

إدارة الأمن السيبراني من منظور إدارة الأعمال
الأثار، العقبات، التداعيات والأهداف
على الشركات المشغلة لشبكات الاتصال الافتراضية (MVNOs)

إعداد الطالب/

محمد أحمد مشرعي

إشراف/

د.الفصيل عبد الحميد

د.فايز جراد

العام الدراسي:

2023

مقدمة:

تعتبر تقنية شبكات الاتصالات الافتراضية واحدة من أبرز وأحدث التقنيات في قطاع الاتصالات، حيث توفر خدمات الاتصالات عبر بنية تحتية مستأجرة، مما يتيح للشركات تقديم خدماتها بتكلفة أقل ومرونة أكبر. ومع تزايد الاعتماد على التقنيات الرقمية في جوانب الحياة الاجتماعية والاقتصادية أصبح الأمن السيبراني ضرورة لا اختياراً بالنسبة لمشغلي هذه الشبكات.

إن إدارة الأمن السيبراني تمثل تحدياً استراتيجياً شديد الأهمية لهذه الشركات، حيث ترتبط قدرة الشركات على حماية بيانات عملائها وحمايتهم من المخاطر الإلكترونية بالاستمرار في النمو والتوسع في هذا المجال. تهدف هذه الدراسة إلى استكشاف الأبعاد المختلفة لإدارة الأمن السيبراني في شركات شبكات الاتصالات الافتراضية من منظور إدارة الأعمال، مع التركيز على الآثار والعقبات والتداعيات التي قد تنشأ نتيجة لتحديات الأمن السيبراني، فضلاً عن الأهداف التي تسعى هذه الشركات لتحقيقها في هذا المجال.

مشكلة الدراسة:

تواجه الشركات المشغلة لشبكات الاتصال الافتراضية تحديًا بالغًا في إدارة الأمن السيبراني صعوبةً وتعقيدًا، حيث أن سرعة تطور هذه التقنيات لا تتوافق مع وسائل الحماية المتوفرة في الأمن السيبراني. إن المخاطر التي تتعرض لها هذه الشركات تزداد بشكل مستمر مهددة سرية البيانات وسلامة النظام وتوافر الخدمة. في ظل هذه الظروف، تعاني الشركات المشغلة لشبكات الاتصال الافتراضية من عدة مشكلات استراتيجية وإدارية في مجال الأمن السيبراني، أهمها:

1. تعقيد البنية التحتية الافتراضية
2. التحديات القانونية والتنظيمية
3. الهجمات المتطورة والمستمرة
4. التوازن بين الأمن والتطور
5. الآثار المالية والتشغيلية

أهمية الدراسة:

تتمثل أهمية هذه الدراسة في تسليط الضوء على إدارة الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية وتوضيح الآثار والتحديات التي تواجهها الشركات في ظل التزايد المستمر للتهديدات السيبرانية وصعوبة الالتزام بالمتطلبات التشريعية. أهمية هذه الدراسة يمكن تفنيدها كالآتي:

1. التحقيق في تأثير الأمن السيبراني على استدامة الشركات
2. تحليل العقبات والتحديات التي تواجه الشركات المشغلة لشبكات الاتصال الافتراضية
3. القيود المالية والقانونية والتشريعية

أهداف الدراسة:

تهدف هذه الدراسة إلى إيضاح أهمية وأثر إدارة الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية وتقديم الحلول لمواجهة التحديات التي تواجهها. تشمل الأهداف الرئيسية:

1. فهم تحديات الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية
2. دراسة الآثار المترتبة على ضعف إدارة الأمن السيبراني
3. تقييم العقبات والتحديات التي تحد من التطبيق السليم لاستراتيجيات وأهداف الأمن السيبراني
4. الحلول والاستراتيجيات التي تساعد في تعزيز الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية

تساؤلات الدراسة

تستند هذه الدراسة إلى مجموعة من التساؤلات الرئيسية التي تهدف إلى توجيه البحث نحو فهم معمق لمفهوم إدارة الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية، والتحديات التي تواجهها هذه الشركات في حماية بنيتها التحتية وبياناتها وخدماتها. التساؤلات التالية تسعى للإجابة على الجوانب المختلفة المتعلقة بالأمن السيبراني في هذا السياق:

1. ما هي التحديات الرئيسية التي تواجه الشركات المشغلة لشبكات الاتصال الافتراضية في إدارة الأمن السيبراني؟
2. ما هي اثار سوء تطبيق سياسات الأمن السيبراني وماهي العواقب؟
3. ما هي الأهداف الاستراتيجية التي يجب أن تكون محور إدارة الأمن السيبراني بالنسبة للشركات المشغلة لشبكات الاتصال الافتراضية؟
4. ما هي الحلول والتقنيات المستخدمة لتعزيز الأمن السيبراني ومدى فعاليتها في الشركات المشغلة لشبكات الاتصال الافتراضية

فروض الدراسة:

استنادًا إلى تساؤلات الدراسة، يمكن صياغة مجموعة من الفروض التي تمثل فرضيات يمكن اختبارها في سياق إدارة الأمن السيبراني في شركات شبكات الاتصالات الافتراضية. هذه الفروض تهدف إلى تقديم توجيهات واضحة حول كيفية تأثير العوامل المختلفة على أمن هذه الشركات، وتساعد في تحديد الممارسات الأكثر فعالية في مواجهة التحديات السيبرانية. الفروض الرئيسية للدراسة هي:

1. "تواجه الشركات المشغلة لشبكات الاتصال الافتراضية تحديات تقنية وإدارية ومالية معقدة تؤثر على إدارة الأمن السيبراني"
2. "استراتيجيات وسياسات الأمن السيبراني لا يتم اتباعها بالشكل الصحيح في الشركات المشغلة لشبكات الاتصال الافتراضية"
3. "الامتثال للوائح القانونية والتنظيمية له تأثير إيجابي في تحسين الممارسات في الشركات المشغلة لشبكات الاتصال الافتراضية"
4. "الاستثمار في الأمن السيبراني يساهم في حماية الشركات المشغلة لشبكات الاتصال الافتراضية من خسائر غير متوقعة كما يحسن من صورة لدى المستثمرين والعملاء"
5. "الاستراتيجيات والسياسات المرنة والتي تواكب بين الأمان والتطور يساعد الشركات المشغلة لشبكات الاتصال الافتراضية على الحفاظ على سلامة البنية والتحتية والبيانات والخدمات مع استمرار إمكانية التطور والتوسع"

الدراسات السابقة:

المنطلقات النظرية للدراسة:

تستند الدراسة من منطلق نظري إلى عدة مجالات، منها إدارة الأعمال، الأمن السيبراني وإدارة تكنولوجيا المعلومات. وفيما يلي أهم المنطلقات النظرية التي كانت الأساس لهذه الدراسة:

1. نظرية الامتثال التنظيمي
2. نظرية إدارة الموارد البشرية
3. نظرية الابتكار التكنولوجي
4. نظرية إدارة المخاطر

المنهجية وطرق البحث:

تحدد المنهجية التي سيتم اتباعها في هذه الدراسة كيفية جمع البيانات، تحليلها، واستخلاص النتائج من أجل تحقيق أهداف البحث والإجابة على تساؤلاته. بالنظر إلى موضوع الدراسة الذي يركز على إدارة الأمن السيبراني في شركات شبكات الاتصالات الافتراضية.

1. المنهج البحثي:

لتحقيق أهداف الدراسة والإجابة على التساؤلات المطروحة، سيتم اتباع المنهج الوصفي التحليلي، وهو المنهج الأكثر ملاءمة لدراسة موضوع معقد مثل إدارة الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية

2. تصميم البحث:

1. نوع الدراسة:

• دراسة ميدانية تحليلية

2. العينة المستهدفة:

3. الأدوات المستخدمة في جمع البيانات

• الاستبيانات

• المقابلات

• دراسات المستندات والتقارير السنوية للشركات المشغلة لشبكات الاتصال الافتراضية

3. أدوات التحليل:

أ. التحليل الكمي

ب. التحليل النوعي

4. تحليل البيانات وتفسير النتائج:

5. التحقق من مصداقية الدراسة

أدوات الدراسة :

تعتمد هذه الدراسة على مجموعة من الأدوات المتنوعة التي تهدف إلى جمع وتحليل البيانات المتعلقة بإدارة الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية. تتضمن الأدوات التي سيتم استخدامها في الدراسة ما يلي:

1. الاستبيانات
2. المقابلات
3. دراسات المستندات والتقارير السنوية للشركات المشغلة لشبكات الاتصال الافتراضية

حدود الدراسة:

تشير حدود الدراسة إلى القيود التي قد تؤثر على نطاق البحث وتحديد الجوانب التي يمكن دراستها ومقاييسها. تعد هذه الحدود أساسية لفهم مدى تعميم النتائج والقيود التي قد تؤثر على قدرة الدراسة في تقديم استنتاجات عامة. بناءً على موضوع الدراسة "إدارة الأمن السيبراني في الشركات المشغلة لشبكات الاتصال الافتراضية"، يمكن تحديد عدة حدود للدراسة، تتراوح بين الحدود الزمنية والجغرافية والموضوعية.

1. الحدود الزمنية
2. الحدود الجغرافية
3. الحدود الموضوعية
4. حدود البيانات
5. الحدود القانونية والتنظيمية

المراجع: