أيضاً مقارنة النتائج التي تم الحصول عليها مع الأبحاث السابقة والنظريات ذات الصلة. يمكن أن تساعد هذه المقارنة في تحديد ما إذا كانت الاستراتيجيات الحالية فعالة أم تحتاج إلى تعديل. كما يمكن أن توفر التفسيرات رؤى حول المجالات التي تتطلب تحسينات، وتساعد في تطوير توصيات قائمة على البيانات لتحسين الأمن السيبراني.

المرحلة الأخيرة في المنهجية الكمية تتضمن تقديم التوصيات بناءً على نتائج البحث. يتم إعداد تقارير مفصلة تلخص النتائج الرئيسية، وتقدم توصيات لتحسين استراتيجيات الحماية والتخفيف من المخاطر السيبرانية. تشمل هذه التوصيات تحسين السياسات الأمنية، وتحديث الإجراءات الحالية، وتعزيز برامج التدريب والتوعية. تتضمن التقارير أيضاً تحليل الفجوات بين الممارسات الحالية والمعايير المثلى للأمن السيبراني. يمكن أن تساعد هذه التقارير المؤسسات الحكومية في تحديد الأولويات، وتوجيه الموارد بشكل أكثر فعالية لتعزيز الأمان السيبراني.

توفر المنهجية الكمية إطاراً منهجياً وشاملاً لتحليل وتقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. من خلال تصميم الدراسة بشكل دقيق، وجمع البيانات بفعالية، وتحليلها باستخدام

أساليب إحصائية متقدمة، وتفسير النتائج بشكل منهجي، يمكن الحصول على رؤى قيمة تساعد في تطوير استراتيجيات الحماية والتخفيف من المخاطر السيبرانية. تعزز هذه المنهجية من القدرة على تقديم توصيات مبنية على البيانات لتحسين الأمن السيبراني وضمان حماية فعالة للمعلومات والأنظمة في المؤسسات الحكومية.

أدوات الدراسة:

• الاستبيانات

الاستبيانات تُعتبر أداة أساسية لجمع البيانات الكمية في الدراسات الأكاديمية والتطبيقية، خاصة في سياق تقييم مخاطر الأمن السيبراني. تصميم الاستبيان في هذا السياق يتطلب تحديد مجموعة من الأسئلة الدقيقة التي تغطي الجوانب المختلفة للأمن السيبراني. يشمل ذلك تقييم مدى فعالية الاستراتيجيات الأمنية المتبعة، فحص وعي الموظفين بممارسات الأمن السيبراني، وتحليل مدى تطبيق السياسات الأمنية في المؤسسات الحكومية. الأسئلة يجب أن تكون مصممة بعناية لضمان جمع معلومات ذات قيمة. يتم تقسيم الاستبيان إلى أقسام تتناول موضوعات محددة مثل الوعي الأمني، فعالية استراتيجيات الحماية، وتقييم السياسات الأمنية. من المهم أن تتضمن الأسئلة خيارات إجابة واضحة، مثل مقاييس ليكرت، التي تتيح للمشاركين التعبير بدقة عن مدى اتفاقهم مع التصريحات المعروضة. بعد جمع الاستبيانات، يتم إدخال البيانات إلى برامج التحليل الإحصائي مثل SPSS أو Excel، حيث يتم تحليلها لاكتشاف الأنماط والاتجاهات، مما يوفر رؤى حول فعالية الاستراتيجيات الأمنية والتحديات الحالية.

• المقابلات

المقابلات تقدم فرصة للحصول على بيانات نوعية تفصيلية، مما يتيح فهماً أعمق لممارسات الأمن السيبراني والتحديات التي تواجهها المؤسسات الحكومية. يتم إجراء المقابلات مع المسؤولين عن الأمن السيبراني، ومديري تكنولوجيا المعلومات، وموظفين رئيسيين في المؤسسات. إعداد المقابلات يتطلب صياغة أسئلة مفتوحة تشجع المشاركين على تقديم إجابات مفصلة حول استراتيجيات الحماية والتدابير الأمنية. تسجيل المقابلات يمكن أن يكون مفيداً لتوثيق المعلومات بدقة، ويجب أن يتم بشكل يحترم الوقت والخصوصية. بعد إجراء المقابلات، يتم تحليل البيانات باستخدام تقنيات التحليل النوعي مثل تحليل المحتوى أو تحليل الموضوعات.

هذا التحليل يساعد في الكشف عن الأنماط المشتركة والاتجاهات، ويعزز من فهم فعالية الاستراتيجيات الأمنية والتحديات التي تواجهها المؤسسات.

• تحليل الوثائق

تحليل الوثائق يشمل مراجعة دراسة الوثائق الرسمية والتقارير ذات الصلة بالأمن السيبراني، مثل السياسات الأمنية والتقارير السنوية وسجلات الحوادث. عملية جمع الوثائق تتضمن استعراض الوثائق من مصادر داخلية للمؤسسات الحكومية وأيضاً من تقارير الأبحاث السابقة.

تحليل الوثائق يشمل فحص محتوى الوثائق لتحديد مدى توافق السياسات والإجراءات مع المعايير الأمنية المعتمدة. يشمل ذلك تقييم فعالية السياسات الأمنية من خلال مراجعة كيفية تطبيقها ومطابقتها للمعايير. تحليل سجلات الحوادث السيبرانية يمكن أن يكشف عن طبيعة التهديدات وأسبابها، مما يوفر رؤى حول كيفية تحسين استراتيجيات الحماية والتخفيف من المخاطر.

• الأدوات التقنية

الأدوات التقنية تلعب دوراً مهماً في تقييم فعالية الأنظمة الأمنية ومراقبة الأداء السيبراني. تشمل هذه الأدوات برامج الفحص الأمني، أنظمة كشف التسلل، وأدوات تحليل البيانات. برامج الفحص الأمني تُستخدم لاكتشاف الثغرات في الأنظمة والشبكات، وتساعد في تحديد نقاط الضعف التي قد يستغلها المهاجمون. أنظمة كشف التسلل توفر مراقبة مستمرة وتحليل للأنشطة السيبرانية للكشف عن محاولات التسلل والتهديدات. أدوات تحليل البيانات تستخدم لتحليل المعلومات الناتجة عن الأدوات الأمنية الأخرى، مما يساعد في تفسير البيانات وتقديم رؤى حول فعالية التدابير الأمنية ومدى التهديدات التي تواجهها المؤسسات.

• التحليل والتقييم

التحليل والتقييم يتطلب دمج البيانات التي تم جمعها من الاستبيانات والمقابلات وتحليل الوثائق والأدوات التقنية. تتضمن هذه الخطوة تفسير النتائج لتقديم صورة شاملة عن فعالية استراتيجيات الحماية والتخفيف من المخاطر السيبرانية.

تفسير النتائج يشمل فحص البيانات لاكتشاف الأنماط والاتجاهات، ومقارنة النتائج بالمعايير والأهداف البحثية. بعد تفسير البيانات، يتم إعداد تقارير مفصلة تلخص النتائج الرئيسية وتقديم توصيات لتحسين استراتيجيات الأمان السيبراني. هذه التقارير توفر أساساً قوياً لتحسين الأمان السيبراني وحماية المعلومات والأنظمة بشكل فعال.

حدود الدراسة :

✓ الحدود البشرية

تعتبر الحدود البشرية من العوامل الرئيسية التي تحدد نطاق الدراسة، حيث تشير إلى الفئات والأفراد المشاركين في البحث. في دراسة تقييم مخاطر الأمان السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، يتم تحديد الحدود البشرية بناءً على الأشخاص الذين يتعاملون مباشرة مع الأمان السيبراني في هذه المؤسسات. تشمل الفئات الرئيسية المستهدفة في هذه الدراسة المسؤولين عن إدارة الأمان السيبراني، مديري تكنولوجيا المعلومات، فرق الاستجابة للحوادث السيبرانية، وأيضاً الموظفين الذي يتعاملون مع أنظمة المعلومات بشكل يومي.

التركيز على هذه الفئات يتيح الحصول على رؤى شاملة حول فعالية الاستراتيجيات الأمنية المطبقة، كما أن إشراك هؤلاء الأفراد يمكن أن يوفر معلومات قيمة حول تحديات تطبيق السياسات الأمنية ومستوى الوعي بممارسات الأمان السيبراني. الحدود البشرية تشمل كذلك تحديد معايير اختيار المشاركين، مثل الخبرة العملية في مجال الأمان السيبراني، ودرجة المسؤولية في المؤسسة، لضمان جمع بيانات دقيقة وموثوقة تعكس واقع الأوضاع الأمنية.

✓ الحدود الزمانية

الحدود الزمانية تشير إلى الفترة الزمنية التي تُجرى فيها الدراسة، والتي تلعب دوراً مهماً في تحديد سياق النتائج وتفسيرها. في دراسة تقييم مخاطر الأمان السيبراني، يتم تحديد الفترة الزمنية بناءً على متطلبات البحث والأهداف المرجوة. عادةً ما تتضمن الدراسة فترة زمنية محددة لجمع البيانات وتحليلها، تقع هذه الفترة من أكتوبر 2023 حتى يوليو 2024م.

الاهتمام بالحدود الزمانية يضمن التناسق في جمع البيانات وتحليلها، كما يتيح فرصة لملاحظة التغيرات في الأوضاع الأمنية والتقنيات المستخدمة بمرور الوقت. على سبيل المثال، قد تتغير استراتيجيات الأمان السيبراني وتطور التقنيات

المستخدمة في الحماية بشكل مستمر، لذا من الضروري تحديد فترة زمنية مناسبة لمراقبة هذه التغيرات وتقييم تأثيرها على فعالية الأمان السيبراني.

✓ الحدود المكانية

الحدود المكانية تتعلق بالموقع الجغرافي الذي تُجرى فيه الدراسة، وتحدد نطاق المؤسسات التي سيتم فحصها في البحث. في هذه الدراسة، تركز الحدود المكانية على المؤسسات الحكومية في المملكة العربية السعودية، وهذا يشمل مختلف الجهات الحكومية التي تمتلك أنظمة معلومات حساسة والتي تحتاج إلى تقييم استراتيجيات الحماية والتخفيف من المخاطر السيبرانية.

الحدود المكانية تشمل أيضًا اختيار المؤسسات التي ستتم دراسة الأمن السيبراني فيها، مثل الوزارات، الهيئات الحكومية، والوكالات العامة. من المهم تحديد المواقع الجغرافية بدقة لضمان أن الدراسة تعكس التنوع في المؤسسات الحكومية من حيث حجمها ونوعها وأنواع التهديدات التي قد تواجهها. تشمل الحدود المكانية أيضًا التعرف على اختلافات بين المناطق المختلفة في المملكة، مثل المدن الكبرى مقابل المناطق الريفية، لضمان أن النتائج تمثل الواقع الأمني السيبراني بشكل شامل.

المراجع:

- Abdullah Alrubaiq من الاسترداد (2021). <https://www.mdpi.com/2624-800X/1/2/17>
- Ahmad Alshammari .(2023) .A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia من الاسترداد 13(4) .
<https://www.etasr.com/index.php/ETASR/article/view/6091>
- Alok Mishra .(2022) .Attributes impacting cybersecurity policy development: An evidence from seven nations من الاسترداد .
<https://www.sciencedirect.com/science/article/pii/S0167404822002140>
- Anastasios Giannaros .(2023) .Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions من الاسترداد .
<https://www.mdpi.com/2624-800X/3/3/25>
- Eugenia Lostri .(2022) .A Shared Responsibility: Public-Private Cooperation for Cybersecurity من الاسترداد <https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity>
- Frank Cremer .(2022) .Cyber risk and cybersecurity: a systematic review of data availability من الاسترداد <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/>
- Halima Kure .(2021) .An Assets Focus Risk Management Framework for Critical Infrastructure Cyber Security Risk Management من الاسترداد .
https://www.researchgate.net/publication/332969258_An_Assets_Focus_Risk_Management_Framework_for_Critical_Infrastructure_Cyber_Security_Risk_Management
- Iman Almomani .(2021) .Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia من الاسترداد <https://peerj.com/articles/cs-703/>
- John M. Borky .(2018) .Protecting Information with Cybersecurity من الاسترداد <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7122347/>
- Liudmyla Pryimenko 5 .(2024) .Key Steps on How to Perform a Cybersecurity Risk Assessment من الاسترداد <https://www.ekransystem.com/en/blog/how-to-perform-a-cybersecurity-risk-assessment>
- Nawaf Alhalafi .(2021) .Cybersecurity Policy Framework in Saudi Arabia: Literature Review من الاسترداد <https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.736874/full>
- Ogugua Chimezie Obi .(2024) .COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES من الاسترداد https://www.researchgate.net/publication/377957344_COMPREHENSIVE_REVIEW_ON_CYBERSECURITY_MODERN_THREATS_AND_ADVANCED_DEFENSE_STRATEGIES
- Olufunmilayo Olabode .(2023) .The Relevance Of Cybersecurity Awareness Training For Employees In Small and Medium Enterprises (SMEs) من الاسترداد https://www.researchgate.net/publication/376538971_The_Relevance_Of_Cybersecurity_Awareness_Training_For_Employees_In_Small_and_Medium_Enterprises_SMEs

Samuel Onimisi Dawodu .(2023) .CYBERSECURITY RISK ASSESSMENT IN BANKING:

METHODOLOGIES AND BEST PRACTICES . تم الاسترداد من

https://www.researchgate.net/publication/376806023_CYBERSECURITY_RISK_ASSESSMENT_IN_BANKING_METHODOLOGIES_AND_BEST_PRACTICES

Shahriar Akter .(2022) .Reconceptualizing cybersecurity awareness capability in the data-driven

digital economy . تم الاسترداد من <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9345286/>

Wajdi Alhakami .(2024) .Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A

Fuzzy Decision-Making Approach . تم الاسترداد من

<https://openurl.ebsco.com/EPDB%3Agcd%3A16%3A19342416/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A178454206&crl=c>

Mid-Ocean University

College of Management

Department of Risk management



**Cybersecurity Risk Assessment in Government Organizations in the
Kingdom of Saudi Arabia: Protection and Mitigation Strategies**

Preparation:

Madhawi Mohammad Al Mutairi

Supervision:

2024