المملكة العربية السعودية
المؤسسة العامة للتدريب التقني والمهني
الإدارة العامة لتصميم وتطوير المناهج

أساسيات الأمن السيراني

مقدمة

الحمد لله وحده، نده والصلاة والسلام على من لا نبي بعده، محمد وعلى آله وصحبه، وبعد:

تسعى المؤسسة العامة للتدريب التقني والمهني لتأهيل الكوادر الوطنية المدربة القادرة على شغل الوظائف التقنية والفنية والمهنية المتوفرة في سوق العمل، ويأتي هذا الاهتمام نتيجة للتوجهات السديدة من لدن قادة هذا الوطن التي تصب في مجملها نحو إيجاد وطن متكامل يعتمد ذاتياً على موارده وعلى قوة شبابه المسلح بالعلم والإيمان من أجل الاستمرار قدماً في دفع عجلة التقدم التموي: لتصل بعون الله تعالى

المصاف الدول المتقدمة صناعياً. وقد خطت الإدارة العامة لتصميم وتطوير المناهج خطوة إيجابية تتفق مع التجارب الدولية المتقدمة في بناء البرامج التدريبية وفق أساليب علمية حديثة تحاكي متطلبات سوق العمل بكافة تخصصاته ، وقد تمثلت هذه الخطوة في مشروع إعداد المعايير المهنية الوطنية الذي يمثل الركيزة لقلبي متطلباته الأساسية في بناء البرامج التدريبية، إذ تعتمد المعايير في بنائها على تشكيل لجان تخصصية تمثل سوق العمل والمؤسسة العامة للتدريب التقني والمهني بحيث تتوافق الرؤية العلمية مع الواقع العملي الذي تفرضه متطلبات سوق العمل، لتخرج هذه اللجان في النهاية بنظرة متكاملة لبرنامج تدريبي أكثر التصاقا بسوق العمل، وأكثر واقعية في تحقيق متطلباته الأساسية. وتتناول هذه الحقيبة التدريبية – أساسيات الأمن السيبراني المتدربي للكليات التقنية والمعاهد العليا التقنية للبنات موضوعات حيوية تتناول كيفية اكتساب المهارات اللازمة لهذا التخصص.

والإدارة العامة لتصميم وتطوير المناهج وهي تضع بين يديك هذه الحقيبة التدريبية تأمل من الله عز وجل أن تسهم بشكل مباشر في تأصيل المهارات الضرورية اللازمة، بأسلوب مبسط يخلو من التعقيد. وبالاستعانة بالتطبيقات والأشكال التي تدعم عملية اكتساب هذه المهارات.

والله نسأل أن يوفق القائمين على إعدادها والمستفيدين منها لما يحبه ويرضاه: إنه سميع مجيب الدعاء

الإدارة العامة لتصميم وتطوير المناهج

تمهيد

الحمد لله رب العالمين والصلاة والسلام على رسوله محمد بن عبد الله وعلى آله وصحبه ومن اهتدى بهديه وبعد.

الأمن السيبراني، المعروف أيضًا بأمن المعلومات أو السيبرسكيورتي، هو مجال حيوي في تكنولوجيا المعلومات يهدف إلى حماية الأفراد والمؤسسات والأنظمة من التهديدات والهجمات السيبرانية. يتمثل الهدف الرئيسي للأمن السيبراني في الحفاظ على خصوصية البيانات والمعلومات، وضمان سلامتها، وتأمين استدامة الخدمات الإلكترونية.

بفعل التكنولوجيا المتقدمة، أصبحت الصناعات والمؤسسات تعتمد بشكل كبير على الأنظمة والشبكات الرقمية. وبالتالي، أصبح الأمان السيبراني أمرًا بالغ الأهمية، حيث يقوم بحماية هذه الأصول الرقمية من الاختراقات والتهديدات السيبرانية.

يهدف الأمن السيبراني في المقام الأول إلى الوقاية من الهجمات الرقمية الخطيرة والفيروسات المتطورة. يشمل ذلك مكافحة الاختراقات السيبرانية والاحتيال الإلكتروني واسترداد البيانات المسروقة. بالإضافة إلى ذلك، يشمل أيضًا اكتشاف الثغرات في الأنظمة وإصلاحها لضمان سلامة البيانات والمعلومات.

الوحدة التدريبية الأولي

أهمية الأمن السيبراني

الوحدة الأولى : أهمية الأمن السيبراني

الجدارة:

يتمكن المتدرب من معرفة مفهوم الأمن الســـيبراني وفهم الحماية من الهجمات الإلكترونية وأهمية الأمن السيبراني.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- ما هو الأمن السيبراني.
- أهمية الامن السيبراني.

الوقت المتوقع للتدريب:

١٢ ساعة.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب فهم الأمن السيبراني و أهميتة.

أهمية الأمن السيبراني

ما هو الأمن السيراني

الأمن السـيبراني (أو الأمـان السـيبراني) هو مجموعـة من الإجراءات والتقنيـات والممارسـات التي تهدف إلى حماية الأنظمة والشـبكات الإلكترونية والبيانات من التهديدات والهجمات الإلكترونية. يتعلق الأمن السـيبراني بضـمان سـلامة وسـرية المعلومات وضمان توفير توافر الخدمات الإلكترونية. إليك بعض الجوانب الرئيسية للأمن السيبراني:

1. **الحمايـة من الهجمـات الإلكترونيـة** :يتعين على منظمـات وأفراد تنفيذ إجراءات لحماية أنظمتهم وشبكاتهم من هجمات الكمبيوتر والبرامج الضارة والاختراقات.

شرح عن الحماية من الهجمات الإلكترونية بصورة مُفصّلة في شكل فقرات:

فهم الهجمات الإلكترونية:

الحمـايـة من الهجمـات الإلكترونيـة تبـدأ بـالفهم الجيـد للأنواع المختلفـة لهـذه الهجمات. يمكن أن تشمل هذه الهجمات الفيروسات والديدان وبرامج التجسس والاختراقات والهجمات الاجتماعية والاحتيالية. كل نوع من هذه الهجمات يتطلب استراتيجيات حماية مختلفة.

العتيبي, عبد الرحمن بن بجاد شـارع المرشـدي, علي, & إبراهيم ميرغني محمد. مشـرف. (2020). دور الأمن السـيبراني في تحقيق رؤية 2030 (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية).

تحديث الأنظمة والبرمجيات:

يجب أن تكون أنظمتك وبرامجك دائمًا محدّثة. تحديثات البرامج تعالج ثغرات الأمان وتقلل من فرص نجاح الهجمات. من المهم تمكين تحديث التلقائي للأنظمة والبرامج الأساسية.

استخدام جدار ناري قوي:

تكوين جدار ناري فعال يسمح بمراقبة وتصفية حركة البيانات على الشبكة. يمكنه منع الوصول غير المصرح به إلى الأنظمة والبيانات.

إعداد سياسات الوصول والصلاحيات:

ضبط سياسات الوصول والصلاحيات بحيث يتم منح الوصول إلى الموارد الحساسة فقط للأشخاص الذين يحتاجون إليها لأغراض العمل، ويتم تقييد الوصول للمستخدمين غير المصرح بهم.

توعية الموظفين:

قد يكون أهم خط الدفاع ضد الهجمات الإلكترونية هو الموظفون. يجب تدريب الموظفين على كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية والملفات المرفقة المشبوهة وكيفية التصرف بأمان عبر الإنترنت.

تنفيذ نظام مراقبة وكشف عن التهديدات:

توظيف نظام مراقبة شبكي قوي وأدوات كشف عن التهديدات يمكنهما رصد الأنشطة الغير معتادة وتحليل السجلات للكشف عن الهجمات المحتملة في وقت حقيقي.

تطبيق استراتيجية الاستجابة للحوادث:

إعداد واختبار خطة استجابة للحوادث للتعامل مع الهجمات الإلكترونية بفعالية، بما في ذلك تحديد الإجراءات والفرق المسؤولة عن التحقيق والاستجابة.

مراجعة وتقييم مستمر:

يجب مراجعة وتقييم استراتيجية الأمان بشكل دوري لضمان ملائمتها مع التهديدات الجديدة والتحديثات التكنولوجية. تحتاج إلى تكييف الإجراءات والتدابير بمرور الوقت.

الامتثال والتوجيهات القانونية:

تأكد من التوافق مع اللوائح والتشريعات المتعلقة بالأمان السيبراني وحماية البيانات في منطقتك أو صناعتك.

بتنفيذ هذه الخطوات، يمكنك تقوية الأمان السيبراني لمنظمتك والحماية من الهجمات الإلكترونية بفعالية. تذكر أن الأمان السيبراني هو جهد مستمر وشامل يتطلب الاستعداد والتحسين المستمر.

2. **إدارة الهويات والوصول** :يجب التحقق من هويات المستخدمين ومنحهم الوصول إلى الموارد الرقمية بناءً على مستوى الاختصاص والحاجة.

شرح عن إدارة الهويات والوصول (IAM) بصورة مُفصلة في شكل فقرات:

فهم إدارة الهويات والوصول:

إدارة الهويات والوصول هي عملية تحديد وتنفيذ منهجية لضبط من يمكنه الوصول إلى الموارد والمعلومات في منظمتك وكيفية الوصول إليها. تهدف

IAMإلى ضـمان أن المسـتخدمين فقط يحصـلون على الصـلاحيات والوصـول اللازمين لأغراض عملهم وبناءً على دورهم في المنظمة.

إنشاء هويات المستخدمين:

تبدأ عملية IAM بإنشـاء هويات فردية لكل مسـتخدم داخل المنظمة. هذه الهويات يجب أن تكون فريدة ومحددة بمعلومات شخصية لكل مستخدم، مثل اسم المستخدم وكلمة المرور والبريد الإلكتروني.

تحديد الصلاحيات والأدوار:

بعد إنشـاء هويات المسـتخدمين، يجب تحديد الصـلاحيات والأدوار التي سـيتم منحها لكل مسـتخدم. يمكن تعريف الأدوار بنـاءً على وظـائف ومسـؤوليات المستخدمين داخل المنظمة.

إدارة الوصول:

باستخدام أنظمةIAM ، يمكنك تنفيذ وإدارة حقوق الوصول للمستخدمين بناءً على الأدوار والصـلاحيات المعينة. هذا يشـمل منح الوصـول إلى التطبيقات والملفات وقواعد البيانات والخوادم.

ضمان الامتثال والأمان:

إدارة الهويات والوصول تساعد على ضمان الامتثال للسياسات واللوائح الأمنية وحماية المعلومات الحساسة. يمكن إعداد سياسات IAM لتفعيل متطلبات الأمان الخاصة بالمنظمة.

مراقبة وتدقيق الوصول:

توفير إمكانية مراقبة وتدقيق الوصـول يسـمح للمنظمة بمراقبة الأنشـطة التي تتم داخل النظام وتتبع من قام بالوصول إلى أي معلومة أو مورد.

إعداد الطوارئ واستعادة البيانات:

جزء من إدارة الهويات والوصـــول يتضـــمن التفكير في الاســـتجابة لحالات الطوارئ وخطط اســـتعادة البيانات. يجب تنفيذ إجراءات لإلغاء الوصـــول في حالات الخرق أو الفقدان وضمان استعادة البيانات بأمان.

التدريب والتوعية:

توجد حاجة إلى تدريب موظفي المنظمة على كيفية اســـتخدام نظام IAM وفهم السياسـات والأمان المتعلقة به. تعزيز التوعية يسـاعد في تقليل الأخطاء البشـرية وتعزيز الأمان.

مراجعة دورية وتحسين:

يجب مراجعة إعدادات IAM بشـــكل دوري لضـــمان أنها لا تزال تتناســـب مع احتياجات المنظمة وتحديثها وتحسينها بمرور الوقت.

إدارة الهويات والوصـول هي جزء أسـاسـي من اسـتراتيجية الأمان السـيبراني وتقليل مخاطر الهجمات الإلكترونية وحماية البيانات الحساسة.

3. **تحليل الأمان** :يجب مراقبة الأنشطة السيبرانية والكشف عن التهديدات والهجمات المحتملة بشكل فعّال.

شرح عن تحليل الأمان بصورة مُفصّلة في شكل فقرات:

فهم تحليل الأمان:

تحليل الأمان هو عملية تقييم النظام أو التطبيق لتحديد ضـــعف الأمان ومخاطر الهجمات الإلكترونية المحتملة. يهدف تحليل الأمان إلى تحديد الثغرات والمشاكل الأمنية وتصنيفها وتقديم توصيات لتعزيز الأمان.

مراجعة النظام:

يجب أن تبدأ عملية تحليل الأمان بفحص النظام أو التطبيق بمفردك أو باســتخدام أدوات تحليل الأمان المتاحة. هذا يشـــمل تقييم هندســـة الأمان وتكوين الأمان وسياسات الأمان.

تصنيف المخاطر:

بناءً على النتائج المســـتنتجة من المراجعة، يجب تصـــنيف المخاطر بحيث يتم تحديد مدى خطورة كل ثغرة أمنية والتأثير المحتمل على النظام أو التطبيق.

تحليل المشاكل الأمنية:

بعد تصـنيف المخاطر، يجب تحليل المشـاكل الأمنية بعمق. هذا يشـمل فهم كيفية استغلال الثغرات المكتشفة وما إذا كان يمكن للمهاجمين الوصول إلى البيانات أو التأثير على النظام.

توصيات التحسين:

بناءً على نتائج التحليل، يجب إعداد توصيات لتحسين الأمان. يمكن أن تشمل هذه التوصيات تحسينات في الهندسة الأمانية، والإعدادات، وسياسات الأمان، وتوجيهات الأمان للمستخدمين.

تنفيذ التوصيات:

بعد تطوير التوصيات، يجب تنفيذها بعناية. هذا يتضمن تعديل النظام أو التطبيق وتكوينه وتدريب المستخدمين على السلوكيات الأمنية.

اختبار واختبار الأمان:

يجب اختبار النظام أو التطبيق بعد تنفيذ التوصيات للتحقق من فعالية التحسينات والكشف عن أي مشكلات أمنية متبقية.

مراجعة دورية:

تحليل الأمان هو عملية متكررة ومستمرة. يجب مراجعة الأمان بشكل دوري لضمان أن النظام أو التطبيق لا يزال محميًا بشكل فعال ضد التهديدات الجديدة والمتغيرة.

توثيق العملية:

يجب توثيق جميع مراحل عملية تحليل الأمان بما في ذلك النتائج، والتصنيف، والتحليل، والتوصيات، والتنفيذ، والاختبار. هذا يساعد في تتبع الأمان والامتثال.

تحليل الأمان هو جزء أساسي من استراتيجية الأمان السيبراني ويساعد في تحديد ومعالجة الثغرات الأمنية قبل أن تتسبب في هجمات إلكترونية أو انتهاكات أمنية.

4. **التدريب والتوعية** :تعتمد الأمان السيبراني أيضًا على تعليم وتوعية الموظفين والمستخدمين بشأن مخاطر الأمان السيبراني وكيفية التصرف بأمان عبر الإنترنت.

شرح عن التدريب والتوعية بأمان المعلومات بصورة مُفصّلة في شكل فقرات:

أهمية التدريب والتوعية بأمان المعلومات:

التدريب والتوعية بأمان المعلومات هما عنصران أساسيان في استراتيجية الأمان السيبراني. فالعديد من الهجمات الإلكترونية تحدث بسبب أخطاء بشرية أو تصرفات غير حذرة. التدريب والتوعية يمكنهما تقليل هذه المخاطر وزيادة الوعي بأمان المعلومات.

تصميم برامج التدريب والتوعية:

عند تصميم برامج التدريب والتوعية، يجب أن تكون مخصصة لاحتياجات المؤسسة والموظفين. يمكن أن تشمل هذه البرامج تدريبًا على كيفية التعرف على هجمات البريد الإلكتروني الاحتيالية والتعامل معها، وكذلك التعرف على أمان كلمات المرور واستخدامها بشكل آمن.

التوعية بالتهديدات السيبرانية:

يجب تعزيز التوعية بأنواع مختلفة من التهديدات السيبرانية وكيفية التعامل معها. يمكن تضمين توعية حول الفيروسات وبرامج التجسس والهجمات الاجتماعية والتهديدات المتقدمة المستمرة.

تعزيز السلوك الآمن:

يجب توجيه الموظفين والمستخدمين نحو السلوك الآمن عبر الإنترنت وعلى الأجهزة. يشمل ذلك عدم مشاركة كلمات المرور ومعلومات حساسة مع الأشخاص الغير معتمدين وعدم فتح مرفقات رسائل البريد الإلكتروني المشبوهة.

التدريب العملي:

يفضل أن تشمل برامج التدريب تدريبًا عمليًا يتيح للمشاركين ممارسة مهارات الأمان على أرض الواقع. يمكن أن يتضمن ذلك محاكاة هجمات وكيفية التعامل معها.

تقييم التفاعل:

يجب تقييم فعالية برامج التدريب والتوعية باستمرار. يمكن استخدام استبيانات واختبارات لقياس مدى استيعاب المشاركين وفهمهم للمواد والقضايا المتعلقة بالأمان.

تحديث المحتوى:

يجب تحديث المحتوى بانتظام للتأكد من أنه يتناسب مع التهديدات الجديدة والتحديثات التكنولوجية. العالم السيبراني متغير بسرعة، لذلك يجب أن تتم متابعة التغييرات.

تشجيع التواصل:

تشجيع التواصل بين الموظفين والمستخدمين حول الأمان السيبراني يمكن أن يساهم في تبادل المعرفة والمعلومات حول التهديدات والأمان.

المراجعة والتقييم:

يجب مراجعة برامج التدريب والتوعية بشـــكل دوري لقياس تأثيرها وتحديد المجالات التي تحتاج إلى تحسين.

التدريب والتوعية بأمان المعلومات هما جزء أساسي من الأمان السيبراني ويساهمان في حماية المنظمة من الهجمات الإلكترونية وتعزيز الوعي بأمان المعلومات بين الموظفين والمستخدمين.

5. **الامتثال والتشـــريعات** :يجب على المؤســـســـات الالتزام باللوائح والتشـــريعات المتعلقة بالأمان السيبراني وحماية البيانات.

شرح عن الامتثال والتشريعات بصورة مُفصّلة في شكل فقرات:

أهمية الامتثال والتشريعات:

الامتثال يشير إلى الالتزام بالقوانين واللوائح التي تنظم سلوك المؤسسات وحماية البيانات والأمان الســـيبراني. يُعتبر الامتثال أحد أهم جوانب الأمان الســـيبراني حيث يساعد على تقليل المخاطر والحفاظ على سمعة المؤسسة.

القوانين واللوائح المتعلقة بالأمان السيبراني:

تختلف التشـريعات واللوائح المتعلقة بالأمان السـيبراني من دولة إلى أخرى ومن صـناعة إلى أخرى. على سبيل المثال، في الولايات المتحدة، تتضـمن التشريعات مثل قانون الحماية الصحية والمعلومات الصحية الإلكترونية (HIPAA) وقانون الاتصـالات السـلكية واللاسـلكية .(CFAA) في الاتحاد الأوروبي، هناك اللائحة العامة لحماية البيانات.(GDPR)

متطلبات الامتثال:

متطلبات الامتثال تشـــمل مجموعة متنوعة من الأمور، مثل حماية البيانات الشخصية، وتأمين الشبكات والأنظمة، وإجراءات الإبلاغ عن انتهاكات البيانات، وتقديم التقارير، والتدقيق، والتوجيهات القانونية لمنظمات الأعمال.

تأثير الامتثال على الأعمال:

الالتزام بالتشريعات واللوائح يمكن أن يؤدي إلى تكاليف إضافية وزيادة التعقيدات في العمليات اليومية للمنظمة. ومع ذلك، يمكن أيضًا أن يساعد في تحسين سمعة المؤسسة وبناء الثقة لدى العملاء والشركاء التجاريين.

التوجيهات والأمان السيبراني:

الامتثال للتشريعات يتطلب أيضًا الامتثال لمتطلبات الأمان السيبراني. يجب تنفيذ ســياســات وإجراءات أمان مثل تشــفير البيانات، وإدارة هويات المســتخدمين، واستجابة لحالات الطوارئ السيبرانية لضمان الامتثال الكامل.

التدقيق والتقييم:

من المهم أن تقوم المؤسسة بتقييم مدى امتثالها بشكل دوري وإجراء تدقيق داخلي أو استعانة بمراجعين خارجيين للتحقق من الامتثال والتحسين المستمر.

العقوبات على عدم الامتثال:

عدم الامتثال للتشريعات قد يعرض المؤسسة لعواقب قانونية وعقوبات مالية. قد تفرض غرامات كبيرة على المؤسسات التي تنتهك حقوق الخصوصية أو تعرض البيانات للخطر.

التحديات المستقبلية:

مع التقدم التكنولوجي والتهديدات السـيبرانية المتطورة، من المتوقع أن تزداد تشـريعات الأمان السـيبراني والمتطلبات التنظيمية. من المهم للمؤسـسـات مواكبة هذه التطورات وتكييف استراتيجيات الأمان والامتثال وفقًا لها.

الامتثال والتشـريعات هما عنصـران مهمان في عالم الأمان السـيبراني والمسـاهمين في الحفاظ على البيانات والأنظمة آمنة ومحمية.

6. **الاستجابة لحوادث الأمان** :يجب وضع خطط استجابة للتعامل مع حوادث الأمان السيبراني والتحقيق فيها وإصلاحها.

شرح عن الاستجابة لحوادث الأمان بصورة مُفصّلة في شكل فقرات:

أهمية استجابة حوادث الأمان:

استجابة حوادث الأمان هي عملية أساسية تهدف إلى التعامل مع وتقييم واحتواء الحوادث الأمنية والسـيبرانية التي يمكن أن تؤثر على أمان المعلومات والأنظمة. تلعب هذه العملية دورًا حاسـمًا في تقليل التأثير السـلبي للهجمات والاسـتفادة منها لتعزيز الأمان.

إعداد خطة استجابة لحوادث الأمان:

الخطوة الأولى في استجابة حوادث الأمان هي إعداد خطة محكمة ومحددة لكيفية التعامل مع الحوادث. يجب أن تشـمل هذه الخطة الإجراءات المحددة للإبلاغ عن الحوادث والتحقيق واستجراءات الاستجابة الفورية.

الاستجابة الفورية:

عندما تحدث حادثة أمنية، يجب الاستجابة على الفور. هذا يتضمن عزل النظام المتأثر وإيقاف الهجوم إذا كان ممكنًا، ومراقبة الحادث لتحديد نطاق الأضرار والتحقيق في كيفية حدوثه.

تقييم التأثير:

بمجرد استقرار الحادثة، يجب تقدير التأثير الذي أحدثه الحادث. هل تم التسلل إلى البيانات؟ هل تم تعطيل الخدمات؟ تقدير التأثير يساعد في تحديد الخسائر وتحديد الخطوات اللاحقة.

الإبلاغ والاتصال:

يجب إبلاغ الأطراف المعنية بسرعة، وهذا يمكن أن يشمل فريق استجابة الأمان الداخلي والسلطات المحلية والجهات التنظيمية المعنية إذا كان ذلك مطلوبًا قانونيًا. الاتصال السليم يساعد في تنسيق الاستجابة وتخفيف التأثير.

التحقيق والتحليل:

يتعين إجراء تحقيق دقيق لفهم كيفية ومتى ولماذا حدث الحادث. يساعد هذا التحليل في تحديد الضعف في الأمان وكيفية تحسينه لتجنب تكرار الحوادث في المستقبل.

تصحيح الثغرات:

بناءً على نتائج التحقيق، يجب اتخاذ إجراءات لتصحيح الثغرات وتقوية الأمان. هذا يمكن أن يتضمن تحديث البرمجيات وتعزيز إجراءات الحماية وتدريب الموظفين على السلوكيات الآمنة.

الاستعادة والاستمرارية:

يجب تحقيق الاستعادة بسرعة لضمان استئناف الأنشطة الأساسية للمؤسسة. يجب أن تشمل خطة الاستجابة أيضًا استراتيجيات الاستمرارية لضمان استمرار العمليات الأساسية في حالة وقوع حوادث.

تقييم ما بعد الحادث:

بعد استجابة الحادث، يجب تقييم العملية بأكملها وتحليل كيفية التعامل مع الحادث وما يمكن تحسينه. هذا يساعد في التحضير للمستقبل وتعزيز قدرة المؤسسة على التعامل مع حوادث أمنية مماثلة.

استجابة حوادث الأمان هي عملية حيوية للمؤسسات للتأكد من أنها قادرة على التعامل مع التهديدات السيبرانية والحفاظ على استقرار أعمالها وحماية البيانات والأنظمة الحساسة.

العتيبي, عبد الرحمن بن بجاد شارع المرشدي, علي, & إبراهيم ميرغني محمد. مشرف. (2020). دور الأمن السيبراني في تحقيق رؤية 2030 (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية).

مرجع:

- National Institute of Standards and Technology (NIST). "Cybersecurity Framework." المصدر : https://www.nist.gov/cyberframework

تدريبات

أسئلة اختيار من متعدد:

1. ما هو الهدف الرئيسي للأمن السيبراني؟
   - أ) الهجمات الإلكترونية
   - ب) حماية الأنظمة والبيانات
   - ج) تطوير البرمجيات
2. ما الذي يشمله مجال الأمن السيبراني بالإضافة إلى الحماية من الهجمات؟
   - أ) الطب البشري
   - ب) إصلاح السيارات
   - ج) الوعي الأمني واكتشاف الثغرات
3. ما هو الجانب السلبي الرئيسي للهجمات السيبرانية؟
   - أ) تأمين البيانات
   - ب) فقدان البيانات والتلف
   - ج) تحسين الأمان السيبراني
4. ما هي الجريمة السيبرانية؟
   - أ) الأنشطة الرسمية للحكومة
   - ب) الأنشطة التجارية القانونية
   - ج) الأنشطة غير القانونية عبر الإنترنت
5. ما هي أحد أهداف الأمن السيبراني؟
   - أ) زيادة التعقيد في الأنظمة

- ب) ضمان سلامة وسرية البيانات
- ج) التحكم في الشهرة الشخصية

6. كيف يساهم الأمن السيبراني في الحفاظ على الخصوصية؟
   - أ) من خلال نشر المزيد من البيانات
   - ب) من خلال حماية البيانات من الوصول غير المصرح به
   - ج) من خلال نشر كلمات المرور على نطاق واسع
7. ماذا يعني مصطلح "الجرائم السيبرانية"؟
   - أ) جرائم ترتكب في العالم الواقعي فقط
   - ب) جرائم تشمل الأنشطة الإلكترونية الغير قانونية
   - ج) جرائم ترتكب ضد الأشخاص الشهيرين فقط
8. كيف يمكن أن تؤثر الهجمات السيبرانية على الأنظمة الحيوية مثل الطاقة والصحة؟
   - أ) لا تؤثر بأي شكل من الأشكال
   - ب) يمكن أن تتسبب في توقف الخدمات الحيوية
   - ج) تزيد من كفاءة الأنظمة
9. ما هو الجانب الإيجابي للأمن السيبراني على الاقتصاد والأعمال؟
   - أ) يزيد من التكاليف ويقلل من الأرباح
   - ب) يعزز الثقة ويساهم في الاستدامة الاقتصادية
   - ج) لا توجد له تأثيرات اقتصادية
10. ما هو دور التوعية الأمنية في مجال الأمن السيبراني؟
    - أ) الحصول على المعلومات فقط

- ب) زيادة الوعي حول مخاطر الأمان السيبراني وكيفية الوقاية منها
- ج) ترويج منتجات تجارية

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: الأمن السيبراني يهدف إلى حماية الأنظمة والبيانات فقط.
2. صحيح أو خطأ: الجريمة السيبرانية تشمل أنشطة الإنترنت القانونية.
3. صحيح أو خطأ: الهجمات السيبرانية يمكن أن تتسبب في فقدان البيانات والتلف.
4. صحيح أو خطأ: الأمن السيبراني لا يؤثر على القطاع الاقتصادي.
5. صحيح أو خطأ: التوعية الأمنية تساهم في زيادة الوعي بمخاطر الأمان السيبراني.

الوحدة التدريبية الثانية

المخاطر والتهديدات والثغرات السيبرانية

الوحدة الثانية : المخاطر والتهديدات والثغرات السيبرانية

الجدارة:

يتمكن المتدرب من معرفة المخاطر والتهديدات والثغرات السيبرانية.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- المخاطر والتهديدات.
- الثغرات السيبرانية.

الوقت المتوقع للتدريب:

١٢ ساعة.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب فهم المخاطر والتهديدات والثغرات السيبرانية.

المخاطر والتهديدات والثغرات السيبرانية

مع اعتماد المؤسسات بشكل متزايد على أنظمة المعلومات في أعمالها، يتزايد احتمالية التعرض لمخاطر الأمن السيبراني. هذا يعني أن جميع المنظمات معرضة لخطر الهجمات السيبرانية، وبالتالي يصبح تقييم وإدارة هذه المخاطر أمرًا بالغ الأهمية.

مفهوم مخاطر الأمن السيبراني :مخاطر الأمن السيبراني تشمل التهديدات والهجمات الإلكترونية التي يمكن أن تعرض أنظمة المؤسسات وخدماتها الإلكترونية للخطر. هذه المخاطر لا تؤثر فقط على تقنيات وأجهزة المؤسسات، بل تسبب أيضًا خسائر مالية وتلحق أضرارًا بسمعة المؤسسة.

إدارة مخاطر الأمن السيبراني :إدارة مخاطر الأمن السيبراني تتضمن مجموعة من الخطوات التي يجب اتخاذها بشكل دوري لمواجهة ومعالجة التهديدات الإلكترونية. يشمل ذلك رصد وتحليل وتقييم المخاطر، ومن ثم وضع خطط لمواجهتها باستخدام التقنيات والأدوات الحديثة. إدارة المخاطر السيبرانية تتطلب نظرة شاملة للمخاطر وتعاوناً من جميع أفراد العمل، وليس فقط من أفراد إدارة المخاطر.

سعيد إسماعيل, & محمد. (2022). التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة–دراسة في القانون القطري والمقارن.

تعتمد إدارة مخاطر الأمن السيبراني على استراتيجيات تساعد على تحديد أولويات المخاطر التي يجب التركيز عليها، وذلك لرصد التهديدات الأكثر ضررًا ومواجهتها في الوقت المناسب.

دور فريق أمن تكنولوجيا المعلومات :فريق أمن تكنولوجيا المعلومات مسؤول عن تنفيذ سياسات إدارة مخاطر الأمن السيبراني. يجب على أفراد هذا الفريق أن يكونوا على دراية بأحدث أساليب الهجمات والتهديدات المحتملة لأجهزة الشبكة. يجب أن يقوموا بتحديث أساليب الدفاع ومراقبة تنفيذ السياسات الأمنية للتحقق من فاعليتها في منع التهديدات.

عوامل زيادة مخاطر الأمن السيبراني :

هناك عدة عوامل يمكن أن تزيد من مخاطر الأمن السيبراني، منها:

1. حدوث عطل في الشبكات الذي يمكن أن يؤدي إلى فقدان البيانات الحساسة.
2. استخدام أجهزة المؤسسة من أماكن بعيدة مثل السفر أو المنازل.
3. عدم الالتزام بسياسات الأمن السيبراني وعدم مراجعتها بانتظام.
4. إهمال تحديث كلمات المرور بانتظام.
5. وصول أشخاص غير مختصين إلى نظام الأمن السيبراني والتحكم في الخيارات الإدارية.
6. استخدام أجهزة المؤسسة لإجراء المعاملات المالية عبر الإنترنت مثل تحويل الأموال.
7. الوصول إلى نظام الأمن السيبراني من مواقع أخرى من قبل العملاء.

من الضروري توعية العاملين بأهمية الأمان السيبراني والالتزام بالسياسات والإجراءات الأمنية للمساهمة في الحد من مخاطر الأمن السيبراني وضمان سلامة الأنظمة والبيانات الحساسة.

تتعرض المؤسسات لمجموعة متنوعة من مخاطر الأمن السيبراني، ومن بين هذه المخاطر الشهيرة يمكن التعرف على ما يلي:

1. التجسس :هذا النوع من المخاطر يتمثل في سرقة المعلومات الحساسة من الأنظمة الإلكترونية للمؤسسات من خلال اختراق حركة المرور والوصول غير المصرح به إلى المعلومات المرسلة والمستقبلة بين الأجهزة المختلفة.
2. سرقة كلمات المرور :يعتمد المخترقون عادةً على سرقة كلمات المرور للوصول إلى البيانات الحساسة للمستخدمين. يمكن أن تحدث هذه السرقة عن طريق التنصت أو عبر محاولات التخمين. وتكون كلمات المرور السهلة هدفا سهلا للاختراق.
3. البرامج الضارة :البرامج الضارة هي برامج تسبب أضرارًا للأجهزة أو تسرق المعلومات. يهدف المجرمون الإلكترونيون إلى إطلاق هذه البرامج لسرقة البيانات الحساسة للمستخدمين، وقد تكون هذه البيانات شخصية أو مالية.
4. عمليات الاحتيال :يعتمد المجرمون الإلكترونيون على عمليات الاحتيال للحصول على بيانات المستخدمين. يقومون بإرسال رسائل غير صحيحة عبر البريد الإلكتروني تدعو المستخدمين لتقديم بياناتهم الشخصية. هذا النوع من الاحتيال يعد واحدًا من أكثر الطرق نجاحًا في مخاطر الأمن السيبراني.
5. هجمات على المواقع :بعض المهاجمين السيبرانيين يستهدفون المواقع الغير مشفرة باستخدام أكواد تعطيل تجعل الموقع غير قادر على الاستجابة بشكل صحيح. يقومون بإرسال هذه الأكواد للموقع بمجرد الوصول إليه بهدف تعطيل الخدمة أو سرقة المعلومات.
6. الهندسة الاجتماعية :في عمليات الهندسة الاجتماعية، يستخدم المحتالون وسائل الإقناع لاستدراج المعلومات من المستخدمين. يمكنهم التنكر باسم شخص آخر والتحايل على المستخدمين عبر وسائل التواصل الاجتماعي أو طلب بياناتهم الشخصية. هذا النوع من الهجمات يعتمد على مهارة الإقناع.

من الضروري توعية الأفراد بأمور الأمان السيبراني والالتزام بالسياسات والتدابير الأمنية للمساهمة في تقليل مخاطر الأمن السيبراني وحماية الأنظمة والبيانات الحساسة.

مراحل عملية إدارة مخاطر الأمن السيبراني قبل وقوع المخاطر:

1. تحديد الأصول وبيئة تكنولوجيا المعلومات :قبل أي شيء آخر، يجب تحديد جميع الأصول والموارد التقنية التي تمتلكها المؤسسة وتستخدمها في أعمالها. هذا يتضمن التطبيقات، والأنظمة، والأجهزة المختلفة. يجب أيضًا فحص بيئة تكنولوجيا المعلومات بما في ذلك الشبكات ونقاط النهاية والبيانات والأجهزة التي يمكن استخدامها في هجمات.
2. تحديد المخاطر وتقييمها :بمعرفة الأصول، يمكن البدء في تحديد المخاطر المحتملة. يتم ذلك عن طريق تقييم مدى تعرض هذه الأصول للتهديدات المحتملة وتقدير مدى تأثير هذه التهديدات على عمل المؤسسة. يمكن استخدام مصطلحات مثل مستوى التهديد والضرر المالي المحتمل لتصنيف المخاطر.
3. وضع استراتيجية قوية لإدارة مخاطر الأمن السيبراني :بناءً على تقييم المخاطر، يجب وضع استراتيجية محكمة لإدارة هذه المخاطر. هذه الاستراتيجية يجب أن تشمل تحديد الأولويات، وتخصيص الموارد، ووضع سياسات وإجراءات أمنية، وتحديد الفرق المسؤولة عن تنفيذ هذه السياسات.
4. تنفيذ الحلول ورصد الفاعلية :بعد وضع الاستراتيجية، يجب تنفيذ الحلول الأمنية المختارة. هذا يمكن أن يشمل تحديث البرمجيات، وتعزيز التدريب للموظفين، وتكييف السياسات والإجراءات. يجب أيضًا رصد فعالية هذه الحلول لضمان تحقيق الأمان المطلوب.
5. تقييم وتحسين مستمر :عملية إدارة مخاطر الأمن السيبراني ليست عملية مرة واحدة، بل هي دورية ومستمرة. يجب استعراض وتحسين استراتيجيات الأمان بناءً على التهديدات الجديدة والتغيرات في بيئة تكنولوجيا المعلومات.

يجب أيضًا تقديم التدريب والتوعية المستمرة للموظفين حول مخاطر الأمن السيبراني.

باختصار، إدارة مخاطر الأمن السيبراني تتطلب التعرف على الأصول وتقييم المخاطر ووضع استراتيجية وتنفيذ الحلول ومراقبة الفاعلية بشكل مستمر. هذا العمل الدائم يساعد في تعزيز الأمان السيبراني وحماية المؤسسة من التهديدات السيبرانية المتزايدة.

مراحل عملية إدارة مخاطر الأمن السيبراني بعد حدوث مخاطر سيبرانية:

1. تحديد المخاطر :بعد حدوث مخاطر سيبرانية، يقوم فريق إدارة المخاطر بتحديد التهديدات المحتملة سواء في الوقت الحالي أو في المستقبل. يشتمل ذلك على تحليل البيانات والبرامج والأجهزة المتأثرة.
2. الحماية من المخاطر :تهدف هذه المرحلة إلى حماية البيانات والبرامج والأجهزة الخاصة بالمنظمة من الأضرار الناتجة عن المخاطر السيبرانية. ذلك يتضمن تعزيز التدابير الأمنية وتحسين السياسات والإجراءات الأمنية.
3. كشف المخاطر :يجب تنفيذ نظم كشف عن المخاطر لرصد الأنشطة والتهديدات السيبرانية المحتملة. يشمل ذلك تحليل سجلات النشاط والإبلاغ عن الحوادث الأمنية.
4. الاستجابة للمخاطر :بمجرد اكتشاف التهديدات السيبرانية، يتعين على المنظمة الاستجابة بسرعة واتخاذ إجراءات لمواجهة المخاطر. ذلك يتضمن عزل التهديد والتعافي من الأضرار والتعامل مع الهجوم بشكل فعال.
5. التعافي من المخاطر :بعد معالجة المخاطر والتعامل مع التهديدات، يجب على المنظمة العمل على استعادة الأنظمة والبيانات إلى حالتها الطبيعية. تشمل هذه المرحلة تقييم الأضرار وتحسين إجراءات الأمان لمنع حدوث تهديدات مماثلة مستقبلاً.

6. التقييم والتحسين المستمر :يجب أن تكون إدارة مخاطر الأمن السيبراني عملية مستمرة ودورية. يجب تحديث سياسات الأمان والتدابير الوقائية بناءً على التقييم المستمر للمخاطر والتهديدات الجديدة.

باختصار، إدارة مخاطر الأمن السيبراني بعد حدوث المخاطر تتضمن تحديد وحماية وكشف واستجابة وتعافي وتقييم وتحسين مستمر للأمان السيبراني لضمان استدامة وحماية المنظمة من التهديدات السيبرانية.

خطوات تقييم المخاطر السيبرانية:

الخطوة الأولى: تحديد قيمة المعلومات لا يمكن حماية ما لا تعرفه. لذلك، يجب أن تبدأ بتحديد البيانات والمعلومات الحساسة التي تمتلكها المنظمة وتقييم قيمتها. هذه الخطوة تساعد في فهم أهمية المعلومات والأصول التي تحتاج إلى الحماية.

الخطوة الثانية: تحديد أولويات الأصول بناءً على تحديد الأصول، يجب تحديد الأولويات بناءً على أهميتها وتأثيرها على العمليات التنظيمية. هذا يشمل إنشاء قائمة بالأصول الحرجة التي يجب تقييمها بأفضل الطرق.

الخطوة الثالثة: تحليل المخاطر في هذه الخطوة، يتعين عليك تحليل المخاطر وتقدير احتمالية وتأثير كل مخاطر الأمن السيبراني. يمكن استخدام مقاييس مثل مقياس تقييم المخاطر لتصنيف المخاطر بناءً على معايير محددة.

الخطوة الرابعة: تحديد نقاط الضعف يتعين عليك تحديد نقاط الضعف في بنيتك التحتية وأنظمتك. يمكن ذلك من خلال تقييم الثغرات الأمنية والضعف التي يمكن أن تستغلها المخاطر السيبرانية.

الخطوة الخامسة: تحليل الضوابط قم بمراجعة وتحليل الضوابط الأمنية الموجودة لديك، وتحقق من فعاليتها في تقليل المخاطر. يمكن أيضًا تحسين الضوابط الحالية أو إضافة ضوابط جديدة إذا كان ذلك ضروريًا.

الخطوة السادسة: حساب تقييم المخاطر قم بحساب تقييم المخاطر لكل مخاطر الأمن السيبراني المحددة. يشمل ذلك تحديد مستوى التهديد واحتمالية استغلاله

وتقدير التأثير الناتج عنه. يمكن استخدام هذه المعلومات لتصنيف المخاطر وتحديد الأولويات.

الخطوة السابعة: التوثيق لا تنسى توثيق جميع النتائج والمعلومات المتعلقة بتقييم المخاطر. يجب أن تكون هذه الوثائق متاحة للإدارة والفرق المعنية وتحديثها بشكل منتظم.

عملية تقييم المخاطر السيبرانية يجب أن تتم بانتظام وتتكرر لضمان استمرار تحليل وتقييم المخاطر بما يتناسب مع التطورات التكنولوجية والبيئية.

المخاطر الأمنية والامتثال:

المخاطر الأمنية تشير إلى عملية رصد وتقييم التهديدات الإلكترونية المستهدفة لبيانات وبرامج وأجهزة المؤسسات، والجهود المبذولة لتنفيذ خطط للحد من هذه المخاطر، بالإضافة إلى استخدام وسائل الحماية من المخاطر الإلكترونية.

أما الامتثال، فيشير إلى الالتزام بالشروط الصناعية والتنظيمية، فضلاً عن الشروط القانونية مثل اللائحة العامة لحماية البيانات (GDPR) وغيرها من اللوائح التي تنظم التعامل مع البيانات وحمايتها والامتثال لها.

أهمية المخاطر الأمنية والامتثال :تحقق المخاطر الأمنية والامتثال العديد من الفوائد الهامة للمؤسسات، ومن أبرزها:

1. التخفيف من المخاطر: يساعد التركيز على إدارة المخاطر الأمنية والامتثال في تقليل المخاطر المرتبطة بالأعمال والتي تشمل المخاطر التجارية والتقنية والقانونية.
2. حماية البيانات والأصول: تساهم جهود الأمان والامتثال في حماية البيانات والبرامج والأصول التنظيمية من التهديدات والهجمات الإلكترونية.
3. الامتثال للقوانين واللوائح: يساعد الامتثال في تجنب المسائل القانونية والعقوبات المالية المحتملة بسبب عدم الامتثال للقوانين واللوائح السارية.

4. حماية السمعة: من خلال الالتزام بالمعايير والممارسات الأمنية والامتثال للمتطلبات القانونية، يمكن للمؤسسات حماية سمعتها ومصداقيتها.

إدارة المخاطر في أمن المعلومات :إدارة المخاطر في أمن المعلومات تعمل على حماية نظم وبيانات المؤسسات من التهديدات الأمنية. تشمل هذه العملية الخطوات التالية:

1. تحديد المخاطر: يتضمن ذلك تحديد الضوابط والبيانات والأصول المهمة وتحليل التهديدات المحتملة ونقاط الضعف.
2. التقييم: تشمل هذه المرحلة جمع المعلومات ذات الصلة بالمخاطر المحددة لتحليلها وتصنيفها وتقدير تأثيرها.
3. المعالجة: تتضمن هذه المرحلة اتخاذ الإجراءات لمعالجة المخاطر، سواءً بإصلاحها بشكل كامل أو جزئي أو تقليل تأثيرها.
4. التواصل مع المسؤولين: يتطلب ذلك التواصل مع أصحاب القرار داخل المؤسسة لإبلاغهم بتفاصيل المخاطر والتكلفة المرتبطة بمعالجتها.
5. المراقبة: يتعين مراقبة تنفيذ إجراءات إدارة المخاطر للتأكد من فاعليتها وتحديثها بشكل دوري.

باختصار، إدارة المخاطر الأمنية والامتثال هي عنصر أساسي لحماية المؤسسات من التهديدات السيبرانية والامتثال للمعايير واللوائح الصناعية والقانونية. يجب أن تكون هذه الجهود جزءًا من استراتيجية الأمان والتخطيط التكنولوجي لضمان استدامة الأعمال وحماية البيانات والأصول.

سعيد إسماعيل, & محمد. (2022). التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة–دراسة في القانون القطري والمقارن.

تدريبات

أسئلة اختيار من متعدد:

1. ما هي مخاطرة سيبرانية شائعة تستهدف الحصول على معلومات سرية من خلال إرسال رسائل تأخذ مظهر رسائل موثوقة؟
   - أ) البريد السام
   - ب) الفيروسات
   - ج) الاحتيال الاجتماعي
2. ما هي التهديدات السيبرانية التي تستغل الثغرات في البرمجيات أو الأنظمة للوصول إلى البيانات؟
   - أ) الفيروسات
   - ب) الاحتيال الاجتماعي
   - ج) الهجمات عبر البريد الإلكتروني
3. ما هي التهديدات التي تهدف إلى إلحاق الضرر بأنظمة الكمبيوتر وتشويه البيانات؟
   - أ) الاحتيال الاجتماعي
   - ب) البرمجيات الخبيثة(Malware)
   - ج) هجماتDDoS
4. ما هي الثغرة التي تتيح للمهاجم الوصول غير المصرح به إلى النظام عن طريق تمرير بيانات غير صالحة؟
   - أ SQL Injection)
   - ب) الفيروسات
   - ج) الاحتيال الاجتماعي

5. ما هي التهديدات التي تستهدف تشفير الملفات وابتزاز الأموال من المستخدمين؟
   - أ) الاحتيال الاجتماعي
   - ب) هجماتDDoS
   - ج) برامج الفدية(Ransomware)
6. ما هي المخاطرة التي تنطوي على استغلال الأمان الضعيف لأجهزة الإنترنت المتصلة بها أجهزة ذكية مثل الكاميرات وأجهزة التوجيه؟
   - أ) البرمجيات الخبيثة(Malware)
   - ب) هجماتIoT
   - ج) الاحتيال الاجتماعي
7. ما هو التهديد الذي يهدف إلى استنساخ موقع ويب مزيف للتسبب في الاحتيال على المستخدمين واستغلال معلوماتهم؟
   - أ) الفيروسات
   - ب) الاحتيال الاجتماعي
   - ج) هجماتPhishing
8. ما هي التهديدات التي تستهدف تدمير البنية التحتية للشبكة أو الخوادم؟
   - أ) الاحتيال الاجتماعي
   - ب) هجماتDDoS
   - ج) البرمجيات الخبيثة(Malware)
9. ما هو نوع التهديد الذي يعتمد على تجميد أنظمة الكمبيوتر والمطالبة بفدية لإعادة فتحها؟
   - أ) الاحتيال الاجتماعي

- ب) البرمجيات الخبيثة(Malware)
- ج) هجمات التصيّد السحابي

10. ما هي الثغرة التي يتم استغلالها لسرقة معلومات تسجيل الدخول وكلمات المرور عن طريق تسجيل المفاتيح المطبوعة على لوحة المفاتيح؟

- أ) Keylogger
- ب) الفيروسات
- ج) هجماتDDoS

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: الاحتيال الاجتماعي هو نوع من التهديدات السيبرانية يستهدف التأثير على نظام الكمبيوتر.
2. صحيح أو خطأ: هجمات DDoS تهدف إلى تشويه البيانات وتدمير البنية التحتية.
3. صحيح أو خطأ: البرمجيات الخبيثة (Malware) تشمل الفيروسات وبرامج التجسس.
4. صحيح أو خطأ: هجمات Phishing تستخدم رسائل مزيفة للاحتيال على المستخدمين والحصول على معلوماتهم.
5. صحيح أو خطأ Keylogger :هو نوع من الثغرات السيبرانية يستخدم لتسجيل معلومات تسجيل الدخول.

الوحدة التدريبية الثالثة

المحافظة علي السرية والسلامة والتوافر

الوحدة الثالثة : المحافظة علي السرية والسلامة والتوافر

الجدارة:

يتمكن المتدرب من المحافظة علي السرية والسلامة والتوافر.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- المحافظة علي السرية والسلامة والتوافر

الوقت المتوقع للتدريب:

6 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب كيفية المحافظة علي السرية والسلامة والتوافر.

المحافظة علي السرية والسلامة والتوافر

أمن المعلومات

هو مجموعة الإجراءات والممارسات التي تهدف إلى حماية المعلومات والمحافظة عليها من التهديدات الخارجية، مثل الإتلاف أو السرقة أو التخريب. يتمثل هدف أمن المعلومات في ضمان سلامة وسرية المعلومات والبيانات، وذلك باستخدام تقنيات وأساليب متعددة لمنع واكتشاف واستجابة للتهديدات والاختراقات الأمنية.

تاريخ أمن المعلومات:

تاريخ أمن المعلومات يمتد إلى فترة طويلة منذ بداية التواصل وتبادل المعلومات بين البشر. في البداية، كان أمن المعلومات يتعلق بحماية المعلومات المادية والوثائق الهامة من السرقة أو الكشف غير المصرح به. مع تطور التكنولوجيا وظهور وسائل الاتصال الإلكتروني، أصبح أمن المعلومات يشمل أيضًا البيانات الرقمية والمعلومات المخزنة على الأجهزة الإلكترونية والشبكات.

بدر الحيمودي. (2023). الأمن السيبراني وحماية الأنظمة المعلوماتية. North African Journal of Scientific Publishing (NAJSP), 174-189.

على مر العقود، شـــهدت مفاهيم أمن المعلومات تطورًا كبيرًا، وأصـــبحت تشـــمل مجموعة متنوعة من التحديات والتهديدات مثل الهجمات الســـيبرانية والاختراقات والبرمجيات الخبيثة. وتطورت الأســـاليب والتقنيات المســـتخدمة في أمن المعلومات بما يتناســـب مع هذه التحديات، مما أدى إلى تطوير مجموعة متنوعة من أدوات الحماية والتشفير وأنظمة الكشف عن التهديدات.

الفرق بين الأمن السيبراني وأمن المعلومات:

الأمن الســـيبراني (Cybersecurity) هو جزء من أمن المعلومات (Information Security)ويتعامل بشـــكل خاص مع حماية النظم الإلكترونية والشبكات والبيانات الرقمية من التهديدات السيبرانية. إليك بعض الفروق الرئيسية بين الأمن السيبراني وأمن المعلومات:

1. نطاق التطبيق:

- الأمن الســـيبراني يركز على حماية النظم الإلكترونية والشـــبكات والأنظمة الرقمية ومعالجة التهديدات الإلكترونية مثل الهجمات السيبرانية والبرامج الضارة.
- أمن المعلومات يتعامل مع حماية المعلومات بصـــفة عامة ســـواء كانت في شكل ورقي أو رقمي، ويشمل أيضًا جوانب فيزيائية مثل الوصول إلى المباني والأمن البيئي.

2. التركيز:

- الأمن الســـيبراني يركز بشـــكل أســـاســـي على الحماية من الهجمات والاختراقات الإلكترونية والتحقق من هويات المستخدمين والأجهزة.

- أمن المعلومات يشـمل جوانب أوسـع من السـياسـات والإجراءات والتقنيات لضـمان سـلامة المعلومات والتعامل مع مختلف التهديدات سواء الإلكترونية أو غيرها.

3. المدى الزمني:

- الأمن السيبراني يتعامل بشكل أكثر فورية مع التهديدات الحالية ويشمل استجابة سريعة للاختراقات والاستجابة للأحداث السيبرانية الفورية.
- أمن المعلومات يشـمل اسـتراتيجيات طويلة الأمد لحماية المعلومات والبنية التحتية التكنولوجية ويشـمل أيضًـا تطوير سـياسـات وإجراءات وتدريب الموظفين.

باختصـار، الأمن السـيبراني هو جزء مهم من مجال أمن المعلومات ويتعامل بشـكل خاص مع التهديدات والهجمات الإلكترونية، بينما يغطي أمن المعلومات مجموعة أوسع من الجوانب التي تتعلق بحماية وسلامة المعلومات بمفهومها الشامل.

الأمن السيبراني

هو مجموعة من الإجراءات والتدابير التي تهدف إلى حماية الأجهزة والشـبكات الإلكترونية من الهجمات والتهديدات غير المصـرح بها. يشـمل الأمن السـيبراني الجهود المبذولة لمنع الوصول غير المصرح به إلى البيانات والمعلومات الحساسة، والحفاظ على سلامة الأنظمة الرقمية والحماية من التخريب والسرقة الإلكترونية.

هذا المجال يتطلب توظيف خبراء ذوي خبرة عالية في مجال الأمن السـيبراني للقيام بمراقبة وحماية الأنظمة والبنية التحتية الإلكترونية من الهجمات الإلكترونية. ويشمل الأمن السـيبراني حماية الأجهزة الحوسـبية، والخوادم، ومخزن البيانات السـحابي، بحيث يهدف إلى منع والتصـدي لأي محاولة للاختراق أو الاختراق غير المصـرح به.

تنصـــب اهتمامات الأمن الســـيبراني حول الكشـــف عن التهديدات والاختراقات الإلكترونية بشـكل فوري، واتخاذ التدابير اللازمة لمعالجتها والرد عليها. يهدف إلى الحفاظ على تواجد آمن على الإنترنت للمؤسسات والأفراد على حد سواء.

تعد المؤسسـات والحكومات والمنظمات تحقيق الأمن السـيبراني من أهم الأولويات، حيث يمكن أن تتسـبب الهجمات السـيبرانية في خسـائر مالية كبيرة، وتهديد الأمن الوطني، والتسبب في تسريب معلومات حساسة.

بشـكل عام، الأمن السـيبراني يركز على الدفاع عن الأنظمة والبيانات الرقمية من الهجمات والتهديدات الإلكترونية، ويشمل تطوير استراتيجيات الأمان وتنفيذ التدابير الوقائية والرد السريع على الحوادث السيبرانية.

سياسة أمن المعلومات

هي مجموعة من الإجراءات والتوجيهات التي تُنفذ في المؤسسات والمنظمات بهدف حماية المعلومات والبيانات الحســـاســـة والمهمة من التهديدات الأمنية وضـــمان ســلامتها. تركز ســياســة حماية المعلومات على تحديد القواعد والمعايير التي يجب اتباعها لضمان أمان المعلومات ومنع الوصول غير المصرح به إليها. **وتتضمن هذه السياسة عادة العناصر التالية:**

1. تحديد الأهداف: تبيان الأسباب والأهداف التي تدفع المؤسسة لتطبيق سياسة حماية المعلومات، مثل حماية المعلومات التجارية الحساسة أو تحقيق الامتثال للتشريعات واللوائح الصناعية.
2. نطاق التنفيذ: تحديد نطاق تطبيق ســـياســـة حماية المعلومات، بما في ذلك الأصول والبيانات والأنظمة التي يجب حمايتها.

3. المسؤوليات والأذونات: توضيح من هم المسؤولون عن تنفيذ وإدارة سياسة حماية المعلومات، وتحديد من يمتلك الأذونات والصلاحيات للوصول إلى المعلومات والبيانات الحساسة.
4. قواعد الاستخدام: تحديد قواعد وإرشادات استخدام المعلومات والأنظمة بشكل صحيح وآمن، بما في ذلك سياسات كلمات المرور والوصول البدني والتحكم في البيانات.
5. التدريب والتوعية: توفير التدريب للموظفين حول سياسة حماية المعلومات وضرورة الامتثال لها، بالإضافة إلى تعزيز التوعية بمخاطر الأمان السيبراني.
6. إجراءات التنفيذ: توضيح الإجراءات والتدابير الفعلية التي يجب اتخاذها لحماية المعلومات، مثل التشفير والمراقبة والكشف عن الاختراق.
7. مراقبة وتقييم: إنشاء آليات لمراقبة تنفيذ سياسة حماية المعلومات وتقييم فعاليتها، والقيام بتحسينها بناءً على الاحتياجات والتهديدات الجديدة.
8. تقرير واستجابة: تحديد كيفية التعامل مع انتهاكات الأمان والتقارير الأمنية والاستجابة السريعة للتهديدات والهجمات السيبرانية.

سياسة حماية المعلومات تعد أداة أساسية للمؤسسات في الحفاظ على أمان معلوماتها والامتثال للمعايير الأمنية والقوانين ذات الصلة.

كيف تحمي بياناتك من الاختراق؟

تتوفر عدد من الآليات التي تضـــمن تطبيق مفهوم حماية المعلومات بالشـــكل الأمثل ومنها:

تثبيت برامج مضادات الفيروسات

حيث تعمل هذه البرامج على فحص المعلومات بشـكل دوري وحمايتها من التعرض للفيروسات التي تحتوي على برمجيات تخريبية أو تجسسية.

كشف نقاط الضعف

من أهم عناصـر أمن المعلومات هي كشـف نقاط الضـعف في الأنظمة والتي تجعلها عرضةً للهجمات ومحاولات الاختراق، يتم ذلك عبر الاستعانة بالخبراء والمختصين الذين تتمثل مهمتهم في محاكاة عمليات الاختراق للكشف عن نقاط الضعف والتي قد تمثل خطرًا على سلامة المعلومات وسريتها.

اعتماد سياسة النسخ الاحتياطي

يتيح النســـخ الاحتياطي للمعلومات تأمينها من عمليات التخريب والتلف المحتملة جراء التعرض للهجمات ومحاولات الاختراق، حيث تســـعى بعض أنظمة الحماية إلى إتلاف المعلومات وحذفها بشـكل كامل عند تعرضـها لمحاولات الاختراق، تعد هذه الوسـيلة الملاذ الأخير الذي يهدف إلى منع تسـريب المعلومات والوصـول إليها من قبل جهات غير مصرح لها.

تشفير المعلومات

يفيد تشفير المعلومات في إضـافة قيم إضـافية إلى عملية حماية المعلومات، بالإضـافة إلى إتاحة المجال لتبادل المعلومات وإرسـالها دون الخوف من تسـريبها أو تعرضـها للاختراق .إذ تضـمن عملية التشفير عدم استفادة الجهة المخترِقة للمعلومات منها في حال استطاعت الوصول إليها.

تحديد الجهات المخولة بالوصول للمعلومات

يؤمن تحديد الجهات المخولة في اســـتخدام وتعديل المعلومات في الكشـــف عن محاولات الوصول بشكل غير قانوني إليها .

في الختام، يعد أمن المعلومات من أساسيات تأمين وحماية المعلومات، حيث يصنف على أنه من أهم الأمور التي ينبغي على الشـركات والمؤسـسـات والأفراد على حد سواء اتباعها والاهتمام بها في حال أرادوا حماية معلوماتهم من الهجمات السيبرانية والبرامج الضارة التي تهدف إلى تخريب أو سرقة المعلومات.

بـدر الحيمودي. (2023). الأمن الســـيبراني وحمـايـة الأنظمـة المعلومـاتيـة. North African Journal of Scientific Publishing (NAJSP), 174-189.

تدريبات

أسئلة اختيار من متعدد:

1. ما هي أحد أهم أهداف الأمان السيبراني؟
   - أ) الإبطاء التقني
   - ب) المحافظة على السرية والسلامة والتوافر
   - ج) زيادة الاستهلاك الإلكتروني
2. ما الذي يشمله مفهوم السرية في الأمان السيبراني؟
   - أ) الحفاظ على تكنولوجيا حديثة
   - ب) الحفاظ على سرية المعلومات والبيانات
   - ج) توفير خدمات مستدامة
3. ما الذي يعنيه التوافر في سياق الأمان السيبراني؟
   - أ) أن تكون المعلومات متاحة للجميع على الإنترنت
   - ب) أن تكون الخدمات والمعلومات متاحة وقابلة للوصـــول في الوقت الضروري
   - ج) أن تكون البيانات غير قابلة للوصول
4. ما هو الهدف الرئيسي للمحافظة على السلامة في الأمان السيبراني؟
   - أ) الحفاظ على البيانات في مكان آمن
   - ب) تجنب الأخطاء البشرية
   - ج) الحفاظ على سلامة الأنظمة والخدمات
5. ما هي التقنيات التي تستخدم لتحقيق التوافر في الأمان السيبراني؟
   - أ) التشفير

- ب) الاحتياطات والاستعادة من الكوارث
- ج) الحماية من الفيروسات

6. ما هو الاحتياط والاســـتعادة من الكوارث (Disaster Recovery) في الأمان السيبراني؟
   - أ) استراتيجية للحفاظ على البيانات دائمًا في الوضع النشط
   - ب) خطة لاستعادة الأنظمة والبيانات بعد وقوع حالة طارئة
   - ج) توفير إمكانية الوصول إلى المعلومات لجميع المستخدمين
7. ما هو التشفير في سياق الأمان السيبراني؟
   - أ) عملية حماية المعلومات من الوصــول غير المصــرح به عن طريق تحويلها إلى نص غير مفهوم
   - ب) عملية تسجيل الدخول إلى الأنظمة
   - ج) تصميم الشبكات الآمنة
8. ما هو الجانب الأساسي للسلامة في الأمان السيبراني؟
   - أ) الحفاظ على سلامة الأشخاص
   - ب) الحفاظ على سلامة البيئة
   - ج) الحفاظ على سلامة الأنظمة والبيانات
9. ما هي السياسات والإجراءات التي تضمن المحافظة على السرية والسلامة والتوافر؟
   - أ) مسح كل البيانات
   - ب) تدقيق السجلات وتحليلها
   - ج) تقسيم البيانات إلى عدة نسخ

10. ما هي الطريقة الأساسية لحماية البيانات والمعلومات من الوصول غير المصرح به؟

- أ) تخزينها في أماكن ظاهرة
- ب) تنفيذ السياسات والضوابط والتحقق من الهوية
- ج) نشرها على الإنترنت بشكل عام

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: السرية في الأمان السيبراني تعني الحفاظ على التكنولوجيا حديثة.
2. صحيح أو خطأ: التشفير هو عملية تحويل المعلومات إلى نص غير مفهوم للحفاظ على السرية.
3. صحيح أو خطأ: الاحتياط والاستعادة من الكوارث هما استراتيجيتان تساهمان في المحافظة على التوافر.
4. صحيح أو خطأ: الجانب الأساسي للسلامة في الأمان السيبراني هو الحفاظ على سلامة الأن

الوحدة التدريبية الرابعة

ضبط الوصول والتوثيق والتصريح وعدم الإنكار

الوحدة الرابعة : ضبط الوصول والتوثيق والتصريح وعدم الإنكار

الجدارة:

يتمكن المتدرب من ضبط الوصول والتوثيق والتصريح وعدم الإنكار.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- ضبط الوصول والتوثيق.
- التصريح وعدم الانكار.

الوقت المتوقع للتدريب:

6 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب كيفية ضبط الوصول والتوثيق والتصريح وعدم الإنكار.

ضبط الوصول والتوثيق والتصريح وعدم الإنكار

ضبط الوصول

ضبط الوصول للأمن السيبراني هو عملية تحديد وإدارة من يمكنه الوصول إلى موارد ومعلومات النظام السيبراني داخل منظمة أو شبكة. تهدف هذه العملية إلى ضمان أمان المعلومات والحواسيب والشبكات من التهديدات السيبرانية عن طريق تقييد الوصول إلى المعلومات بحسب الاحتياجات والصلاحيات.

إليك بعض الخطوات الأساسية لضبط الوصول لتعزيز الأمن السيبراني:

1. تحديد الصلاحيات: يجب تحديد ماهية الصلاحيات والوصول التي تحتاجها الأشخاص لأداء واجباتهم. هذا يشمل تحديد مين يمكنه الوصول إلى أي بيانات أو أنظمة معينة وبمستويات صلاحيات محددة.
2. تطبيق مبدأ أقل الامتيازات: ينص هذا المبدأ على منح كل مستخدم أو جهاز فقط الصلاحيات اللازمة لأداء مهامه. فإذا لم يكن لديهم حاجة للوصول إلى معلومات معينة، يجب منعهم من الوصول إليها.
3. إدارة هويات المستخدمين: يتعين إنشاء وإدارة هويات المستخدمين بعناية، بما في ذلك تعيين كلمات مرور قوية وتنفيذ إجراءات اتصال آمنة مثل التحقق من الهوية متعدد العوامل.

جمال الدين, ه. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية, 24(1), 189-230.

4. تطبيق نماذج التفويض: يمكن استخدام نماذج التفويض للتحقق من الصلاحيات وتنظيم الوصول. يمكنك تحديد من يمكنه الموافقة على طلبات الوصول ومتى يمكن تنفيذها.
5. مراقبة الوصـول: يجب تسـجيل ومراقبة الأنشـطة المرتبطة بالوصـول إلى النظام السيبراني، مما يتيح تتبع الأنشطة غير المصرح بها وكشف أي أنشطة مشبوهة.
6. تحديث دوريًا: يجب تحديث سياسات وإجراءات ضبط الوصول بشكل دوري للتأكد من مواكبتها للتطورات التكنولوجية والأمان.
7. التدريب والتوعية: يجب توعية الموظفين بأهمية الأمان السـيبراني وتدريبهم على كيفية التعامل مع المعلومات والبيانات بشكل آمن.

ضبط الوصول للأمن السيبراني يعتبر جزءًا مهمًا من استراتيجية الأمان العامة لأي منظمة أو شبكة، ويساهم بشكل كبير في تقليل مخاطر الهجمات السيبرانية وحماية المعلومات الحساسة.

التوثيق

التوثيق هو جزء أساسـي من اسـتراتيجية الأمن السـيبراني ويسـهم بشـكل كبير في تعزيز الأمان وحماية المعلومات والبيانات من التهديدات السـيبرانية. التوثيق يعني التحقق من هوية الأفراد أو الأجهزة التي تحاول الوصـول إلى النظام أو الموارد السيبرانية، وتقديم الصلاحيات اللازمة بناءً على هذه الهويات.

إليك كيف يتم توثيق الأمان السيبراني:

1. **توثيق المسـتخدمين :**يتضـمن التوثيق التحقق من هوية المسـتخدمين الذين يحاولون الوصول إلى النظام. يتم ذلك عادة عبر استخدام اسم المستخدم وكلمة المرور، ويمكن أيضًـا اسـتخدام تقنيات أخرى مثل البصـمة الرقمية أو الهوية المتعددة العوامل (MFA) مثل رمز تحقق أو جهاز مفتاحي.

2. **توثيق الأجهزة :**يتعين أيضًا التحقق من هوية الأجهزة التي تتصل بالشبكة أو تحاول الوصول إلى التطبيقات والمعلومات. هذا يساعد في منع الأجهزة غير المصرح بها من الوصول.
3. **توثيق الجلسات :**يتم تسجيل وتوثيق الجلسات النشطة للمستخدمين للتحقق من أنهم ما زالوا مصرحين بالوصول ولم يتم تجاوز صلاحياتهم.
4. **إعداد السجلات :(Logging)** يجب تسجيل جميع الأنشطة والمحاولات غير المصرح بها في النظام. هذه السجلات تعمل كأدلة تفصيلية تساعد في تتبع الأحداث والاكتشاف المبكر لأنشطة مشبوهة.
5. **استخدام التوثيق متعدد العوامل :(MFA)** يُفضل استخدام توثيق متعدد العوامل لزيادة الأمان. هذا يعني أن المستخدمين يحتاجون إلى توفير أكثر من معلومة للدخول، مثل ما يعرف وما يملك (مثل كلمة مرور ورمز تحقق على هاتف ذكي).
6. **تحديد وإدارة الصلاحيات :**يجب تحديد الصلاحيات بعناية للمستخدمين والأجهزة. يجب منح كل مستخدم أو جهاز فقط الصلاحيات اللازمة لأداء مهامهم.
7. **تحديث وتطوير النظام :**يجب تحديث وتطوير نظام التوثيق بشكل دوري لمواكبة أحدث التقنيات والتهديدات السيبرانية.
8. **التدريب والتوعية :**يجب تدريب المستخدمين على كيفية استخدام التوثيق بشكل صحيح وتوعيتهم بأهمية الأمان السيبراني والمخاطر المحتملة.

باختصار، التوثيق يعزز الأمان السيبراني من خلال التحقق من هويات المستخدمين والأجهزة وتطبيق الصلاحيات بشكل دقيق، مما يقلل من مخاطر التهديدات السيبرانية ويحمي المعلومات والبيانات.

التصريح

التصـريح (أو الصـلاحيات) هو جزء مهم من اسـتراتيجية الأمن السـيبراني، حيث يساهم في تحقيق التحكم والحماية في النظام السيبراني ومنع الوصول غير المصرح به إلى المعلومات والموارد الحسـاسـة. التصـريح يعني تحديد مدى الصـلاحية والوصول للأفراد أو الأجهزة أو التطبيقات على أساس هويتهم ودورهم.

إليك كيف يتم تطبيق التصريح في الأمن السيبراني:

1. **تحديد الصـلاحيات :**يجب تحديد الصـلاحيات بعناية لكل مسـتخدم أو جهاز أو تطبيق. يعني ذلك تحديد ما إذا كان لديهم الحق في الوصـول إلى أو تعديل معلومات معينة أو استخدام موارد معينة.
2. **الصـلاحيات الأدنى :(Principle of Least Privilege - PoLP)** يُفضـل تطبيق مبدأ الصـلاحيات الأدنى، وهذا يعني أن يتم منح المسـتخدمين فقط الصـلاحيات التي يحتاجونها لأداء مهامهم. على سـبيل المثال، موظف الإدارة ليس بحاجة إلى صلاحيات إدارة الشبكة.
3. **التحقق من الهوية :**يتعين التحقق من هوية المستخدمين والأجهزة قبل منحهم الوصول. يمكن استخدام أسماء المستخدمين وكلمات المرور وأساليب التوثيق المتعددة العوامل لضمان هويتهم.
4. **الصلاحيات المبتنية على الأدوار (Role-Based Access Control - RBAC):** يمكن تقديم الصـلاحيات بناءً على الأدوار والمسـميات الوظيفية للمستخدمين. هذا يجعل إدارة الصلاحيات أكثر فعالية ومرونة.
5. **التحكم في الصـلاحيات :**يجب تطبيق التحكم في الصـلاحيات وتحديد القواعد والقيود التي تحكم اسـتخدام الصـلاحيات. على سـبيل المثال، يمكن منع المستخدمين من حذف الملفات أو تعديلها إذا لم تكن لديهم هذه الصلاحية.

6. **تتبع ورصد الصلاحيات :**يجب تسجيل ومراقبة جميع الأنشطة المتعلقة بمنح واستخدام الصلاحيات. يمكن استخدام السجلات لمعرفة من حاول الوصول غير المصرح به أو استخدام الصلاحيات بشكل غير قانوني.
7. **التدريب والتوعية :**يجب توعية المستخدمين بأهمية الصلاحيات والأمان السيبراني والمخاطر المحتملة. يجب أيضًا تدريبهم على كيفية استخدام الصلاحيات بشكل آمن.
8. **تحديث الصلاحيات بشكل دوري :**يجب مراجعة وتحديث الصلاحيات بشكل دوري لضمان أنها ما زالت ملائمة لاحتياجات المستخدمين وأمان النظام.

باختصار، التصريح هو عنصر أساسي في استراتيجية الأمن السيبراني يسهم في الحفاظ على سلامة المعلومات ومنع الوصول غير المصرح به. تطبيق الصلاحيات بشكل صحيح يقلل من مخاطر التهديدات السيبرانية ويحمي النظام السيبراني والبيانات.

عدم الانكار

مبدأ عدم الانكار (Non-Repudiation) هو مفهوم مهم في مجال الأمن السيبراني، وهو يشير إلى القدرة على تأكيد أو إثبات أن مستخدم معين قام بعمل معين أو قام بإرسال معلومات معينة، وذلك بحيث لا يمكن للمستخدم نفي هذا العمل في وقت لاحق.

هذا المفهوم يكون ضروريًا في العديد من السيناريوهات السيبرانية حيث يمكن أن يساهم في تحقيق الأمان والثقة في التفاعلات عبر الإنترنت والتوقيع الإلكتروني. إليك كيف يمكن تحقيق مبدأ عدم الانكار في مجال الأمن السيبراني:

1. **التوقيع الرقمي :**يتمثل التوقيع الرقمي في استخدام تقنيات التشفير لإنشاء توقيع إلكتروني فريد لمرسل معين على البيانات أو الرسائل. هذا التوقيع يمكن التحقق منه بواسطة الأطراف الأخرى للتأكد من هوية المرسل وأن البيانات لم تتم تلاعبها.

2. **سجلات الأنشطة (Audit Logs):** يتم تسجيل جميع الأنشطة الهامة في النظام بما في ذلك الوصول إلى المعلومات والتعامل معها. يمكن استخدام هذه السجلات لتتبع وتحقيق الأنشطة ومعاقبة المختلفين إذا كان هناك خلاف.
3. **استخدام شهادات الهوية الرقمية :**تعتبر شهادات الهوية الرقمية وسيلة للتحقق من هوية المستخدمين عبر الإنترنت. توفر هذه الشهادات مستوى عاليًا من الأمان والتوثيق.
4. **الوثائق القانونية والاتفاقيات :**يمكن استخدام وثائق قانونية واتفاقيات لتحقيق عدم الانكار. على سبيل المثال، يمكن تضمين بنود في عقد تفاهم تنص على التزام الأطراف بالمعاملات والأنشطة المتعلقة بالأمان.
5. **توثيق الأحداث والوقائع :**يتمثل ذلك في تسجيل وتوثيق جميع الأحداث والوقائع المهمة التي تحدث في النظام. يتيح ذلك للأطراف تتبع سجل الأحداث للتحقق من صحة وقائع معينة.
6. **الشهادات الرقمية للبريد الإلكتروني :**يمكن استخدام شهادات البريد الإلكتروني للتحقق من هوية المرسلين وسلامة الرسائل الإلكترونية.

في الختام، مبدأ عدم الانكار يلعب دورًا مهمًا في ضمان الأمان والمصداقية في البيئة السيبرانية. إذا تم تطبيقه بشكل فعال، فإنه يمكن أن يحمي الأنظمة والبيانات من الانكار ويسهم في توثيق العمليات والمعاملات.

جمال الدين, ه. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية, 24(1), 189-230.

تدريبات

أسئلة اختيار من متعدد:

1. ما الهدف الرئيسي لضبط الوصول في الأمان السيبراني؟
   - أ) الحفاظ على سرية البيانات
   - ب) تقليل سرعة الاتصال بالإنترنت
   - ج) زيادة عدد المستخدمين
2. ما هو التوثيق في الأمان السيبراني؟
   - أ) التحقق من هوية المستخدمين ومصداقيتهم
   - ب) تشفير البيانات
   - ج) حجب الوصول إلى الشبكة
3. ما هو التصريح في سياق الأمان السيبراني؟
   - أ) الإجراء الذي يتيح للمستخدمين الوصول إلى جميع البيانات
   - ب) العملية التي يتم فيها إعطاء المستخدمين أذونات محددة للوصول إلى المعلومات
   - ج) الحفاظ على البيانات دائمًا في الوضع النشط
4. ما هو مبدأ "عدم الإنكار" في الأمان السيبراني؟
   - أ) القدرة على رفض الوصول للمستخدمين المصرح لهم
   - ب) السماح للمستخدمين بالتنكر عند الدخول إلى الشبكة
   - ج) عدم القدرة على إلغاء الوصول إلى البيانات المسجلة
5. ما هي السياسة التي تحدد الأذونات والصلاحيات للمستخدمين في النظام؟

- أ) سياسة العدم الإنكار
- ب) سياسة الحفاظ على السلامة
- ج) سياسة التوثيق المزدوج

6. ما هو الهدف الرئيسي لضبط الوصول إلى البيانات؟
   - أ) تسهيل الوصول لجميع المستخدمين
   - ب) الحفاظ على البيانات ومنع الوصول غير المصرح به
   - ج) زيادة حجم التخزين على السيرفرات
7. ما هو التوثيق المزدوج(Two-Factor Authentication) ؟
   - أ) طريقة للتحقق من هوية المستخدم باستخدام عاملين مختلفين
   - ب) توثيق البيانات باستخدام نص غير مفهوم
   - ج) تحديد الأذونات للمستخدمين
8. ما هي الفائدة الرئيسية لتطبيق التصريح في النظام؟
   - أ) زيادة سرعة الوصول إلى البيانات
   - ب) منع الوصول غير المصرح به وتقليل المخاطر الأمنية
   - ج) زيادة تشفير البيانات
9. ما هي أحد أمثلة التوثيق في الأمان السيبراني؟
   - أ) إدخال كلمة مرور فقط
   - ب) إدخال اسم المستخدم وكلمة المرور
   - ج) إدخال اسم المستخدم فقط
10. ما هي الأهمية الرئيسية لعدم الإنكار في الأمان السيبراني؟
    - أ) منع المستخدمين من الوصول إلى البيانات

- ب) تسجيل وتوثيق جميع الأنشطة للتحقق من الهوية
- ج) منع المستخدمين من إنكار مشاركتهم في النشاطات

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: ضبط الوصول يهدف إلى السماح للجميع بالوصول إلى البيانات دون قيود.
2. صحيح أو خطأ: التوثيق يتطلب إدخال اسم المستخدم وكلمة المرور فقط.
3. صحيح أو خطأ: التصريح يساهم في منع الوصول غير المصرح به للبيانات.
4. صحيح أو خطأ: عدم الإنكار يعني أن المستخدمين لديهم القدرة على نفي مشاركتهم في الأنشطة التي قاموا بها.
5. صحيح أو خطأ: التوثيق المزدوج يتطلب استخدام عاملين مختلفين للتحقق من هوية المستخدم

الوحدة التدريبية الخامسة

التشفير وإستخداماته

الوحدة الخامسة : التشفير وإستخداماته

الجدارة:

يتمكن المتدرب من التشفير وإستخداماته.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- التشفير
- استخدامات التشفير.

الوقت المتوقع للتدريب:

6 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب كيفية التشفير وإستخداماته.

التشفير وإستخداماته

التشفير في مجال الأمن الإلكتروني يشير إلى عملية تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مشفر، مما يجعلها غير قابلة للفهم والاستخدام من قبل أي شخص غير مخول. يُعتبر التشفير وسيلة أساسية لحماية البيانات والمعلومات على الإنترنت من الاختراق والسرقة.

عملية التشـــفير تعتمد على اســـتخدام ما يُعرف بالمفاتيح، وهي مجموعة من القيم الرياضـــية التي تســـتخدم لتحويل البيانات بحيث يمكن فقط لأولئك الذين يملكون المفاتيح الصـحيحة فك تشـفيرها. وهذا يجعل التشـفير وسـيلة فعالة لحماية البيانات والمعلومات من المتسللين.

عندما تُشفر البيانات، تصبح غير قابلة للقراءة بشكل مباشر. وعند استلامها من قِبل المستلم الصحيح، يتم استخدام المفتاح المناسب لفك تشفيرها واستعادتها إلى حالتها الأصلية كنص قابل للقراءة.

حكمت اسـماعيل, & ياسـين. (2023). اداء طرق التشـفير الكتلي وتحليل المخاطر. مجلة الرافدين لعلوم الحاسوب والرياضيات, 17(1), 23-33.

مدى قوة التشفير يتوقف على تعقيد المفتاح وأسلوب التشفير المستخدم. كلما كان المفتاح أكثر تعقيدًا، زادت صعوبة فك تشفير البيانات بواسطة أي شخص غير مخول. يُستخدم التشفير أيضًا لحماية كلمات المرور، حيث يتم تشفيرها بحيث لا يمكن فهمها بسهولة من قِبل المتسللين.

بشكل عام، التشفير هو أداة حاسمة للأمان السيبراني، ويتم استخدامه في العديد من السيناريوهات لحماية البيانات والمعلومات وضمان عدم وصولها إلى الأطراف غير المصرح لها.

توجد اثنتان من التقنيات الرئيسية للتشفير هي الأكثر انتشاراً: التشفير المتماثل والتشفير غير المتماثل. يتعلق الفرق بينهما بكيفية استخدام المفاتيح في عملية التشفير وفك التشفير:

1. **التشفير المتماثل (Symmetric Encryption):** يُعرف أيضاً بالتشفير بنفس المفتاح. في هذا النوع من التشفير، يتم استخدام نفس المفتاح لكل من عملية التشفير وفك التشفير. يعني ذلك أنه يجب على المرسل والمستلم أن يمتلكوا نفس المفتاح السري لضمان التواصل الآمن. وهذا يجعل التشفير المتماثل أسرع وأقل تعقيداً من البدائل غير المتماثلة. ومع ذلك، يتطلب توزيع المفتاح بشكل آمن إلى المستلمين وحفظه بعيداً عن المتسللين.
2. **التشفير غير المتماثل (Asymmetric Encryption):** يُعرف أيضاً بالتشفير بمفتاحين. في هذا النوع من التشفير، يتم استخدام مفتاحين مختلفين، مفتاح عام ومفتاح خاص. يتم مشاركة المفتاح العام بشكل عام ويمكن استخدامه لتشفير البيانات، بينما يُحتفظ المستخدم بالمفتاح الخاص بسرية. يمكن فقط استخدام المفتاح الخاص المتوافق مع المفتاح العام لفك تشفير البيانات. هذا يزيد من أمان العمليات ولا يتطلب توزيع المفتاح الخاص بنفس الطريقة التي يتطلبها التشفير المتماثل.

بشـــكل عام، كل من التشـــفير المتماثل والتشـــفير غير المتماثل لهما اســـتخداماتهما المختلفة ويتم اختيار النوع المناسب حسب حاجة السيناريو ومتطلبات الأمان.

أمثلة على خوارزميات التشفير:

يُســـتخدم خوارزميات التشـــفير لتحويل البيانات إلى نص مشـــفر، حيث تعمل هذه الخوارزميات على تغيير البيانات بطريقة تجعلها غير قابلة للقراءة بســـهولة، ويمكن فقط فك تشفيرها باستخدام مفتاح معين. وهنا بعض الأمثلة على خوارزميات التشفير الشهيرة:

1. **AES معيار التشـفير المتقدم :(**يُشـار إليه أيضًـا باسـمRijndael ، وهو خوارزمية تشـفير متماثل اعتمدت على نطاق واسـع لحماية البيانات. تعتبر AESواحدة من أكثر الخوارزميات أمانًا وسـرعة. يتم اسـتخدامها في تطبيقات الرسـائل المشـفرة مثل Signal وبرامج الضـغط والأرشـفة مثل WinZip.
2. **RSA خوارزمية :(RSA)** تعتبر RSA خوارزمية غير متماثلة وتعتمد على زوج من المفاتيح: مفتاح عام ومفتاح خاص. يُستخدم المفتاح العام لتشفير البيانات، بينما يُحتفظ بالمفتاح الخاص سرًا ويُستخدم لفك التشفير. تُستخدم RSAفي العديد من تطبيقات الأمان والمصادقة عبر الإنترنت.
3. **Twofish:** تُستخدم خوارزمية Twofish في تطبيقات البرامج والأجهزة، وهي معروفة بسرعتها وأمانها. يمكن العثور على Twofish في برامج مثل PhotoEncryptوGPG، بالإضـــافة إلى البرنامج مفتوح المصـــدر TrueCrypt.
4. **RC4 خوارزمية :(RC4)** تم اسـتخدامها في WEP وWPA، وهما بروتوكولات تشفير شائعة في أجهزة التوجيه اللاسلكية.
5. **3DES المعيار الثلاثي لتشفير البيانات :(**تمثل تطويرًا لخوارزميةDES ، وهي تســـتخدم في بعض الأمور الأمنية رغم تراجع اســـتخدامها مع مرور الوقت.

تعتبر هذه الخوارزميات أمثلة على تقنيات التشفير الشهيرة والمستخدمة على نطاق واسع لحماية البيانات وتأمين الاتصالات عبر الإنترنت والشبكات.

التشفير أثناء النقل مقابل التشفير في حالة السكون: الاختلافات والأهمية

غالبًا ما يتم تقسيم حلول التشفير إلى تشفير البيانات أثناء النقل وتشفير البيانات في حالة السكون، وذلك استنادًا إلى حالة البيانات ومدى تنقلها.

تشفير البيانات أثناء النقل :يشير هذا إلى عملية تشفير البيانات أثناء انتقالها من جهاز إلى آخر، كما يحدث عندما يتم نقل البيانات عبر الإنترنت أو عبر الشبكات الخاصة. وخلال هذه العملية، تكون البيانات في حالة تعرض مباشر لخطر الاعتراض والاختراق. يهدف التشفير أثناء النقل إلى حماية البيانات من الوصول غير المصرح به عندما تتنقل من مكان إلى آخر.

تشفير البيانات في حالة السكون :تشير هذه الحالة إلى حالة البيانات عندما تكون محفوظة دون تحرك أو نقل نشط. وعادةً ما تكون البيانات في حالة السكون على وسائط تخزين مثل الأقراص الصلبة أو الأجهزة السحابية دون استخدامها بنشاط. وعلى الرغم من أن هذه الحالة تزيد من أمان البيانات بسبب الوصول المقيد إليها، إلا أنها ليست محصنة تمامًا.

من الجدير بالذكر أن البيانات في حالة السكون قد تكون ذات قيمة كبيرة للمتسللين، لأنها عادةً ما تحتوي على معلومات حساسة وذات أهمية كبيرة.

أهمية التشفير في حالة السكون :يعمل التشفير في حالة السكون على تقليل فرص الوصول غير المصرح به إلى البيانات في حالة فقدها أو سرقتها، ويمنع الوصول غير المصرح به إليها عن طريق ميزات الأمان المضمنة في الأجهزة. ومن خلال تأخير الوصول إلى البيانات، يمنح مالك البيانات وقتًا إضافيًا لاكتشاف أي اختراقات أو خروقات أمان.

كمثال على تقنية تشفير البيانات في حالة السكون، يُذكر نظام تشفير البيانات الشفاف(TDE) ، الذي يتم استخدامه من قبل الشركات مثل Microsoft و Oracleو .IBMيعمل TDE على تشفير ملفات قواعد البيانات على مستوى

القرص الصلب ووسائط النسخ الاحتياطي، مما يزيد من أمان البيانات عندما تكون في حالة سكون.

ملاحظة :يجب ملاحظة أن التشفير في حالة السكون لا يحمي البيانات أثناء عملية النقل.

مفهوم تشفير البيانات الثنائي بين الأطراف: التفسير والأهمية

عبارة "تشفير البيانات الثنائي بين الأطراف" هي مصطلح شائع تستخدم للإشارة إلى أنظمة التشفير التي تتيح فقط للأطراف المشتركة في التواصل (واللذين يمتلكون مفاتيح خاصة) فك تشفير المعلومات المبادرة بينهم. هذا يعني أنه حتى مقدم الخدمة أو المزود الذي يتوسط في التواصل ليس لديه وسيلة لفك تشفير المحادثة. تشمل هذه السيناريوهات على سبيل المثال التشفير الكامل بين طرفين.

يمكن إعادة تعيين تشفير البيانات الثنائي بين الأطراف بمعرفة كلمة المرور الخاصة بالمستخدم، مثلما يحدث في بعض الأجهزة مثل iPhone عند نسيان كلمة المرور. وعند إعادة تعيينها، يمكن فقدان الوصول إلى البيانات المشفرة التي تم نسيان كلمة المرور لها، مما يجعلها غير قابلة للاسترداد. ولكن بإمكان المستخدم إعادة إنشاء نسخ احتياطية للبيانات وإعادة ضبط كلمة المرور لحمايتها مستقبلاً.

فوائد تشفير البيانات:

1. **الحفاظ على تكامل البيانات :**يمكن أن يحمي التشفير البيانات من التلاعب أو التغيير غير المصرح به، حيث يصعب على المتسللين تحريف البيانات المشفرة.
2. **الامتثال للتنظيمات :**يساعد التشفير في الامتثال لقوانين ولوائح الأمان وحماية البيانات التي تفرضها الهيئات التنظيمية، وخاصة في الصناعات الحساسة مثل الخدمات المالية والرعاية الصحية.
3. **حماية البيانات أثناء النقل :**يضمن التشفير سلامة البيانات أثناء نقلها بين الأجهزة وعبر الشبكات، حمايةً من الاعتراض والاختراقات أثناء النقل.

4. **حماية البيانات في التخزين السحابي :**يساعد التشفير في الحفاظ على خصوصية البيانات المخزنة في خدمات التخزين السحابي.
5. **تأمين المكاتب عن بُعد :**يحمي التشفير البيانات في بيئات العمل عن بُعد، مما يقلل من مخاطر الوصول غير المصرح به.
6. **حماية الملكية الفكرية :**يُستخدم التشفير لحماية المحتوى المحمي بحقوق النشر مثل الموسيقى والبرامج من الاستخدام غير المصرح به والاستنساخ غير القانوني.

باختصار، يعمل التشفير على زيادة أمان وسلامة البيانات في مختلف السيناريوهات، ويسهم في الحفاظ على خصوصيتها وسلامتها.

الاستخدامات الشائعة والمهمة للتشفير في حياتنا اليومية

نتعامل مع التشفير في مختلف جوانب حياتنا اليومية، حيث يلعب دورًا حاسمًا في حماية البيانات والمعلومات. إليك بعض الاستخدامات الشائعة والمهمة للتشفير:

1. **تأمين المعاملات المالية :**عند استخدام أجهزة الصراف الآلي أو القيام بمعاملات مالية عبر الإنترنت باستخدام هواتفنا الذكية، يتم استخدام التشفير لحماية البيانات المرسلة والمستقبلة خلال هذه المعاملات.
2. **تأمين الأجهزة الشخصية :**يتم استخدام التشفير لحماية بياناتنا على أجهزة الكمبيوتر المحمولة والهواتف الذكية من الوصول غير المصرح به.
3. **حماية الاتصالات عبر الإنترنت :**معظم مواقع الويب الآمنة تستخدم بروتوكول "HTTPS" الذي يشمل طبقة إضافية من التشفير (SSL/TLS) لحماية بيانات المستخدمين أثناء إرسالها واستقبالها عبر الإنترنت.
4. **تأمين التطبيقات والخدمات :**تستخدم تطبيقات الرسائل مثل WhatsApp التشفير لحماية رسائل المستخدمين، ويمكن أيضًا تشفير بريد الكتروني باستخدام تقنيات مثل.OpenPGP

5. **استخدام الشبكات الافتراضية الخاصة (VPN):** يتم تشفير حركة البيانات عند استخدام VPN للتصفح الآمن عبر الإنترنت وحماية الخصوصية.
6. **حماية البيانات في التخزين السحابي:** يُفضل تشفير الملفات والبيانات المخزنة في خدمات التخزين السحابي للحفاظ على خصوصيتها.
7. **التوقيع الرقمي:** يستخدم التشفير في إثبات مصداقية المعلومات والوثائق من خلال التوقيعات الرقمية، وهو جزء من إدارة الحقوق الرقمية.
8. **محو البيانات:** يُمكن استخدام التشفير لحذف البيانات بشكل آمن ومنع استردادها، مما يساهم في حفظ الخصوصية والأمان.

التشفير يعتبر جزءًا أساسيًا من أمان البيانات والمعلومات في عصر الاتصالات الرقمية، ويساهم بشكل كبير في الحفاظ على سرية وسلامة البيانات الحساسة والشخصية.

حكمت اسماعيل, & ياسين. (2023). اداء طرق التشفير الكتلي وتحليل المخاطر. مجلة الرافدين لعلوم الحاسوب والرياضيات, 17(1), 23-33.

تدريبات

أسئلة اختيار من متعدد:

1. ما هو التشفير في سياق الأمان السيبراني؟
   - أ) عملية إخفاء المعلومات للوصول الغير مصرح به
   - ب) عملية تسجيل الأنشطة على الشبكة
   - ج) عملية تسريع الاتصال بين الأجهزة
2. ما هي وحدة القياس الشائعة لقوة التشفير؟
   - أ) البايت(Byte)
   - ب) الجيجابايت(Gigabyte)
   - ج) البت(Bit)
3. ما هو التشفير المتناسق(Symmetric Encryption) ؟
   - أ) نوع من التشفير يستخدم مفتاحًا واحدًا للتشفير وفك التشفير
   - ب) نوع من التشفير يستخدم مفتاحين مختلفين للتشفير وفك التشفير
   - ج) نوع من التشفير يعتمد على البصمات الرقمية
4. ما هو التشفير اللاسلكي(Wireless Encryption) ؟
   - أ) نوع من التشفير يتم استخدامه في شبكات الجوال
   - ب) نوع من التشـــفير يتم اســـتخدامه في شـــبكات الواي فاي لحماية الاتصالات اللاسلكية
   - ج) نوع من التشفير يتم استخدامه في الاتصالات الفضائية
5. ما هو التشفير المفتوح المصدر(Open Source Encryption) ؟
   - أ) نوع من التشفير يتم استخدامه فقط في الشركات

- ب) نوع من التشـفير يسـتند إلى تقنيات متاحة للجميع ويمكن مراجعتها وتعديلها بواسطة المطورين المستقلين
- ج) نوع من التشفير يتم استخدامه فقط في الأجهزة الحكومية

6. ما هو التشفير غير المتزامن(Asymmetric Encryption) ؟

- أ) نوع من التشفير يستخدم مفتاحًا واحدًا للتشفير وفك التشفير
- ب) نوع من التشفير يستخدم مفتاحين مختلفين للتشفير وفك التشفير
- ج) نوع من التشفير يتم استخدامه في تحقيق الوصول إلى الإنترنت

7. ما هو دور مفتاح التشفير في عملية التشفير؟

- أ) يتم استخدامه لتشفير البيانات
- ب) يتم استخدامه لفك تشفير البيانات
- ج) يتم استخدامه لتسجيل الأنشطة على الشبكة

8. ما هي واحدة من استخدامات التشفير في الحياة اليومية؟

- أ) حفظ النسخ الاحتياطية من البيانات
- ب) تسجيل المكالمات الهاتفية
- ج) تحرير الوثائق النصية

9. ما هو تشفير SSL/TLS المستخدم في الاتصالات الآمنة عبر الإنترنت؟

- أ) نوع من التشفير المتناسق
- ب) نوع من التشفير اللاسلكي
- ج) نوع من التشفير اللاسلكي

10. ما هي أحد اسـتخدامات التشفير في الرسائل الإلكترونية؟

- أ) حفظ المرفقات

- ب) حماية البيانات السرية والمحادثات من الوصول غير المصرح به
- ج) تحديد مكان المرسل

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: التشفير يهدف إلى جعل البيانات غير مفهومة للأشخاص الذين ليس لديهم مفتاح التشفير الصحيح.
2. صحيح أو خطأ: التشفير المفتوح المصدر يعني أن التقنيات المستخدمة في التشفير متاحة للعامة ويمكن مراجعتها وتعديلها بحرية.
3. صحيح أو خطأ: التشفير اللاسلكي يستخدم فقط في الاتصالات عبر الإنترنت ولا يشمل الاتصالات السلكية.
4. صحيح أو خطأ: التشفير غير المتزامن يستخدم مفتاحًا واحدًا للتشفير وفك التشفير.
5. صحيح أو خطأ: مفتاح التشفير يستخدم لتسجيل الأنشطة على الشبكة وليس لعمليات التشفير.

الوحدة التدريبية السادسة

الحوكمة وإدارة المخاطر السيبرانية

الوحدة السادسة : الحوكمة وإدارة المخاطر السيبرانية

الجدارة:

يتمكن المتدرب من الحوكمة وإدارة المخاطر السيبرانية.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- الحوكمة.
- إدارة المخاطر السيبرانية.

الوقت المتوقع للتدريب:

9 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب كيفية الحوكمة وإدارة المخاطر السيبرانية.

الحوكمة وإدارة المخاطر السيبرانية

الأمن السيبراني يمثل إطار عمل حاسم يتبعه المنشآت لضمان حماية وسلامة أنظمتها وبياناتها من التهديدات السيبرانية. يتضمن الأمن السيبراني مكونات أساسية تشمل:

1. **الحوكمة :**تتعامل الحوكمة مع إنشاء إطار عمل لتحديد السياسات والإجراءات وعمليات اتخاذ القرارات التي توجه جهود الأمن السيبراني للمنشآة. يتضمن ذلك تحديد الأدوار والمسؤوليات، وإقامة آليات الاتصال الواضحة، وضمان مشاركة القيادة التنفيذية في مبادرات الأمن السيبراني.
2. **إدارة المخاطر :**تشمل إدارة المخاطر تحديد وتقييم وتقليل المخاطر المحتملة التي تهدد أصول المنشآة وعملياتها الرقمية. يشمل ذلك الخطوات التالية:

- تحديد المخاطر: تحديد الأصول وتحليل النقاط الضعيفة وتحديد التهديدات المحتملة.
- تقييم المخاطر: تقدير احتمالية حدوث المخاطر وتقدير تأثيرها.
- تخفيف المخاطر: تنفيذ الضوابط والإجراءات لتقليل المخاطر إلى مستوى مقبول.

زكي حسين متولي, م., مصطفى, عبد العال سالم غريب, & حسين. (2022). قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة الخارجية: دراسة تطبيقية. المجلة العلمية للدراسات المحاسبية, 4(4), 245-328.

- مراقبة المخاطر: مراقبة ومراجعة المخاطر بشكل مستمر مع تغير الظروف والتهديدات.

3. **الالتزام :**يتعلق الالتزام بالامتثال للوائح والتشريعات والمتطلبات القانونية ومعايير الأمن السيبراني المتعلقة بنشاط المنشآة. يهدف الامتثال إلى ضمان أن تتفق التدابير الأمنية للمنشآة مع اللوائح المعمول بها، مما يحول دون تعرض المنشآة للعقوبات القانونية ويحفظ سمعتها.

الأمن السيبراني يعد أساسيًا في العالم الرقمي الحديث، حيث يسهم في حماية المنشآت وبياناتها ويساعدها على مواجهة والتصدي للتهديدات السيبرانية المتزايدة.

مفهوم) GRC الحوكمة وإدارة المخاطر والامتثال(

GRCهو اختصار يشير إلى مفهوم الحوكمة وإدارة المخاطر والامتثال. عادةً ما تكون الشركات على دراية بهذه المصطلحات، ولكنها قد مارست في الماضي على نحو منفصل. يقوم نموذج GRC بدمج هذه العناصر في نموذج واحد متكامل ومنسق. يهدف ذلك إلى مساعدة الشركات على تحسين الكفاءة، وتقليل المخاطر المتعلقة بعدم الامتثال، وزيادة مشاركة المعلومات بشكل أكثر فاعلية.

الحوكمة الحوكمة تمثل مجموعة السياسات والقواعد والهياكل التي تستخدمها المؤسسة لتحقيق أهدافها وضمان التفوق في أعمالها. تحدد الحوكمة المسؤوليات والأدوار المختلفة للأطراف ذات الصلة، مثل مجلس الإدارة والإدارة التنفيذية. على سبيل المثال، تشمل الحوكمة إنشاء سياسات تتعلق بالمسائل الأخلاقية وتحديد السياسات المالية.

إدارة المخاطر إدارة المخاطر تشمل تحديد وتقييم ومعالجة المخاطر التي يمكن أن تؤثر على أنشطة المؤسسة وأهدافها. تشمل هذه العملية تحليل الأصول وتحديد التهديدات والثغرات وتقييم تأثيرها المحتمل واحتمالية وقوعها. بناءً على هذه المعلومات، تتخذ إجراءات للحد من المخاطر والتأكد من تحقيق الامتثال.

الامتثال الامتثال يتعلق بالالتزام باللوائح والمعايير والتشريعات ذات الصلة لقطاع المؤسسة. يشمل ذلك تصميم سياسات وإجراءات لضمان الامتثال بشكل مستدام

وتقديم التقارير اللازمة للجهات المعنية. على سبيل المثال، قد تضمن سياسات الامتثال احترام حقوق الخصوصية للعملاء والامتثال للتشريعات المالية.

باختصار، GRCهو نهج تكاملي يساعد المؤسسات على تحقيق الكفاءة والامتثال وإدارة المخاطر بشكل فعال من خلال دمج الحوكمة وإدارة المخاطر والامتثال في استراتيجيتها وعملياتها اليومية.

وتشمل الحوكمة الرشيدة العناصر التالية:

- الأخلاق والمساءلة
- شفافية تبادل المعلومات
- سياسات حل النزاعات
- إدارة الموارد

تنفيذ الحوكمة وإدارة المخاطر والامتثال في مجال الأمن السيبراني

لتحقيق برنامج فعال للحوكمة وإدارة المخاطر والامتثال في مجال الأمن السيبراني، يجب على المنشآت اتباع الخطوات التالية:

1. **التقييم :**يتعين على المنشآت فهم مشهد الأمن السيبراني لديها بشكل شامل، بما في ذلك تحديد الأصول المهمة والتهديدات المحتملة ونقاط الضعف والمتطلبات التنظيمية.
2. **تطوير السياسات :**يتضمن ذلك إنشاء سياسات واضحة وشاملة للأمن السيبراني تتوافق مع المعايير واللوائح والتشريعات السارية.
3. **تقييم المخاطر :**يشمل هذا تحديد وتقييم المخاطر وتحديد أولوياتها، مع مراعاة تأثيرها المحتمل واحتمال وقوعها.
4. **تنفيذ الرقابة :**يتطلب ذلك تنفيذ الضوابط والإجراءات الأمنية المناسبة للتخفيف من المخاطر المحددة. ذلك يشمل الحلول التقنية والعمليات وتدريب الموظفين.

5. **المراقبة وإعداد التقارير :**يجب مراقبة التدابير الأمنية بشـــكل دوري وتقييم فعاليتها. يتعين أيضًا إعداد تقارير منتظمة للإدارة وأصحاب المصلحة.
6. **تخطيط اســتجابة للحوادث :**يجب تطوير وصــياغة خطة اســتجابة للحوادث وتحديثها بانتظام لضمان اتخاذ إجراءات سريعة وفعالة في حالة وقوع حادث سيبراني.

الخلاصة :الحوكمة وإدارة المخاطر والامتثال في مجال الأمن السيبراني تمثل إطار عمل حيوي يمكن للمنشـــآت من خلاله التنقل بثقة في البيئة الســـيبرانية المعقدة. من خلال بناء هياكل الحوكمة وإدارة المخاطر وضـــمان الامتثال، يمكن للمنشـــآت بناء مرونة تســاعدها على مواجهة التهديدات الســيبرانية المتزايدة، وذلك بما يحافظ على كفاءتها التشغيلية ويحمي سمعتها. في عصر يتزايد فيه التهديد السيبراني باستمرار، يعد تبني نهج شـامل للحوكمة وإدارة المخاطر والامتثال ضـرورة حاسـمة للمنشـآت التي تتطلع إلى الازدهار في العالم الرقمي.

أهمية نموذج :GRC الحوكمة وإدارة المخاطر والامتثال

من خلال تنفيذ نموذج GRC (الحوكمة وإدارة المخاطر والامتثال)، يمكن للشركات اتخاذ قرارات أفضل في بيئة تفهم بشكل أفضل للمخاطر. يساعد برنامج GRCالفعّال أصحاب المصلحة الرئيسيين على وضع السياسات واتخاذ القرارات من منظور مشترك، والامتثال للمتطلبات التنظيمية. بفضل نموذجGRC ، يمكن للشركة بأكملها توجيه جهودها نحو تحقيق الأهداف بطريقة متنسقة.

فيما يلي بعض الفوائد الرئيسية لتنفيذ استراتيجية GRC في المؤسسات:

1. **اتخاذ القرارات المستندة إلى البيانات :**يمكن للشركات اتخاذ قرارات مستندة إلى البيانات بشكل أفضل من خلال مراقبة الموارد ووضع القواعد والأطُر العملية، واستخدام برمجيات وأدوات.GRC
2. **تحسين العمليات :**يبسط نموذج GRC العمليات ويجعلها تركز على ثقافة مشتركة تعزّز القيم الأخلاقية وتهيئ بيئة صحية تحفّز النمو. كما يساعد في تطوير الثقافة التنظيمية القوية واتخاذ القرارات الأخلاقية في المنظمة.

3. **تعزيز الأمن السيبراني :**يساعد نهج GRC المتكامل في استخدام تدابير أمان البيانات لحماية بيانات العملاء والمعلومات الحساسة. هذا يساعد المؤسسات على الامتثال للوائح خصوصية البيانات مثل اللائحة العامة لحماية البيانات (GDPR)، مما يعزز ثقة العملاء ويحمي من العقوبات.

تجدر الإشارة إلى أن الدافع وراء تنفيذ استراتيجية GRC يكمن في التحديات التي تواجه الشركات في بيئة الأعمال المعاصرة، مثل التهديدات السيبرانية والتغيرات التنظيمية وحاجة الشركات للامتثال وحماية البيانات والتعامل مع عدم اليقين. إن تبني نهج متكامل للحوكمة وإدارة المخاطر والامتثال ليس مجرد اختيار، بل هو ضرورة لضمان استدامة الأعمال في هذا العصر الرقمي.

آلية عمل نموذج GRC (الحوكمة وإدارة المخاطر والامتثال)

يعتمد نموذج GRC (الحوكمة وإدارة المخاطر والامتثال) في أي منظمة على مبادئ أساسية لضمان التعاون والتنسيق بين الإدارات المختلفة التي تتعامل مع الحوكمة وإدارة المخاطر والامتثال. يشمل هذا التعاون أصحاب المصلحة الرئيسيين الذين يلعبون أدوارًا متعددة في المنظمة. إليك بعض الأمثلة:

1. **كبار المديرين التنفيذيين :**يقومون بتقييم المخاطر عند اتخاذ القرارات الإستراتيجية ويحددون الاتجاهات الرئيسية للمؤسسة.
2. **الأقسام القانونية :**تقوم بمساعدة الشركات في فهم والتعامل مع التعرض للمخاطر القانونية والقضايا ذات الصلة.
3. **إدارة المالية :**تضمن الامتثال للمتطلبات التنظيمية المالية وتدعم الإجراءات الضرورية.
4. **إدارة الموارد البشرية :**تتعامل مع معلومات التوظيف الحساسة وتضمن الامتثال للمتطلبات ذات الصلة.
5. **أقسام تكنولوجيا المعلومات :**تعمل على حماية البيانات من التهديدات السيبرانية وضمان الأمان السيبراني.

نظام الإطار العمل GRC هو العنصر الأساسي لإدارة المخاطر والامتثال والحوكمة في المنظمة. يتضمن هذا الإطار تحديد السياسات الرئيسية التي توجه جهود المؤسسة نحو أهدافها. من خلال تبني هذا الإطار، يمكن للشركة تنظيم العمليات بشكل فعّال واتخاذ قرارات مستنيرة وضمان استدامة الأعمال.

الشركات تستند إلى أطُر عمل GRC لتوجيه مسارات العمل وتنظيم السياسات وتحقيق الأهداف الإستراتيجية. قد يتضمن ذلك استخدام البرمجيات والأدوات المتخصصة لتنظيم ومراقبة نجاح هذا الإطار.

مفهوم نضج GRC يقيس مدى تكامل الحوكمة وتقييم المخاطر والامتثال داخل المؤسسة. النضج العالي في GRC يشير إلى تحقيق أعلى كفاءة وفعالية في إدارة المخاطر والامتثال بتكلفة منخفضة. وعلى النقيض، النضج المنخفض يشير إلى عدم تحقيق الإنتاجية المطلوبة وعدم التنسيق الكافي بين وحدات الأعمال.

زكي حسين متولي, م., مصطفى, عبد العال سالم غريب, & حسين. (2022). قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة الخارجية: دراسة تطبيقية. المجلة العلمية للدراسات المحاسبية, 4(4), 245-328.

تدريبات

أسئلة اختيار من متعدد:

1. ما هي الهدف الرئيسي للحوكمة السيبرانية؟
   - أ) زيادة الإنتاجية
   - ب) تحسين الأمان وإدارة المخاطر السيبرانية
   - ج) توفير الترفيه للموظفين
2. ما هو دور مجلس الإدارة (Board of Directors) في الحوكمة السيبرانية؟
   - أ) يدير عمليات الشركة اليومية
   - ب) يتولى مسؤولية تقييم المخاطر السيبرانية واتخاذ القرارات الاستراتيجية ذات الصلة
   - ج) يدير الأمور الفنية للشركة
3. ما هو تعريف إدارة المخاطر السيبرانية؟
   - أ) عملية حماية البيانات فقط
   - ب) عملية تحديد وتقييم ومراقبة المخاطر السيبرانية واتخاذ الإجراءات اللازمة للتعامل معها
   - ج) تطوير البرمجيات والتقنيات السيبرانية
4. ما هي واحدة من مبادئ الحوكمة السيبرانية؟
   - أ) الإهمال في مراقبة الأنشطة السيبرانية
   - ب) الشفافية والمساءلة
   - ج) تجاهل التقنيات الحديثة
5. ما هو الهدف الرئيسي لإدارة المخاطر السيبرانية؟

- أ) القضاء على جميع المخاطر السيبرانية
- ب) التعرف على المخاطر واتخاذ إجراءات للتحكم بها والحد منها
- ج) تجاهل المخاطر وعدم التعامل معها

6. ما هو دور مسؤول أمان المعلومات (CISO) في الشركة؟

- أ) يدير العمليات اليومية للشركة
- ب) يتولى مسؤولية تقييم المخاطر السيبرانية وتطبيق السياسات والتدابير الأمنية
- ج) يدير قسم الموارد البشرية

7. ما هو دور الأمان السيبراني في الحوكمة السيبرانية؟

- أ) ليس له دور في الحوكمة السيبرانية
- ب) يعتبر جزءًا من استراتيجية الحوكمة للحفاظ على الأمان وإدارة المخاطر
- ج) يعمل بشكل مستقل عن الحوكمة السيبرانية

8. ما هو تعريف تصنيف المخاطر السيبرانية (Cyber Risk Classification)؟

- أ) عملية تصنيف الشبكات السيبرانية إلى أنواع مختلفة
- ب) عملية تصنيف المخاطر السيبرانية بناءً على مستوى التهديد والتأثير
- ج) عملية تصنيف البرامج الضارة

9. ما هو الهدف الأساسي للمراجعة السيبرانية(Cyber Audit) ؟

- أ) العثور على الثغرات السيبرانية وتجنبها
- ب) التحقق من مطابقة التقنيات السيبرانية للمعايير والسياسات

- ج) القيام بعمليات تجسس سيبراني

10. ما هو تعريف الوعي السيبراني(Cyber Awareness) ؟

- أ) عملية توعية الكمبيوترات بالمخاطر السيبرانية
- ب) توعية الموظفين والأفراد بمخاطر الأمان السيبراني وكيفية التصرف بأمان
- ج) استخدام التقنيات السيبرانية للوعي

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: الحوكمة السيبرانية ليست ضرورية للمؤسسات والشركات.
2. صحيح أو خطأ: الهدف الرئيسي لإدارة المخاطر السيبرانية هو التعامل مع جميع المخاطر بنسبة 100٪.
3. صحيح أو خطأ: تصنيف المخاطر السيبرانية يعتمد على التهديدات فقط دون النظر في التأثير.
4. صحيح أو خطأ: الأمان السيبراني لا يتعامل مع الهجمات السيبرانية.
5. صحيح أو خطأ: دور مجلس الإدارة في الحوكمة السيبرانية يتضمن تقديم الدعم المالي فقط.
6. صحيح أو خطأ: تصنيف المخاطر السيبرانية يساعد في تحديد أولويات الحماية السيبرانية.
7. صحيح أو خطأ: الوعي السيبراني يتعامل فقط مع الجوانب التقنية للأمان السيبراني.
8. صحيح أو خطأ: الحوكمة السيبرانية تتعامل مع كيفية إدارة المخاطر السيبرانية داخل المؤسسة.
9. صحيح أو خطأ: المراجعة السيبرانية تقوم بالتحقق من تطبيق السياسات السيبرانية داخل المؤسسة.

10. صحيح أو خطأ: الأمان السيبراني لا يشمل حماية البيانات والمعلومات فقط، بل أيضًا الحفاظ على توافر الأنظمة والخدمات السيبرانية.

الوحدة التدريبية السابعة

حماية البيانات والأنظمة والشبكات

الوحدة السابعة : حماية البيانات والأنظمة والشبكات

الجدارة:

يتمكن المتدرب من حماية البيانات والأنظمة والشبكات.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- حماية البيانات.
- الأنظمة والشبكات.

الوقت المتوقع للتدريب:

9 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب كيفية حماية البيانات والأنظمة والشبكات.

حماية البيانات والأنظمة والشبكات

أمان الشبكات هو مجموعة من الإجراءات والتدابير التي تهدف إلى توفير أقصى مستوى من الحماية للبيانات والمعلومات على الشبكة من جميع أشكال التهديدات، سواء كانت داخلية أو خارجية. يتضمن ذلك استخدام الأدوات والتقنيات الضرورية لحماية الموارد والأنظمة الرقمية والاتصالات على الشبكة.

تتمثل فوائد أمان الشبكات في:

1. **حماية البيانات الحساسة :**يتيح أمان الشبكات الحفاظ على خصوصية وسرية البيانات والمعلومات الحساسة ومنع الوصول غير المصرح به إليها.
2. **ضمان الوصول الصحيح :**يساعد في التحقق من أن الأفراد والجهات المصرح لهم فقط يمكنهم الوصول إلى الموارد والبيانات المهمة.
3. **الوقاية من التهديدات السيبرانية :**يقلل من خطر الهجمات السيبرانية ويعزز من مقاومة الاختراقات والاستجابة لها بفعالية.
4. **تحسين أداء الشبكة :**يمكن تحقيق أداء أفضل للشبكة من خلال توفير حماية واجتياز لاختبارات الأمان وتحسين استقرارها.

بودوشة, شاكر, بلجودي, & احلام/مشرف. (2017). حماية البيانات الشخصية في مجال التجارة الالكترونية (Doctoral dissertation, جامعة جيجل).

أمان الشبكات يعتمد على عدة أنواع من تقنيات الحماية والأدوات التي تشمل:

1. **جدران الحماية :(Firewalls)** تعمل على منع الوصول غير المصرح به إلى الشبكة وتصفية حركة المرور الواردة والصادرة.
2. **أذونات الوصول :(Authorization)** تحدد الصلاحيات والأذونات للمستخدمين والأنظمة للوصول إلى الموارد والبيانات.
3. **برامج مكافحة البرامج الضارة :(Antivirus Software)** تكتشف وتزيل البرامج الضارة والفيروسات من الأنظمة.
4. **أمان التطبيق :(Application Security)** تضمن حماية التطبيقات البرمجية من التهديدات والهجمات السيبرانية.
5. **منع فقدان البيانات :(Data Loss Prevention)** يمنع تسرب أو فقدان البيانات الحساسة.
6. **أمان البريد الإلكتروني :(Email Security)** يمنع رسائل البريد الإلكتروني الضارة والصيد الاحتيالي.
7. **جمع البيانات ومراقبة الشبكة :(Network Monitoring)** يتيح للمشرفين رصد حركة المرور والأنشطة على الشبكة للكشف عن أي أنشطة غير مصرح بها.
8. **أمان الأجهزة :(Hardware Security)** تتعامل مع حماية الأجهزة الفعلية مثل الخوادم وأجهزة التوجيه والأجهزة المحمولة.

أساسيات حماية الشبكات من الاختراق تشمل الحماية، والكشف، والاستجابة. تتضمن الحماية تنفيذ تدابير الأمان وتكوين النظام بشكل آمن. الكشف يتعامل مع رصد وتحليل الأنشطة على الشبكة لاكتشاف أي تهديدات محتملة. أما الاستجابة فتشمل اتخاذ إجراءات لمواجهة واحتواء الهجمات عندما تحدث.

لتحقيق الأمان الشامل للشبكة، هناك مجموعة متنوعة من التقنيات المختلفة التي يجب تنفيذها. من المهم أيضًا استخدام أكثر من طريقة واحدة للسلامة لأنه في بعض

الأحيان يمكن اختراق خط دفاع واحد، وعندما يتم استخدام العديد من خطوط الدفاع، يصعب على المخترق اختراق الشبكة. الآن دعونا نستكشف الخطوات:

1. **جدران الحماية :**جدران الحماية هي الحاجز الأساسي بين شبكتك الداخلية والشبكة الخارجية على الإنترنت. باستخدام جدران الحماية مع مجموعة معينة من القواعد، يمكنك التحكم في الاتصالات المسموح بها ومنع الاتصالات المشبوهة التي يمكن أن تضر بشبكتك.
2. **ضوابط الوصول :**يجب تقييد الوصول إلى شبكتك والتحكم فيه بشكل دقيق. يجب تحديد من يسمح لهم بالوصول إلى الشبكة وتحديد الأجهزة المسموح بها. ويمكن تطبيق سياسات الأمان وضبط الوصول إلى المعلومات.
3. **برامج مكافحة البرامج الضارة :**تستخدم لاكتشاف وإزالة البرامج الضارة والفيروسات من الأنظمة. يجب تحديث هذه البرامج بانتظام للحفاظ على الحماية.
4. **أمان التطبيق :**يشمل حماية التطبيقات البرمجية من التهديدات والهجمات السيبرانية من خلال تصميم آمن واختبار أمان التطبيق.
5. **منع فقدان البيانات :**يهدف إلى منع تسرب أو فقدان البيانات الحساسة عن طريق مراقبة ومنع نقل البيانات غير المصرح به.
6. **أمان البريد الإلكتروني :**يتعامل مع الحماية من رسائل البريد الإلكتروني الضارة والصيد الاحتيالي ويحد من تسلل البرامج الضارة عبر رسائل البريد الإلكتروني.
7. **جمع البيانات ومراقبة الشبكة بشكل مستمر :**يتيح للمشرفين رصد حركة المرور والأنشطة على الشبكة لاكتشاف أي أنشطة مشبوهة والتصدي لها.
8. **أمان الأجهزة :**يشمل حماية الأجهزة الفعلية مثل الخوادم وأجهزة التوجيه والأجهزة المحمولة من الهجمات السيبرانية والتهديدات.

هذه هي الخطوات الرئيسية التي يجب تنفيذها لضمان أمان الشبكات. إذا تم تنفيذ هذه الإجراءات بشكل صحيح، ستزيد من مقاومة الشبكة للهجمات وتحسين أمانها بشكل كبير.

تأمين الأجهزة الموجودة على الشبكة

تأمين الأجهزة الموجودة على الشبكة يعتبر أمرًا بالغ الأهمية للمحافظة على خصوصية وأمان البيانات التي تتنقل عبر الشبكة. غالبًا ما يُنظر إلى الشبكات على أنها مجرد أجهزة كمبيوتر متصلة بالإنترنت، وهذا الاعتقاد البسيط يمكن أن يجعلها عرضة للاختراق من قِبَل المهاجمين، وبالأخص عند استهداف أجهزتك المحمولة والتطبيقات التي تقوم بتنزيلها.

لذا، يجب عليك اتخاذ خطوات لتأمين الأجهزة المتصلة بالشبكة بهدف حماية خصوصية البيانات والمعلومات الحساسة. إليك بعض الخطوات المهمة لتحقيق ذلك:

1. **معرّف الأجهزة :**قم بتعيين مُعرف فريد لكل جهاز متصل بشبكتك الخاصة، وهذا يشمل الأجهزة المحمولة وأجهزة الكمبيوتر والأجهزة الذكية. يُمكن أن يكون معرّف الجهاز عبارة عن اسم مستخدم وكلمة مرور.
2. **تأمين الواي فاي :**قم بتأمين شبكة الواي فاي الخاصة بك باستخدام كلمة مرور قوية. تأكد من تغيير كلمة المرور الافتراضية للمودم أو جهاز الواي فاي الخاص بك.
3. **مراقبة الأجهزة المتصلة :**قم بمراقبة الأجهزة المتصلة بشبكتك وتحقق من أنها مألوفة وموثوقة. لا تسمح باتصال أي جهاز مجهول بالواي فاي الخاص بك.
4. **تنزيل التطبيقات :**تجنب تنزيل التطبيقات من مصادر غير رسمية أو غير موثوقة. استخدم متاجر التطبيقات الرسمية مثل Google Play Store أو Apple App Storeللحصول على التطبيقات.

5. **تصفح آمن :**تجنب زيارة مواقع الويب التي لا تحتوي على شهادة SSL (Secure Sockets Layer)، والتي توفر تشفيرًا آمنًا للاتصال بين المتصفح والخادم.

تتبع هذه الخطوات ستساهم بشكل كبير في تعزيز أمان الأجهزة الموجودة على الشبكة وحماية بياناتك من الاختراقات والتهديدات السيبرانية.

بودوشة, شاكر, بلجودي, & احلام/مشرف. (2017). حماية البيانات الشخصية في مجال التجارة الالكترونية (Doctoral dissertation, جامعة جيجل).

تدريبات

أسئلة اختيار من متعدد:

1. ما هو أحد أساليب حماية البيانات في حالات الطوارئ مثل حرائق المباني أو الكوارث الطبيعية؟
   - أ) التخزين المزدوج
   - ب) التخزين المشفر
   - ج) التخزين السحابي
2. ما هو الجدار الناري (Firewall) في سياق الأمان السيبراني؟
   - أ) جهاز يحمي المباني من الحرائق
   - ب) برنامج أو جهاز يحمي الشبكة من الهجمات السيبرانية
   - ج) خدمة توصيل الإنترنت
3. ما هي أحد أساليب تشفير البيانات؟
   - أ) النسيج
   - ب) الإخفاء
   - ج) الكسر
4. ما هو الهدف الرئيسي لنظام اكتشاف التسلل (Intrusion Detection System - IDS)؟
   - أ) منع الوصول إلى الإنترنت
   - ب) اكتشاف الهجمات أو الانتهاكات في الشبكة
   - ج) تحليل البيانات الشخصية

5. ما هو الهجوم بالتصيُّد(Phishing Attack) ؟

- أ) هجوم يستهدف البيانات الحساسة عبر إرسال رسائل طلب الصداقة على وسائل التواصل الاجتماعي
- ب) هجوم يستهدف البيانات الحساسة عبر القرصنة
- ج) هجوم يستهدف البيانات الحساسة عبر التلاعب بالمستخدمين للوصول إلى معلوماتهم

6. ما هو التصيُّد الهجين(Spear Phishing) ؟

- أ) نوع من أنواع الصيد الرياضي
- ب) هجوم يستهدف مجموعات كبيرة من الأفراد
- ج) هجوم يستهدف أفراد أو مؤسسات محددة بشكل مستهدف

7. ما هي واحدة من أساليب تعزيز أمان كلمات المرور؟

- أ) استخدام كلمات مرور قصيرة وبسيطة
- ب) تغيير كلمات المرور فقط عند نسيانها
- ج) استخدام كلمات مرور قوية وتحديثها بانتظام

8. ما هو البرنامج الضار(Malware) ؟

- أ) برنامج يزيد من أداء الحاسوب
- ب) برنامج يتسبب في الأضرار للأنظمة أو يسرق المعلومات
- ج) برنامج يستخدم في تحرير الصور

9. ما هو الاختراق الأخلاقي(Ethical Hacking) ؟

- أ) هجوم غير قانوني على الأنظمة
- ب) استخدام القرصنة في الهجمات السيبرانية
- ج) استخدام مهارات القرصنة بشكل قانوني لاختبار الأمان السيبراني

10. ما هي أحد أساليب الاحتيال الإلكتروني(E-Fraud) ؟

- أ) الدفع عبر البطاقة الائتمانية
- ب) استخدام البريد الإلكتروني للاحتيال واستخراج المعلومات الحساسة
- ج) شراء المنتجات عبر الإنترنت بأقل تكلفة.

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: الجدار الناري يعمل على حماية الشبكة من الهجمات السيبرانية.
2. صحيح أو خطأ: تشفير البيانات يقوم بتحويل البيانات إلى صيغة غير قابلة للقراءة حتى وإن تم الوصول إليها.
3. صحيح أو خطأ: نظام اكتشاف التسلل يقوم بالوصول إلى أمان البيانات داخل الشبكة.
4. صحيح أو خطأ: التصيُّد يشمل إرسال رسائل طلب الصداقة فقط.
5. صحيح أو خطأ: التصيُّد الهجين يستهدف أفرادًا أو مؤسسات محددة بشكل مستهدف.
6. صحيح أو خطأ: تغيير كلمات المرور بانتظام ليس له تأثير على الأمان السيبراني.
7. صحيح أو خطأ: البرامج الضارة هي برامج مصممة لتحسين أداء الحواسيب.
8. صحيح أو خطأ: الاختراق الأخلاقي يستخدم مهارات القرصنة للقيام بأنشطة غير قانونية.
9. صحيح أو خطأ: الجدران النارية تقيد الوصول إلى الشبكة فقط دون السماح بالمرور.
10. صحيح أو خطأ: الاحتيال الإلكتروني يتضمن استخدام البريد الإلكتروني للغش والاحتيال بهدف استخراج المعلومات الحساسة.

الوحدة التدريبية الثامنة

الدراية الأمنية ورصد التهديدات السيبرانية

الوحدة الثامنة : الدراية الأمنية ورصد التهديدات السيبرانية

الجدارة:

يتمكن المتدرب من الدراية الأمنية ورصد التهديدات السيبرانية.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- الدراية الأمنية.
- التهديدات السيبرانية.

الوقت المتوقع للتدريب:

6 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب كيفية الدراية الأمنية ورصد التهديدات السيبرانية.

الدراية الأمنية ورصد التهديدات السيبرانية

الدراسة الأمنية (Security Studies) هي مجال دراسي يركز على فهم وتحليل التحديات والمسائل المتعلقة بالأمن الوطني والدولي. يهتم هذا المجال بدراسة مجموعة واسعة من المواضيع المتعلقة بالأمن، بما في ذلك الأمن السياسي والعسكري والاقتصادي والبيئي والاجتماعي.

تشمل مواضيع الدراسة الأمنية ما يلي:

1. الأمن الوطني: دراسة التهديدات التي تواجه الدولة وكيفية حماية الأمن والاستقرار الوطني. يمكن أن تتضمن هذه التهديدات الإرهاب، والنزاعات الداخلية، والأمان الحدودي، والتهديدات السيبرانية، والأمان الطاقوي، والأمن الصحي، والمزيد.
2. العلاقات الدولية والأمن الدولي: دراسة العلاقات بين الدول والمؤسسات الدولية وكيفية التعامل مع النزاعات الدولية والأمن الإقليمي والدولي.
3. الأمن السياسي: تحليل العوامل السياسية التي تؤثر في الأمن الوطني والدولي، مثل السياسات الخارجية والتحالفات والصراعات الداخلية.
4. الأمن الاقتصادي: دراسة كيفية تأثير الاقتصاد والتجارة الدولية على الأمن الوطني والدولي، بالإضافة إلى التهديدات المرتبطة بالأمن الاقتصادي مثل الهجمات السيبرانية على البنية التحتية الحيوية.

الزهراني, عبد الله بن يحي سعيد الخزمري, الشهري, & حسن بن أحمد. مشرف. (2020). استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة: دراسة مقارنة (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية).

5. الأمن البيئي: تقدير تأثير التغيرات المناخية والتلوث على الأمان البيئي والدولي، وكيفية إدارة المخاطر المتعلقة بالبيئة.
6. الأمن الاجتماعي: دراسة العوامل الاجتماعية التي تؤثر في الأمان الوطني والدولي، مثل الصراعات العرقية والدينية والتمييز والهجرة.

تهدف الدراسة الأمنية إلى تزويد الطلاب والباحثين بالأدوات والمفاهيم اللازمة لفهم وتقدير التحديات الأمنية المعاصرة وتطوير استراتيجيات للتعامل معها. يمكن أن تكون هذه الدراسة مفيدة للأفراد الذين يسعون للعمل في مجالات مثل السياسة الخارجية، والأمن القومي، والشؤون الدولية، والأمن السيبراني، والعمل الإنساني، والمزيد.

التهديدات السيبرانية

"التهديدات السيبرانية ومصادرها هي جزء لا يتجزأ من تطور التكنولوجيا والإنترنت، الذي ساهم بشكل كبير في تسهيل التواصل والتفاعل بين الأفراد والجماعات على مستوى عالمي. قبل ظهور الإنترنت، كان التواصل الدولي يعتمد بشكل رئيسي على وسائل مثل البريد السريع والرسائل البرقية، وكانت هذه العمليات تستغرق وقتًا طويلاً لنقل الرسائل والرد عليها.

مع اختراع الإنترنت، تغيرت هذه الديناميات بشكل جذري، حيث أصبح بإمكان الناس التواصل وتبادل المعلومات بشكل فوري وفعال. يُعَتبر الإنترنت اليوم مساحة إلكترونية مشتركة تتيح للأفراد والثقافات التفاعل والتبادل بسهولة.

ومع ذلك، لم يكن الأمر خاليًا من التحديات والتهديدات. ظهرت ما نعرفه اليوم بالتهديدات السيبرانية، وهي تهديدات ومخاطر يمكن أن يواجهها المستخدمون على الإنترنت بغض النظر عن هويتهم أو دورهم. يمكن أن تأتي هذه التهديدات من أفراد

أو جماعات أو مؤسسات، وتهدف عادة إلى إلحاق الضرر والتدمير أو الاستفادة من الأهداف المستهدفة.

تشمل هذه التهديدات أنواعًا متعددة من الهجمات، مثل هجمات الاختراق والسرقة السيبرانية والابتزاز الإلكتروني والتخريب. وغالبًا ما تتم تلك الأنشطة الضارة من قبل مجموعات من المخترقين والمجرمين السيبرانيين الذين يعملون في الظلام على الويب.(Dark Web)

على الرغم من الإيجابيات التي جلبها الإنترنت، فإن وجوده أيضًا أتاح الفرص للأشخاص غير الأخلاقيين لارتكاب أعمال إجرامية عبر الشبكة. يتعين على المجتمع الدولي تبني استراتيجيات فعالة لمكافحة هذه التهديدات وحماية الأمان السيبراني للمستخدمين".

مصادر التهديدات السيبرانية

"تواجهنا يوميًا على الإنترنت مجموعة متنوعة من التهديدات السيبرانية، وتأتي هذه التهديدات من مصادر متعددة ومتنوعة، مما يجعل المستخدمين في جميع أنحاء العالم عرضة للخطر. فالإنترنت أصبح مكانًا للتواصل والتفاعل بين الأفراد والجماعات، ولكنه أيضًا جذب العديد من الجهات الضارة، ومن بين أبرز مصادر التهديدات السيبرانية:

1. المنظمات الإجرامية السيبرانية: هذه المنظمات تتخصص في الأنشطة الإجرامية عبر الإنترنت وتهدف إلى السرقة والابتزاز والتخريب. تقوم بتنفيذ هجمات قوية ومحددة تستهدف مختلف الأفراد والمؤسسات.
2. القراصنة: يعمل القراصنة عادة بشكل فردي ويتخصصون في اختراق الأنظمة والشبكات. يمتلكون مهارات برمجية وأدوات تساعدهم في تنفيذ عمليات القرصنة.

3. الإرهابيون: تستخدم بعض الجماعات الإرهابية هجمات سيبرانية لتدمير البنى التحتية والمرافق الحيوية في مناطق معينة بهدف نشـــر الرعب والتأثير على الأمان.
4. المنافسون: تستخدم بعض الشركات والمؤسسات القراصنة لمهاجمة منافسيها وسرقة معلوماتهم التنافسية أو تدمير بنيتهم التحتية.
5. الحكومات: قد تســـتخدم الحكومات بعض المخترقين لأغراض اســـتخباراتية وهجمات سيبرانية ضد دول أخرى بهدف التجسس أو التخريب.
6. شـــركاء العمل: قد يتورط بعض موظفي الشـــركات في عمليات القرصـــنة لأسباب مثل الانتقام أو الحصول على معلومات محددة.

تلك المصـــادر تشـــكل تحديات ســـيبرانية مســـتمرة للأمان على الإنترنت، وتتطلب مكافحتها جهودًا مشـــتركة واســـتراتيجيات فعالة لحماية المعلومات والبيانات الحساسة".

مخاطر التهديدات السيبرانية

"تُعَتَبَر التهديدات السيبرانية نقطة سوداء في عالم الإنترنت، حيث تلحق سنويًا آلاف الأضـــرار بمســـتخدمي الإنترنت في جميع أنحاء العالم، بغض النظر عن نوعهم واحتياجاتهم. تتضمن هذه التهديدات مجموعة متنوعة من المخاطر، بما في ذلك:

1. البرمجيات الضـــارة: تشـــكل البرمجيات الضـــارة تهديدًا يســـتهدف أجهزة المستخدمين عبر الإنترنت، وعادةً ما تأتي من خلال البريد الإلكتروني. تسبب هذه البرمجيات الضارة تدميرًا لأنظمة الأجهزة وسرقة البيانات أو تلفها.
2. التجسس والتنصت: يُعد التجسس والتنصت عمليات اختراق تستهدف جهاز المســـتخدم ومراقبة المكالمات والبيانات بدون علمه. يمكن لتثبيت برامج VPNحماية جهازك من هذا الخطر.
3. برامج الفدية: تمثل برامج الفدية تهديدًا كبيرًا حيث تُشـــفر وتقفل ملفات المستخدم بعد اختراقها، مع مطالبة المستخدم بدفع فدية لاستعادة بياناته.

4. سرقة كلمات المرور: يتم سرقة كلمات المرور الشخصية وتغييرها من قبل المخترقين، مما يعرض البيانات للسرقة ويجعلها غير آمنة.
5. هجمات الصيد: تشمل هجمات الصيد رسائل تستند إلى المصداقية والتي تُطلب من المستخدمين إدخال معلومات شخصية هامة بمجرد النقر على الروابط.
6. هجمات المواقع: تستهدف هذه الهجمات مواقع الويب الضعيفة وتستهدف الاختراق والسرقة أو التعطيل.
7. فيروس طروادة: يتم استدراج المستخدمين لتنزيل برامج تنكر بأنها قانونية ولكنها في الواقع ضارة.
8. هجمات :SQL تستهدف هجمات SQL تغيير واستغلال قواعد البيانات على المواقع.
9. رفض الخدمة الموزع: تستهدف هذه الهجمات الخوادم الرئيسية لتعطيل الخدمات وتحطيم الأداء.

هذه المخاطر تجعل الأمان على الإنترنت أمرًا حاسمًا، وتشدد على أهمية اتخاذ التدابير اللازمة لحماية البيانات الشخصية والأنظمة".

إحصائيات الهجمات الإلكترونية

- يستمر تزايد وتطور التهديدات السيبرانية سنة بعد سنة، نتيجة للتقدم في مجال البرمجيات والإمكانيات المتاحة في هذا المجال. وهذا التطور أثر بشكل كبير على أمان الإنترنت وأثار قلقًا متزايدًا.
- تبلغ تكلفة الجرائم الإلكترونية السنوية العالمية حوالي 10.5 تريليون دولار، ومن المتوقع أن تزيد بمعدل نمو سنوي يبلغ حوالي 15٪، وذلك بحلول عام 2025.
- تقع حوالي ثلثي الهجمات والانتهاكات السيبرانية نتيجة لأخطاء بشرية، وتصل نسبتها إلى حوالي 85٪ من مجموع التهديدات.
- أكثر من نصف الهجمات الإلكترونية تستهدف أهدافًا مالية، بنسبة تبلغ حوالي 70٪، وتليها السرقات الفكرية والاختراق والتجسس.
- تصل حوالي 95٪ من البرمجيات الضارة التي تخترق أجهزتنا عبر الإنترنت عبر البريد الإلكتروني والرسائل الواردة.
- يحدث هجوم برامج الفدية كل ثانية في جميع أنحاء العالم.
- من المتوقع أن تبلغ تكلفة الأضرار الناتجة عن الهجمات الإلكترونية:
  - 190ألف دولار في الثانية.
  - 11.4مليون دولار في الدقيقة.
  - 684.9مليون دولار في الساعة.
  - 16.4مليار دولار في اليوم.
  - 115.4مليار دولار في الأسبوع.
  - 500مليار دولار في الشهر.
  - 6تريليون دولار في السنة.

- من المتوقع أن تصل قيمة صناعة الأمان السيبراني والحماية السيبرانية إلى حوالي 400 مليار دولار أمريكي بحلول عام 2027، نظرًا لزيادة الطلب على التكنولوجيا وأهمية حماية الأنظمة.
- يتجاوز 80٪ من الهجمات الإلكترونية المستهدفة هجمات التصيد الاحتيالي.
- تتعرض يوميًا أكثر من 30,000 موقع عالمي للاختراق.
- تتم تنفيذ أكثر من 23,000 هجوم DDoS على الإنترنت يوميًا.
- تتعرض يوميًا أكثر من 65,000 شركة صغيرة ومتوسطة في الولايات المتحدة لأنواع متعددة من الهجمات الإلكترونية.
- من المتوقع زيادة تكاليف الهجمات برامج الفدية بحوالي 300 مليار دولار في العقد المقبل.
- سُجلت حالة وفاة واحدة على الأقل في عام 2020 نتيجة لاختراق نظام جامعة دوسلدورف الألمانية.

خريطة الهجمات الإلكترونية وأفضل المواقع لمتابعتها

في ظل الزيادة الكبيرة في استخدام الإنترنت وتوسع نطاق وجوده في كل مكان، تصاعدت بؤرة الهجمات الإلكترونية وأصبحت تشكل تهديدًا كبيرًا على الشركات، والمؤسسات، وحكومات العالم من حيث أمانهم السيبراني. لذا، أصبح من الضروري وجود خرائط توضح سير وتطور هذه الهجمات الإلكترونية لحظة بلحظة. ومن بين الخرائط البارزة في هذا السياق:

1. **خريطة تفاعلية للهجمات الإلكترونية من شركة Norse:** تقدم شركة Norseخريطة تفاعلية تمثل الهجمات السيبرانية حول العالم بشكل واسع ودقيق. تستند هذه الخريطة إلى أكثر من 8 ملايين حساس استشعار لجمع المعلومات حول الهجمات الإلكترونية، وتعرض تفاصيل حول مكان وسير تطور البرمجيات الضارة.

2. **Kaspersky Lab:** تقدم Kaspersky Lab خريطة تفاعلية تساعد في تتبع الهجمات الإلكترونية والفيروسات حول العالم. تعرض الخريطة الهجمات على شكل كرة أرضية تفاعلية، مما يسهل تحديد بلد معين للحصول على تفاصيل دقيقة حول الهجمات السيبرانية في تلك المنطقة.
3. **FireEye خريطة التهديدات السيبرانية:** تقدم FireEye خريطة توضح الهجمات الإلكترونية في منطقة معينة خلال الـ 30 يومًا السابقة. تساعد هذه الخريطة على متابعة التهديدات السيبرانية والتبليغ عن أي هجمات تم رصدها.
4. **CheckPoint و Fortinet:** تعتبر هذه الشركتين أيضًا من مقدمي الخدمات الأمنية السيبرانية، وتقدمان معلومات متعمقة عن الهجمات الإلكترونية والتهديدات السيبرانية حول العالم.

هذه الخرائط تلعب دورًا حيويًا في توعية الجمهور بشأن التهديدات السيبرانية وتمكن المحترفين من مراقبة ومكافحة هذه الهجمات بشكل فعال.

الزهراني, عبد الله بن يحي سعيد الخزمري, الشهري, & حسن بن أحمد. مشرف. (2020). استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة: دراسة مقارنة (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية).

تدريبات

أسئلة اختيار من متعدد:

1. ما هو الهدف الرئيسي للدراية الأمنية(Security Awareness) ؟
   - أ) تدريب المهنيين في مجال الطب
   - ب) زيادة وعي الموظفين بأمور الأمان السيبراني
   - ج) تصميم تطبيقات الجوال
2. ما هي الأداة التي يمكن استخدامها لرصد التهديدات السيبرانية والاختراقات؟
   - أ) برامج مكافحة البرمجيات الخبيثة
   - ب) الهواتف الذكية
   - ج) الأقراص اللوحية
3. ما هو الهدف الرئيسي لرصد التهديدات السيبرانية؟
   - أ) تنظيم الفعاليات الاجتماعية
   - ب) الكشف المبكر عن هجمات الأمان السيبراني
   - ج) تصميم مواقع الويب
4. ما هو الفرق بين الفيروس وبرنامج التجسس (Spyware) في سياق الأمان السيبراني؟
   - أ) الفيروس يتعمد سرقة المعلومات، بينما برنامج التجسس يتسبب في تلف البرامج
   - ب) الفيروس يقوم بتصوير الأفلام، بينما برنامج التجسس يقوم بالتنصت على المكالمات
   - ج) لا يوجد فرق بينهما
5. ما هو الاختراق الأخلاقي(Ethical Hacking) ؟

- أ) هجوم غير قانوني على الأنظمة
- ب) استخدام القرصنة في الهجمات السيبرانية
- ج) استخدام مهارات القرصنة بشكل قانوني لاختبار الأمان السيبراني

6. ما هي أحد أساليب الهجوم السيبراني التي تستند إلى اختبار النظام والبحث عن ثغراته؟

- أ) الهجمات بالبريد الإلكتروني
- ب) الهجمات بالهندسة الاجتماعية
- ج) الاختراق الأخلاقي

7. ما هو الهجوم بالتصيُّد(Phishing Attack) ؟

- أ) هجوم يستهدف البيانات الحساسة عبر إرسال رسائل طلب الصداقة على وسائل التواصل الاجتماعي
- ب) هجوم يستهدف البيانات الحساسة عبر القرصنة
- ج) هجوم يستهدف البيانات الحساسة عبر التلاعب بالمستخدمين للوصول إلى معلوماتهم

8. ما هو التصيُّد الهجين(Spear Phishing) ؟

- أ) نوع من أنواع الصيد الرياضي
- ب) هجوم يستهدف مجموعات كبيرة من الأفراد
- ج) هجوم يستهدف أفراد أو مؤسسات محددة بشكل مستهدف

9. ما هو البرنامج الضار(Malware) ؟

- أ) برنامج يزيد من أداء الحواسوب
- ب) برنامج يتسبب في الأضرار للأنظمة أو يسرق المعلومات
- ج) برنامج يستخدم في تحرير الصور

10. ما هي واحدة من الأساليب الرئيسية لزيادة الدراية الأمنية لدى الموظفين في مؤسسة؟

- أ) تجربة القرصنة
- ب) التدريب وورش العمل
- ج) الاستفادة من البرمجيات الضارة

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: الدراية الأمنية هي معرفة الموظفين بأمور الأمان السيبراني والتهديدات الحالية.
2. صحيح أو خطأ: رصد التهديدات السيبرانية يتضمن مراقبة الأنشطة السيبرانية للتحقق من وجود هجمات.
3. صحيح أو خطأ: الفيروس وبرنامج التجسس هما نفس الشيء.
4. صحيح أو خطأ: الهجوم بالتصيُّد هو هجوم يستخدم الصفحات الويب المزيفة للوصول إلى معلومات المستخدمين.
5. صحيح أو خطأ: الهجوم بالتصيُّد يستهدف عادة الأفراد بدلاً من المؤسسات.
6. صحيح أو خطأ: الاختراق الأخلاقي يتعامل مع اختبار الأمان السيبراني بشكل قانوني وموافقة مسبقة.
7. صحيح أو خطأ: البرنامج الضار هو برنامج مصمم لتحسين أداء الحواسوب.
8. صحيح أو خطأ: البريد الإلكتروني المزيف هو مثال على هجوم بالتصيُّد.
9. صحيح أو خطأ: الهجمات السيبرانية لا تهدد الأمان السيبراني للأفراد.
10. صحيح أو خطأ: التدريب وورش العمل هي وسيلة فعالة لزيادة الدراية الأمنية لدى الموظفين.

الوحدة التدريبية التاسعة

إكتشاف الحوادث السيبرانية والإستجابة لها

الوحدة التاسعة : إكتشاف الحوادث السيبرانية والإستجابة لها

الجدارة:

يتمكن المتدرب من إكتشاف الحوادث السيبرانية والإستجابة لها.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- الحوادث السيبرانية.

الوقت المتوقع للتدريب:

9 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب كيفية إكتشاف الحوادث السيبرانية والإستجابة لها.

إكتشاف الحوادث السيبرانية والإستجابة لها

في مجال أمن المعلومات، تُشير مصطلح "الحوادث" إلى أي حدث ضار يحدث في نظام المعلومات أو الشبكة، والذي يمكن أن يمثل تهديدًا لأحد أهداف أمان المعلومات الثلاثة: السرية والسلامة والتوفر. وبناءً على ذلك، يعتمد نجاح المنظمة في حماية أنظمتها على قدرة فريق الاستجابة للحوادث على تحليل هذه الحوادث المحتملة واتخاذ التدابير الوقائية المناسبة. ومن المؤسف أن العديد من المنظمات لا تدرك أهمية هذا الجانب حتى تحدث كوارث أمنية. لهذا السبب، تعتبر استراتيجية استجابة للحوادث وإدارتها واحدة من العناصر الأساسية في إدارة أمان المعلومات لاكتشاف ومنع الأضرار الناتجة عن هجمات السيبرانية.

أثناء مراحل دورة حياة الهجوم السيبراني، يمكن أن يلعب الكشف المبكر عن الحوادث دورًا مهمًا في تقليل تأثير الهجمات السيبرانية. وتساعد عملية استجابة الحوادث في تحديد المخاطر والتهديدات ونقاط الضعف التي يجب معالجتها لضمان استمرارية العمليات بأمان وكفاءة. يجب أن يُؤخذ في الاعتبار أن الحوادث الأمنية الحرجة يمكن أن تتسبب في خسائر مالية كبيرة وتعرض المؤسسات لعقوبات تشريعية. على سبيل المثال، يمكن للمؤسسات أن تتعرض لعقوبات وفقًا لقوانين الرعاية الصحية (HIPAA) نتيجة لتسرب معلومات الرعاية الصحية.

موسى, ب. ح., & بوسي حمدي. (2023). العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة الدور المعدل لسمات منشأة المحاسبة والمراجعة: دراسة تجريبية. مجلة البحوث المحاسبية, 10(3), 387-458.

يتوقف تصنيف الحوادث الأمنية على مستوى الأضرار التي يمكن أن تسببها التهديدات والاختراقات. ويعتمد تحديد الاستجابة الملائمة للحوادث على فهم أنواع الهجمات والمخاطر المحتملة التي تواجه المنظمة. ويُشدد على أن هناك اختلافًا كبيرًا بين الأحداث (Events) والحوادث الأمنية (Incidents) داخل نظام المعلومات. حيث تمثل الأحداث (Events) أي حدث أو إشعار يمكن رصده في نظام المعلومات، مثل إشعارات البريد الإلكتروني ومحاولات الاتصال بالخوادم وتسجيل المستخدمين في النظام. بينما تمثل الحوادث الأمنية (Incidents) الأحداث الضارة في نظام المعلومات التي تسبب أضرارًا مباشرة أو تمثل محاولة لتسبب الأذى، مثل محاولات غير مصرح بها للوصول إلى النظام والبرمجيات الخبيثة وهجمات حجب الخدمة والوصول غير المصرح به. وعادةً ما يتم تصنيف الحوادث إلى أربع فئات رئيسية استنادًا إلى مستوى تأثيرها وهي: حوادث حرجة وعالية ومتوسطة ومنخفضة.

في مجال أمن المعلومات، يُشير مصطلح "استجابة الحوادث" إلى العمليات والإجراءات التي تهدف إلى استعادة البيئة التشغيلية الطبيعية في منظمة ما بعد حدوث حادث أمني. يتألف عملية استجابة الحوادث من ست خطوات رئيسية، تبدأ بالإعداد المستمر وتنتهي بالتعلم من التجارب السابقة.

1. **مرحلة الإعداد :**تمثل هذه المرحلة الأساسية في تأهيل الفريق والمنظمة للتعامل مع الحوادث المحتملة. يتضمن ذلك تطوير السياسات والقوانين واللوائح المناسبة، والتنسيق مع مزودي الخدمات الخارجية، وإنشاء نظام لتتبع الحوادث. تشمل أعضاء الفريق في هذه المرحلة مجموعة متنوعة من التخصصات مثل أعضاء فريق الاستجابة للحوادث والاتصالات والبيانات والبرامج والأجهزة والوثائق والتقارير. في هذه المرحلة، يتم تدريب الفريق وتزويده بالأدوات والنظم اللازمة.
2. **مرحلة الاكتشاف :**تعني هذه المرحلة الإعلان عن وقوع الحادث وتحديد طبيعته، سواء كان حادثًا أمنيًا أو غير ذلك. يجب أن يكون الاكتشاف شاملًا على مستوى المستخدمين والأنظمة والشبكات وفقًا لهيكلية المنظمة. يشمل الاكتشاف العديد من الجوانب مثل رصد العمليات والخدمات والملفات وأداء

الشبكة والمهام المجدولة والحسابات. يجب على فريق الاستجابة للحوادث أن يكون على علم بـأنواع مختلفـة من الحوادث الأمنيـة وأن يتمكن من تحـديـد التهديدات والمخاطر بشـكل سـريع للبدء في التدابير الاسـتجابة. في نـهاية هذه المرحلة، يتم جمع الأدلة والاحتفاظ بها لاستخدامها في التحقيقات المستقبلية.

3. **مرحلة الاحتواء :**تتضـــمن هذه المرحلة احتواء الحادث ومنع تفاقمه. يتعين على الفريق اتخاذ التدابير اللازمة لمنع انتشـــار الهجوم أو التهديد إلى مناطق أخرى من البيئة التشـغيلية. هذا يشـمل عزل المصـادر المشـتبه بها وإجراءات لإزالة البرمجيات الخبيثة وتصحيح الثغرات الأمنية.
4. **مرحلة الاستئصال :**هذه المرحلة تتعامل مع إزالة التهديد واستعادة النظام إلى حالته الأصـلية. يتضـمن ذلك تنظيف النظام من البرمجيات الضـارة وتصـحيح الثغرات الأمنية واستعادة البيانات المتضررة إلى حالتها الطبيعية.
5. **مرحلة الاسـتعادة :**تهدف هذه المرحلة إلى اسـتعادة البيئة التشـغيلية الطبيعية واســـتئناف العمليات الأســـاســـية. يجب أن يتم اختبار الأنظمة والتأكد من استقرارها قبل استئناف الأنشطة العادية.
6. **مرحلة الدروس المســتفادة :**يتم في هذه المرحلة تقييم أداء فريق الاســتجابة للحوادث والحادث نفسـه واسـتخلاص الدروس المسـتفادة. يتم تحليل ما حدث وتحديد التحســينات الممكنة لتعزيز اســتعداد المنظمة لمواجهة الحوادث المستقبلية.

في مجال أمن المعلومات، يلعب فريق الاســتجابة للحوادث (IRT) دورًا بارزًا في تقدير حجم الأضـــرار الناتجة عن الحوادث الأمنية. يعمل هذا الفريق على مدار السـاعة لتحديد الهجمات ذات الأولوية العالية داخل المنظمة المتأثرة ويسـعى جاهدًا لتقديم حلاً وقائيًا لمنع وقوع أضرار كبيرة في الحاضر والمستقبل. دور IRT يتمثل بشكل رئيسي في تنفيذ التعليمات خطوة بخطوة للاستجابة للهجمات السيبرانية، ويقدم أعضـــاء هذا الفريق خدمات داعمة فيما يتعلق بالمعلومات والمتطلبات العامة. يجب أن يتكون فريق الاسـتجابة للحوادث من مجموعة متنوعة من التخصـصـات بما في ذلك أعضـاء من قسـم أمن المعلومات، وفريق الشـبكة، ومسـؤولي النظام، ومكتب الخدمات، والقسم القانوني، والموارد البشرية والعلاقة العامة.

لتنفيذ مهامه بفعالية، يستخدم فريق الاستجابة للحوادث مجموعة من الأدوات والتقنيات للتعامل مع مشكلات أمان المعلومات الناشئة عن الهجمات. تلك الأدوات تسهم في الحفاظ على البيانات ضمن حدود الاستخدام المخصصة لها وتلعب دورًا حاسمًا في تحقيق الأمان. يجب أن تكون هذه الأدوات سهلة الوصول وجاهزة للاستخدام الفوري، وغالبًا ما يتم تجميعها في مجموعة معروفة بمصطلح "حقيبة الاستجابة السريعة"، والتي تتضمن أدوات لإجراء نسخ احتياطية، وبرامج لتحليل الجرائم الرقمية، وأجهزة تخزين، وأدوات لرصد الشبكة، بالإضافة إلى ملحقات أخرى ذات صلة.

الدور الرئيسي لفريق الاستجابة للحوادث (IRT) هو تعزيز قدرات الأمان الخاصة بالمؤسسة وحماية سرية المعلومات ونزاهتها وتوافر أنظمتها. واستجابة الحوادث تظل الخيار الأمثل للمنظمات التي تسعى للحماية ضد الهجمات السيبرانية. يتطلب نجاح هذا الفريق الكثير من التدريب والتجارب لأعضائه. عند وقوع حادث، تتمثل الأولوية الرئيسية للمنظمة في منع أي فقدان للبيانات. ولهذا الغرض، يجب تطوير نظم احتياطية فعالة وقوية، وعادة ما تكون خارج نطاق البيئة التشغيلية الرئيسية للمؤسسة. توفير بنية تحتية للنسخ الاحتياطي تجمع بين الأمان والتوفر يعد عنصرًا أساسيًا. وبصفة عامة، يمكن للشركات أن تبني مرافق النسخ الاحتياطي الخاصة بها بعيدًا عن مرافق الإنتاج الرئيسية. يمكن أن تتمثل هذه المرافق في شبكات افتراضية خاصة تسمح بالحفاظ على البيانات داخل مباني المنظمة وفي نطاق منفصل.

موسى, ب. ح., & بوسي حمدي. (2023). العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة الدور المعدل لسمات منشأة المحاسبة والمراجعة: دراسة تجريبية. مجلة البحوث المحاسبية, 10(3), 387-458.

تدريبات

أسئلة اختيار من متعدد:

1. ما هو الهدف الرئيسي لعملية اكتشاف الحوادث السيبرانية؟
   - أ) منع حدوث أي هجمات سيبرانية
   - ب) اكتشاف وتحليل الحوادث والاختراقات السيبرانية
   - ج) زيادة سرعة الاتصال بالإنترنت
2. ما هو تعريف التحقق من الأمان (Security Verification) في سياق اكتشاف الحوادث السيبرانية؟
   - أ) التأكد من أن الشبكة غير متصلة بالإنترنت
   - ب) التحقق من أن الأجهزة والنظم محمية بكلمات مرور قوية
   - ج) التحقق من أن تنفيذ الأمان يتم بشكل صحيح وفقًا للمعايير
3. ما هو دور تحليل سجلات الحوادث (Incident Logs) في عملية اكتشاف الحوادث السيبرانية؟
   - أ) تخزين المعلومات السرية
   - ب) تسجيل ومراقبة الأحداث والأنشطة على النظام
   - ج) توليد كلمات مرور جديدة
4. ما هو التحليل التنبؤي للحوادث(Predictive Incident Analysis) ؟
   - أ) تنبؤ حدوث الزلازل
   - ب) تقدير متى ستحدث هجمات سيبرانية مستقبلية
   - ج) تقدير متى ستحدث الهجمات الإرهابية
5. ما هو الهدف الرئيسي لاستجابة الحادث السيبراني (Incident Response)؟

- أ) تجنب الإبلاغ عن الهجوم للسلطات
- ب) استعادة الأمان والوظائف الطبيعية للنظام
- ج) تصفيف الشبكة

6. ما هو دور فريق الاستجابة للحوادث السيبرانية (Incident Response Team)؟

- أ) تنظيم الفعاليات الاجتماعية
- ب) اكتشاف الثغرات في الشبكة
- ج) الاستجابة للحوادث السيبرانية وإدارتها

7. ما هو الهجوم بالامتناع عن الخدمة (DoS) في سياق الحوادث السيبرانية؟

- أ) هجوم يستهدف اختراق البيانات الحساسة
- ب) هجوم يهدف إلى تعطيل خدمة النظام أو الموقع
- ج) هجوم يستهدف التجسس على المكالمات الهاتفية

8. ما هو التحليل الاستباقي (Proactive Analysis) في سياق اكتشاف الحوادث السيبرانية؟

- أ) التحليل الذي يأتي بعد حدوث الهجمة
- ب) التحليل الذي يستخدم للتنبؤ بالهجمات المستقبلية
- ج) التحليل الذي يهدف لاستعادة البيانات المفقودة

9. ما هو الهجوم بالامتثال(Compliance Attack) ؟

- أ) هجوم يستهدف انتهاك قوانين الأمان السيبراني
- ب) هجوم يهدف إلى تشجيع الموظفين على الامتناع عن العمل
- ج) هجوم يستهدف تنظيم الفعاليات الرياضية

10. ما هو الهجوم بالتصـيُّد (Phishing Attack) في سـياق اكتشـاف الحوادث السيبرانية؟

- أ) هجوم يهدف إلى استخراج البيانات من الشبكة
- ب) هجوم يهدف إلى سـرقة البيانات الحسـاسـة عبر رسـائل طلب الصداقة
- ج) هجوم يستهدف تشويه صورة الشركة

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: الهدف الرئيسي لاكتشاف الحوادث السيبرانية هو منع حدوث الهجمات.
2. صحيح أو خطأ: تحليل سجلات الحوادث يعتمد على تسجيل ومراقبة الأحداث والأنشطة على النظام.
3. صـحيح أو خطأ: التحليل التنبؤي للحوادث يهدف إلى تنبؤ متى سـتحدث الهجمات السيبرانية المستقبلية.
4. صـحيح أو خطأ: اسـتجابة الحادث السـيبراني تهدف إلى اسـتعادة الأمان والوظائف الطبيعية للنظام.
5. صـحيح أو خطأ: فريق الاسـتجابة للحوادث السـيبرانية يدير الفعاليات الاجتماعية في المؤسسة.
6. صـحيح أو خطأ: الهجوم بالامتناع عن الخدمة (DoS) يهدف إلى تعطيل خدمة النظام أو الموقع.
7. صحيح أو خطأ: التحليل الاستباقي يأتي بعد حدوث الهجوم ويستخدم لتحليل أثره.
8. صـحيح أو خطأ: الهجوم بالامتثال (Compliance Attack) يسـتهدف انتهاك قوانين الأمان السيبراني.

9. صحيح أو خطأ: الهجوم بالتصيُّد (Phishing Attack) يهدف إلى سرقة البيانات الحساسة عبر رسائل طلب الصداقة.
10. صحيح أو خطأ: اكتشاف الحوادث السيبرانية يتعامل فقط مع الهجمات التي تمت على مستوى البرمجيات.

الوحدة التدريبية العاشرة

التقنيات والحلول المستخدمة في الأمن السيبراني

الوحدة العاشرة : التقنيات والحلول المستخدمة في الأمن السيبراني

الجدارة:

يتمكن المتدرب من التقنيات والحلول المستخدمة في الأمن السيبراني.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- التقنيات والحلول المستخدمة في الأمن السيبراني

الوقت المتوقع للتدريب:

9 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب التقنيات والحلول المستخدمة في الأمن السيبراني.

التقنيات والحلول المستخدمة في الأمن السيبراني

تقنيات وحلول الأمان السـيبراني هي مجموعة من الأدوات والتقنيات والممارسـات التي تهدف إلى حماية الأنظمة والبيانات الرقمية من التهديدات السـيبرانية والهجمات الإلكترونية. هذه التقنيات والحلول تشـمل مجموعة متنوعة من الأسـاليب والتقنيات المتقدمة التي تستخدم للكشف عن التهديدات والتحقق منها والوقاية منها والاستجابة إليها. إليك بعض التقنيات والحلول المستخدمة في مجال الأمان السيبراني:

1. **جدران الحماية (Firewalls):** تعتبر جدران الحماية من أدوات الأمان الأساسية، حيث تسمح بفصل الشبكة الداخلية عن الشبكة الخارجية ومراقبة حركة حركة البيانات ومراقبة الوصول إلى النظام.
2. **أنظمة الكشف عن التسلل - Intrusion Detection Systems) (IDS وأنظمة الوقاية من التسلل Intrusion Prevention) (Systems - IPS:** تعمل هذه الأنظمة على رصد وتحليل حركة الشبكة للكشف عن محاولات التسلل والهجمات، وفي بعض الحالات يمكنها الاستجابة الفورية لمنع هذه المحاولات.
3. **أنظمة إدارة السجلات والمراقبة Security Information) - SIEM) and Event Management):** تستخدم لجمع وتحليل ومراقبة السجلات والأحداث من أنظمة متعددة بهدف كشف الأنشطة غير المعتادة وتحديد التهديدات السيبرانية.

4. **أنظمة الكشف عن البرامج الضارة-(Antivirus and Anti-Malware):** تستخدم للكشف وإزالة البرامج الضارة والفيروسات من الأنظمة والأجهزة.

5. **التشفير :(Encryption)** يتم استخدام التشفير لحماية البيانات من الوصول غير المصرح به عن طريق تحويلها إلى صيغة غير قابلة للقراءة إلا بوجود مفتاح فك التشفير.

6. **إدارة الهوية والوصول (Identity and Access Management - IAM):** تتيح للمؤسسات التحكم في منح الوصول إلى الأنظمة والبيانات على أساس الهوية والصلاحيات، وتتضمن أيضًا التعرف على الهوية مثل الاعتمادات المزدوجة.(Two-Factor Authentication)

7. **جهاز التوجيه الآمن :(Secure Gateways)** يتيح للمستخدمين الاتصال بالشبكة بطريقة آمنة عبر شبكة عامة مثل الإنترنت، ويستخدم في إقامة اتصالات آمنة عن بعد.

8. **أمان التطبيقات :(Application Security)** تقنيات وأدوات لاختبار وتصحيح الثغرات الأمنية في تطبيقات الويب والبرمجيات.

9. **حواجز التفتيش :(Web Application Firewalls - WAFs)** تعمل على حماية تطبيقات الويب من الهجمات مثل حقن SQL والهجمات العبر المواقع.

10. **التدقيق والمراجعة الأمنية (Security Auditing and Review):** عمليات تدقيق ومراجعة دورية للأنظمة والشبكات للتحقق من تطبيق معايير الأمان والامتثال للمتطلبات القانونية والتنظيمية.

11. **الوعي الأمني والتدريب (Security Awareness and Training):** توجيه الموظفين والمستخدمين لفهم التهديدات السيبرانية والممارسات الأمنية الجيدة.

12. **الاستجابة للحوادث :(Incident Response)** تطوير وتنفيذ خطط استجابة للتعامل مع الحوادث الأمنية عند وقوعها.

13. **التحليل التنبؤي (Threat Intelligence):** استخدام المعلومات المتاحة عن التهديدات السيبرانية لفهم وتحليل أنماط الهجمات المحتملة.

14. **الحماية من تسرب البيانات - Data Loss Prevention (DLP):** تطبيق سياسات وتقنيات لمنع تسرب البيانات الحساسة خارج الشبكة.

15. **تحليل سلوك المستخدمين - User Behavior Analytics (UBA):** مراقبة سلوك المستخدمين للكشف عن أنشطة غير عادية أو مشبوهة.

هذه مجرد نظرة عامة على بعض التقنيات والحلول في مجال الأمان السيبراني، وتتطور هذا المجال باستمرار لمواجهة التهديدات الجديدة والمتطورة. تختلف احتياجات الأمان من مؤسسة لأخرى، وبالتالي يجب تنفيذ استراتيجيات وحلول مخصصة تتناسب مع تلك الاحتياجات والتهديدات الخاصة بكل منظمة

. أساليب وتقنيات الهجوم والاختراق السيبراني:

1. سرقة المعلومات:

- تُستخدم الهجمات عبر البريد الإلكتروني لسرقة المعلومات. يتم ذلك عن طريق إرسال رسائل إلكترونية تحت مظهر موثوق به بهدف الحصول على معلومات حساسة. هذا النوع من الهجمات أصبح شائعًا بشكل متزايد.

2. برامج الفدية:

- تعتبر برامج الفدية واحدة من أخطر التقنيات. يتم تصميم هذه البرامج لابتزاز المال من خلال اختراق البيانات والأنظمة وتشفيرها. يتم منع الوصول إلى البيانات إلا بدفع فدية، ولكن ليس هناك ضمان بأن البيانات ستُستعيد حتى بعد دفع الفدية.

3. الهندسة الاجتماعية:

- تمثل الهندسة الاجتماعية أحد أساليب الاختراق حيث يتم إغراء الأفراد بالنقر على روابط ضارة أو تنزيل تطبيقات ضارة. هذا يؤدي إلى اختراق الأنظمة والوصول غير المصرح به إلى البيانات. عادةً ما يتم استخدام استراتيجيات تلاعبية لإقناع الأفراد بالقيام بالإجراءات الضارة.

هذه هي بعض التقنيات والأساليب الشائعة المستخدمة في الهجمات والاختراقات السيبرانية. تُظهر هذه الأمثلة التنوع والتطور الذي يشهده مجال الأمان السيبراني، مما يجعل من الضروري تبني استراتيجيات دفاعية فعالة لحماية البيانات والأنظمة من هذه التهديدات.

أهم تقنيات الأمن السيبراني:

جميع الأنظمة والشبكات في العالم معرضة للهجمات السيبرانية من قبل القراصنة المحترفين والهجمات الإلكترونية. لذلك، يجب اتخاذ تدابير لمكافحة العمليات الاختراقية السيبرانية وحماية البيانات والأنظمة والشبكات.

الخطر الأكبر للشـــركات ليس فقط من الجهات الفاعلة، ولكن أيضًـــا من الجهات الداعمة لهم التي تستهدف شركات ومؤسسات معينة. لذلك، يجب تعزيز نظام الأمان السيبراني للمؤسسات وزيادة القدرة الأمنية السيبرانية في الشركات. ويتطلب الأمر فهمًا عميقًا في مجال الأمان السيبراني لحماية الشبكات والبيانات.

فيما يلي بعض الأدوات والتقنيات المهمة في مجال الأمان السيبراني:

1. **برامج مكافحة البرمجيات الخبيثة:**

- تســاعد في التعرف على البرامج الضــارة مثل الفيروســات وبرامج التجسـس ومكافحتها. تقلل من الضـرر الناتج عن الهجمات السـيبرانية وتقوي الأمان.

2. **تقييد الوصول:**

- يقتصـر الوصـول إلى الشـبكة والموارد على المسـتخدمين المخوَّل لهم فقط. يساعد في تقليل مخاطر الوصول غير المصرح به.

3. **تقنية) DLP منع تسريب البيانات:(**

- تســاعد في حماية البيانات الحســاســة والتحكم في اســتخدامها بشــكل صحيح، وتجنب التسريبات غير المصرح بها.

4. **أمان نقطة النهاية:**

- يهدف إلى حماية أجهزة الحاسوب الشخصية والأجهزة المستخدمة في العمل من هجمات الاختراق.

5. **أنظمة منع التطفل:**

- تراقب حركة مرور الشـبكة وتتعرف على أنواع الهجمات السـيبرانية وتحاول منعها وصدها.

6. **أمان الويب:**

- يعزز الأمان على الويب ويمنع اســتغلال صــفحات الويب كوســيلة للاختراق.

تلك هي بعض التقنيات والأدوات الرئيسية في مجال الأمان السيبراني. يجب استخدام هذه التقنيات بشكل مناسب وتخصيص استراتيجيات أمان ملائمة للمؤسسة لضمان الحماية من التهديدات السيبرانية.

جمال الدين, ه. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية, 24(1), 189-230.

تدريبات

أسئلة اختيار من متعدد:

1. ما هي التقنية التي تستخدم لتحليل سلوك المستخدمين والكشف عن أنشطة غير معتادة في الأمان السيبراني؟
   - أ) التشفير
   - ب) تقنيةDLP
   - ج) تحليل السلوك
2. ما هو تقنية جدار الحماية (Firewall) في الأمن السيبراني؟
   - أ) تقنية تمنع الهجمات على الأنظمة بواسطة الأجهزة
   - ب) تقنية تشفير البيانات
   - ج) تقنية لحماية البريد الإلكتروني فقط
3. ما هي التقنية التي تعتمد على تحليل مرور الشبكة ومراقبته للكشف عن الهجمات السيبرانية؟
   - أ) تقنية الحماية من الفيروسات
   - ب) تقنية أنظمة منع التطفل
   - ج) تقنية استخدام الويب
4. ما هو الهدف الرئيسي لتقنية VPN (Virtual Private Network) في الأمن السيبراني؟
   - أ) تشفير الاتصالات لحماية البيانات
   - ب) توليد كلمات مرور قوية
   - ج) منع الهجمات على الأنظمة

5. ما هي التقنية التي تساعد في تحديد هويات المستخدمين والتحقق منها بواسطة كلمات المرور وأمور أخرى؟
   - أ) تقنية التشفير
   - ب) تقنية تقييد الوصول
   - ج) تقنية التصريح
6. ما هو التوجيه الآمن (Secure Routing) في الأمن السيبراني؟
   - أ) توجيه حركة المرور بسرعة أكبر
   - ب) تقنية توجيه حركة المرور بأمان ومنع التلاعب بها
   - ج) توجيه حركة المرور دون الحاجة لأي تدخل أمان
7. ما هي التقنية التي تعتمد على إعداد سجلات مفصلة للأحداث والأنشطة على النظام وتستخدم لمراقبة واكتشاف الهجمات؟
   - أ) تقنية جدار الحماية
   - ب) تقنية تحليل سجلات الحوادث
   - ج) تقنية تشفير البيانات
8. ما هو تقنية التوثيق (Authentication) في الأمن السيبراني؟
   - أ) تحليل البيانات
   - ب (التحقق من هوية المستخدم وصحة اعتماده
   - ج) تشفير الاتصالات
9. ما هو التحليل السلوكي (Behavioral Analysis) في الأمن السيبراني؟
   - أ) تحليل هويات المستخدمين
   - ب) تحليل سلوك المستخدمين والكشف عن أنشطة غير معتادة
   - ج) تحليل البيانات الكبيرة

10. ما هو الفحص الضوئي (Port Scanning) في الأمن السيبراني؟

- أ) تقنية لاختراق الأجهزة الأخرى
- ب) تقنية لفحص واكتشاف الثغرات والمنافذ المفتوحة في الشبكة
- ج) تقنية لمراقبة حركة المرور على الشبكة

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: تقنية VPN تهدف إلى تشفير الاتصالات لحماية البيانات.
2. صحيح أو خطأ: جدار الحماية هو تقنية تستخدم لتحليل سلوك المستخدمين.
3. صـــــحيح أو خطأ: التوجيه الآمن يهدف إلى توجيه حركة المرور بأمان ومنع التلاعب بها.
4. صحيح أو خطأ: تقنية التوثيق تتعامل مع التحقق من هوية المستخدمين وصحة اعتمادهم.
5. صحيح أو خطأ: التحليل السلوكي يركز على تحليل البيانات الكبيرة للشبكة.

الوحدة التدريبية الحادية عشر

الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني

الوحدة الحادية عشر : الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني

الجدارة:

يتمكن المتدرب من الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني.

الأهداف:

عندما تكمل هذه الوحدة يكون لديك القدرة بإذن الله على:

- الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني.

الوقت المتوقع للتدريب:

9 ساعات.

الوسائل المساعدة:

- حاسب آلي
- آلة حاسبة
- جهاز لعرض البيانات(Data show)

متطلبات الجدارة:

اجتياز الطالب الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني.

الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني\

أولاً- الهندسة الاجتماعية

استعرضت بعض الدراسات والأبحاث موضوع الهندسة الاجتماعية كعلم يتعرض إلى بيان كيفية تأثيره على عقول البشـــر وتغير بعض المفاهيم لديهم والتغرير بهم من خلال استخدام أدوات ووسائل عدة.

و تم تعريفها من قبل البعض تعريفا اجتماعياً وتعريفاً أمنياً كالتالي:

–اجتماعياً:

تُعرف الهندســـة الاجتماعية اجتماعياً على أنها التأثير على مُجمل الســـلوك الاجتماعي، ونمط الحياة والتفكير للمُجتمع برمته، حيث يســعى المُهندس الاجتماعي في هذه الحالة إلى تغيير ســلوك الأفراد وطريقة تصــرفهم، وأســلوب تفكيرهم، من اجل الوصـــول إلى الهدف الذي يرنو إليه، من خلال اســتخدام المعرفة المُكتســبة، والمعلومات التي يتم جمعها خلال أســـاليب الهندســـة الاجتماعية مثل تواريخ ميلاد مؤســســي المؤســســة، أو المُناســبات التي يتم نشــرها وتدوالها من قبل الأفراد الذين يســتخدمون وســائل التواصــل الاجتماعي، بالإضــافة إلى هجمات مثل تخمين كلمة المرور لتحقيق غرض مُحدد ومُسبق.

وتعتمد جهود الهندسة الاجتماعية في هذه الحالة على الأساليب العلمية المُتعارف عليها في تجميع البيانات، وتحليلها، والوصول الى إستنتاجات مُحددة والخروج بتوصيات واضحة قابلة للتنفيذ والتطبيق العلمي. (الاتحاد ، 2013)

-أمنيا:

يُشير مُصطلح الهندسة الاجتماعية أمنياً إلى التأثير على الآخرين، والتلاعب بهم لغرض دفعهم للكشف عن معلومات شخصية، ومثل هذا الاستخدام للهندسة الاجتماعية يندرج تحت ما يعرف بخدعة أو حيلة الثقة، بمعنى اكتساب ثقة الطرف الآخر، ثم خداعه والتحايل عليه، للحصول على بيانات مهمة للنصب عليه، أو لغرض اختراق أجهزة الكمبيوتر الشخصية، أو المهنية المُستخدمة في جهات العمل.

و الهندسة الاجتماعية هي: فن الوصول إلى المباني أو الأنظمة، أو البيانات عن طريق استغلال علم النفس البشري بدلاً من اختراق أو استخدام تقنيات القرصنة التقنية(Hulme,2017 & Goodchild) .

و الهندسة الاجتماعية تُعرف أيضا باسم القرصنة البشرية، وهو فن خداع العاملين والمُستهلكين للكشف عن بيانات الاعتماد الخاصة بهم، ومن ثم استخدامها للوصول إلى الشبكات أو الحسابات.

تصعب حماية الأنظمة من المُتسللين وعمليات قرصنة (هاكر) ، وعلى ما يبدو أنه يُمكن بسهولة اختراق الناس اي كان مكانهم، مما يجعلهم ووظائف وسائل الإعلام الاجتماعية أهدافا معرضة للخطر). (من خلال مواقع الويب أو بالنقر على الروابط الضارة أو تحميل وتثبيت التطبيقات الخبيثة(Conteh &. Schmick,2016) .(

والهندسة الاجتماعية هي فن استخراج معلومات سرية عن طريق التلاعب النفسي، وهي هجوم استراتيجي يعتمد على التفاعل البشري، ونظام احتيال معقد، وخداع الأفراد في إعطاء المعلومات الخاصة بهم ككلمة المرور. ويفضل المُجرمون استغلال ثقة الناس بدلاً من التكنولوجيا، حيث أنه من الأسهل استغلال البشر للميل الطبيعي إلى الثقة، مما يؤدي إلى نقص الوعي لمثل هذه الجرائم، ناهيك عن أن الهندسة الاجتماعية تم التغاضي عنها ولا تُعامل على أنها تشكل تهديدا كبير(Jain& others,2016) .

أما المُهندس الاجتماعي فإنه يعيش بقدرته على التعامل مع الناس في القيام بالأشياء التي تُســـاعده على تحقيق هدفه، ولكن النجاح في هذا الأمر يتطلب غالباً قدرا كبيرا من المعرفة والمهارة في التعامل مع أنظمة الكمبيوتر وشـــبكات الهاتف، لذلك فإن المهندس الاجتماعي قادر على الاســـتفادة من الناس للحصـــول على المعلومات باستخدام التكنولوجيا أو بدونها(MITNICK &. Simon,2015) .

ثانياً- كيف تعمل الهندسة الاجتماعية

يقوم عمل الهندسة الاجتماعية على ما يلي(Kontio,2016) :

- جمع المعلومات : وهذه هي المرحلة الأولى، من أجل الحصول على معلومات أكثر عن الضـــحية المقصـــودة، ويتم جمع المعلومات من مواقع الشـــركة، ومنشـــورات أخرى وأحيانًا عن طريق التحدث إلى مُســـتخدمي النظام المُستهدف، (التواصل معهم).
- خطة الهجوم: يحدد المهاجمون كيفية تنفيذ الهجوم، وما هي الأدوات والوسائل التي يمكن استخدامها في الهجوم.
- أدوات الاستحواذ : تتضمن برامج الكمبيوتر التي سيستخدمها المُهاجم عند بدء الهجوم.
- الهجوم : استغلال نقاط الضعف في النظام المُستهدف، أو الأفراد.
- استخدام المعرفة المُكستبة : وذلك من خلال المعلومات التي تم تحصيلها من الأفراد أو المؤسسات.

ثالثاً- أقسام الهندسة الاجتماعية

تُصنف الهندسة الاجتماعية إلى صنفين :

1.الهندسة القائمة على أساس بشري أو إنساني.

2.الهندسة القائمة على أساس تقني :وهي البرامج والتقنيات التي تُساعد الأشخاص الذين يسعون للحصول على المعلومات وبث الإشاعات للوصول إلى المعلومة التي يريدون استغلالها ومن أمثلة ذلك:

-الاحتيال الإلكتروني(phishing)

الاحتيال الالكتروني: هو محاولة الحصول على معلومات حساسة، مثل أسماء المُستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان باستخدام البريد الإلكتروني، ومواقع البيع بالمزاد أو غير ذلك...

-الاحتيال الصوتي(Vising)

يعتمد هذا النوع على برنامج war Dialler)) وهو برنامج يقوم بالاتصال بالعديد من أرقام الهواتف المُختلفة في المنطقة، وبعد الاتصال يقوم الهاكر بانتظار ضحاياه، ويبدأ الخطر من لحظة رفع السماعة والإجابة على الرسالة الآلية التي تخبره أن بطاقته الائتمانية تخضع للسرقة وعمليات احتيالية وطلب رقم البطاقة، وبعض البيانات السرية وحينها يحصل الهاكر على ما يريد.

-الرسائل الاقتحامية المُزعجة(Spam)

يُعتبر استخدام الرسائل الاقتحامية الأسلوب الأكثر شيوعاً، حيث يتم إرسال نفس البريد الإلكتروني لملايين المُستخدمين مع طلب لتعبئة التفاصيل الشخصية، ويتم استخدام هذه التفاصيل من المُحتالين لأنشطتهم غير المشروعة، ومعظم الرسائل تأتي بمُذكرة عاجلة ويُطلب من المُستخدم إدخال بيانات الاعتماد لتحديث معلومات الحساب أو تغيير التفاصيل أو التحقق من الحسابات. وفي بعض الأحيان، قد يطلبوا تعبئة نموذج للوصول إلى خدمة جديدة من خلال رابط يتم توفيره في البريد الإلكتروني.

ـبرامج مُهمة

وهي ما نشـــهده في بعض المواقع من روابط تحميل برامج، ولكنها تكون مدعومة بكلمات إقناعية عن أهمية ذلك البرنامج المُهكر للجهاز والســـارق للمعلومات الحساسة.

رابعاً : لماذا يلجأ مُعظم الهاكر لاستخدام الهندسة الاجتماعية

يقوم الهاكز باستخدام الهندسة الاجتماعية لعدة أسباب منها: (خنين 2013)

ـ سهولة الإعداد والتنفيذ

لقد أصبح من الصعب اختراق النظام واكتشاف ثغراته، وخاصة إذا كان ذلك النظام محميا من قبل أصحابه، إلا أن كل تلك المصاعب تزول إن وجدت شخصا يوصلك لها. وعلاوة على ذلك فإن الهندسة الاجتماعية لا تتطلب كثيرا من الهاكر سوى أن يتحلى بالود وحسن الأسلوب والثقة والتحليل الجيد للضحية؛ ليسهل عليه إقناعها، وهو أمر لا يحتاج إلى تعليم أو تدريب.

ـقله الحماية والوعي لها

تهتم كثير من الشركات وتحرص على الحماية المادية للشركة، سواء ما يتعلق بالأقفال والأمن البشـــري وتدريب موظفيها، وفي المقابل ربما تجهل كثيراً عن الحماية من الهندسة الاجتماعية، فتعتقد مُعظم الشركات أن الأمن مسؤولية القسم الخاص بها، ولكنها في الحقيقة على كل موظف مســـؤولية حماية نفســـه وحماية المؤسسة، فالمعلومات التي تبدو صغيرة وغير مهمة، قد تكون نقطة هجوم الهاكر ومفتاحه الرئيسي.

ـصعوبة الكشف والتعقب

تُعتبرجرائم الهندسة الاجتماعية من الجرائم النظيفة التي لا يوجد لها أدلة، أو أجهزة، فهي تعتمد كليا على البشرولذلك نجد أن من الصعب جداً كشفها.

المحور الثاني- الأساليب التي يتم استخدامها في الهندسة الاجتماعية

يُفكر المُهاجمون وبشكل مُستمر بأساليب جديدة لخداع الضحايا ومن أشهر الأساليب المُتبعة في مثل هذا النوع من الاختراق ما يلي:

–الهاتف :أكثر هجمات الهندسة الاجتماعية تقع عن طريق الهاتف، حيث يتصل المهاجم مُدعياً أنه شخص ذو منصب وله صلاحيات، ويقوم تدريجيا بسحب المعلومات من الضحية.

–البحث في المُهملات :حيث توجد الكثير من المعلومات الهامة التي يمكن الحصول عليها من سلة مهملات الشخص أو الضحية.

–الهندسة الاجتماعية :حيث يُمكن أن تكون في أي مكان على شبكة الإنترنت، ويُعرف هذا النوع من هجوم الهندسة الاجتماعية على أنها إعادة نظام الرد الآلي (الرد الصوتي التفاعلي) من خلال الرقم المجاني وخداع الناس بالاتصال برقم الهاتف وإدخال التفاصيل الخاصة بهم((Tiwari,2018 . .

–استغلال الشائعات :أصبحت شبكات التواصل الاجتماعي ومنها فيسبوك مصدراً من مصادر انتشار الشائعات وبشكل سريع جدا، بالتالي باتت المُساهمَ الأكبر في نشر الشائعات بشكل أو بآخر، وهي مصدر تسهيل عمل من ينوي استغلال الشائعات لتغليف روابطهم الخبيثة بها. حيث باتت الشائعات تؤثر وبشكل كبير على العالم الحقيقي، فقد تؤدي بأصحاب القرار لاتخاذ قرارات ربما تكون هامة ومصيرية مبنية على معلومات خاطئة، ما يؤدي لانكشاف مزيد من المعلومات التي يُمكن استغلالها لمزيد من هجمات الهندسة الاجتماعية أو غيرها من الهجمات الخبيثة . (عسكر والعكوز ،2013)

–استغلال عواطف الضحية وطباعه الشخصية :يقصد باستغلال العواطف الشخصية استخدام نصوص أو صور تُخاطب عاطفة الضحية وتؤدي إلى سقوطه في فخ فتح وتشغيل الملف الخبيث أو فتح رابط خبيث، ويمكن أن تكون العواطف عواطف سلبية كالحقد الانتقام والحزن والكره والنقمة أو عواطف إيجابية كالحب والحنين والإعجاب وغيرها. ويمكن أيضا للمهاجم استغلال فضول المُستهدف أو غروره أو بحثه عن علاقة عاطفية ما.

–استغلال المواضيع الساخنة :بشكل مشابه لاستغلال الشائعات، يستغل المُهاجمون المواضيع الساخنة لتمرير عمليات احتيالهم بعكس الشائعات. تنتشر المواضيع الساخنة على وسائل الإعلام ذات المصداقية العالية على شكل أخبار عاجلة عادة بسرعة، وعلى وسائل التواصل الاجتماعي بشكل أسرع، وكل

هذا يجعلها طُعما مناسبا لإيهام الضحية بأن الرابط المرفق مع الرسالة مثلا هو أيضا "وديع"، وأن صـاحب الرابط المرفق "صـادق" في ادعائه حول محتوى الرابط كما الرسالة صادقة في نقل الأخبار الساخنة.

–استغلال موضوع الأمن الرقمي وضعف الخبرة التقنية للضحية :في هذا النوع من الهندسـة الاجتماعية يدعي المُهاجم أن رابطا ما أو ملفا ما سـيُسـهم في حماية جهاز الضـحية، في حين أنه في حقيقة الأمر الملف أو الرابط خبيث، وسـيُسـهم في تدمير الجهاز أو الحصول على معلومات مُعينة.

–انتحال الشـخصـي :يُمكن للمهاجم أن ينشـئ مثلا حسـابا على فيسـبوك، أو بريد إلكتروني، أو حساب سكايب، باسم مُستعار أو باسم مُطابق لاسم صديق لك أو لاسم شـخص تعرفه بنية انتحال الشـخصـية، وهو مثال آخر على الهندسـة الاجتماعية. بهدف الحصـول على كلمة سر لحسـاب شـخص ما في فيسـبوك واسـتغلاله لانتحال شخصيته، ومحاولة الوصول إلى معلومات أكثر((Tiwari,2018 .

–اسـتغلال السُـمعة الجيدة لتطبيقات مُعينة :وهنا يدعي المهاجم أن رابطا أو ملفا هو نفسـه النسـخة المُحدثة مثلا من تطبيق معين، لكنه في الحقيقة يتضـمن ملفا خبيثا، وهناك أيضـا حالات أخرى يقوم فيها الرابط بتحميل الملف الخبيث وتنصـيبه ثم تحميل التطبيق الحميد الحقيقي وتنصـيبه بحيث يعتقد الضـحية أنه قام بتنصـيب التطبيق الحميد.

–التصيد الاحتيالي :وهو النوع الأكثر شيوعاً من هجوم الهندسة الاجتماعية ، حيث يقوم المهاجم بإعادة إنشـاء بوابة موقع على شـبكة الإنترنت أو يحصـل على دعم من شـركة مشـهورة ويرسـل الرابط للضـحايا عبر رسـائل البريد الإلكتروني أو المنابر الإعلامية والاجتماعية((Tiwari,2018 .

المحور الثالث : الحماية من الهندسة الاجتماعية

أولاً : كيف نحمي أنفسنا من الهندسة الاجتماعية ؟

لحماية أنفسنا من الهندسية الاجتماعية، علينا اتباع ما يلي:

- :عدم مُشاركة أي معلومات أو أي بيانات شخصية مع أي جهة كانت، فعلى الرغم من سهولة القيام بهذا الأمر إلا أن الكثير من المستخدمين يغفلون عن هذه النصيحة.
- التحقق دائماً من الأشخاص الذين تتحدث إليهم، سواءً عبر الهاتف أو عبر البريد الإلكتروني أو خدمات التواصل الفوري وغيرها، فمثلاً لو كان المُتصل من شركة رسمية فلا تجد حرجاً أن تطلب منه معلوماته الكاملة وأن يقوم بالاتصال من رقم هاتف رسمي يُمكن التحقق منه. (الجودي ، 2018)
- عدم فتح مُرفقات البريد الإلكتروني من أشخاص غير معروفين، نظرا لكون هذه الطريقة مستعملة على نطاق واسع لنشر البرمجيات الخبيثة، أو الحصول على المعلومات الشخصية، وذلك من خلال انتحال هوية شركات كبرى وإرفاق بعض الملفات في البريد((Tiwari,2018 .
- العمل على تأمين الهاتف الذكي أو الحاسب المحمول، وفلترة البريد المُزعج من خلال الاعتماد على أدوات خاصة، وكذا برامج قوية لمُكافحة الفيروسات ورسائل وصفحات التصيد((Tiwari,2018 .

ثانياً : التدابير الوقائية ضد الهندسية الاجتماعية

من الملاحظ أن مُعدل نجاح الجرائم الحاسوبية يرتفع بشكل مُطرد، وهو أمر راجع إلى زيادة مُستوى الهندسة الاجتماعية، والعروض التي يتم تقديمها من طرف جهات خبيثة. لهذا على الشركات أن تظل مُدركة للتهديد الذي يتربص بها، بحيث تكون قادرة على الاستجابة للهجمات، عبر توفير الضمانات التقنية وغير التقنية التي يُمكن تنفيذها لخفض المخاطر المُرتبطة بالهندسة الاجتماعية إلى مسُتوى مقبول، وهنا تلجأُ بعض شركات (كَحَلٍّ) إلى إضافة طبقات مُتعددة لمُخططاتها الأمنية حتى إذا فشلت الآلية في الطبقة الخارجية، هناك إليه واحدة في الطبقة الداخلية يمكن أن يُساعد في منع تهديد قد يتحول إلى كارثة (التخفيف من حدة المخاطر)، وهذا المفهوم المعروف بالدفاع متُعدد الطبقات أو الدفاع في العمق.

وهذا هيكل يتضمن مزيجاً من التدابير الاحترازية .Conteh &) : Schmick,2016)

– السياسة الأمنية :وهي سياسة مكتوبة بشكل جيد، وينبغي أن تشمل النهج التقني وغير التقني. وينبغي إدماج كل منظمة الأمن في أهدافها التشغيلية.

–التعليم والتدريب :يتعين على الموظفين حضـــور التداريب المطلوب، كما يتعين على المنظمات برمجة دورات تدريبية تنشيطية من حين لآخر.

–توجيه شبكة الاتصال :يجب أن تكون لدى المُنظمة خطة لحماية شبكة الاتصال بمواقع whitelisting وتعطيل التطبيقات غير المُســتخدمة والمنافذ، وعلى مُستخدمي الشبكة الحفاظ على كلمات السر المُعقدة والتي يجب أن تتغير كل 60 يوماً.

–عمليات مُراجعة الحســابات :المُنظمات التي لها نشـــاط عليها التحقق من التقيد بسياسة الأمن، والتي تشمل العناصر الهامة المُتعلقة بأمن الأشخاص والمُنظمة.

المحور الرابع :الاستنتاجات والتوصيات

أولا : الاستنتاجات

بعد أن استعرض الباحث عددا من المحاور التي تتعلق بالهندسة الاجتماعية واختراق عقول البشر، قد توصل إلى الاستنتاجات التالية:

- الهندسة الاجتماعية هي فن الوصول إلى المباني أو الأنظمة، أو البيانات عن طريق استغلال علم النفس البشري، من خلال الإيهام بأمور عدة، أو الإشاعة أو الاستدراج، أو استخدام أساليب الإغراء.
- المُهندس الاجتماعي قادر على الاستفادة من الناس للحصول على المعلومات باستخدام التكنولوجيا أو بدونها.
- وصل عصر المعلومات إلى مرحلة النُضج، مرفوق الزيادة في استخدام شبكة الإنترنت.
- الإنســـانية تتطور ســـريعاً، كما تغذي نمو المعارف العامة الموجودة إلى حد كبير.

- أصـــبح العالم الرقمي، بُنية تحتية مُلائمة لمجموعة كبيرة من الجرائم الجنائية الإلكترونية.
- الناس هم محور سلسلة العدوى في غالبية وأكبر هجمات قراصنة الكمبيوتر.
- تســعى الهندســة الاجتماعية لاســتخدام الإشــاعات كأهم مدخل لها من أجل اقتناص ضحاياها.

ثانيا : التوصيات

بعد أن استعرض الباحث الاستنتاجات المُتعلقة بالدراسة فإنه يوصي بما يلي:

- الســـعي لتعديل القوانيين المُتعلقة بالجرائم الإلكترونية والقرصـــنة، بحيث يتناســـب القانون والفعل المُقترف، وحجم الأضـــرار الناتجة عن ذلك الفعل وأثرها على الضحية
- تكثيف المُبادرات والحملات التي تركز على كيفية اســتخدام التكنولوجيا بكافة أنواعها، حتى لا يقع أي فرد أو مؤسسة في شراك المُتربصين سواء القراصنة (الهاكرز) أو الأشخاص الذين يسعون إلى الحصول على المعلومات بأي ثمن وأي وسيلة.
- التحذير وبشـكل مُسـتمر وبكافة الوسـائل من خطر الإشـاعة وتداولها، كونها تُشكل صيداً سهلا لبعض الذين يبحثون عن استثمارها في تحقيق مصالحهم.
- التركيز على عملية التنشئة الاجتماعية المُتعلقة بتربية وتهذيب الجيل الرقمي، من حيث ثنيهم عن الإدمان على اســـتخدام الأدوات التكنولوجية والرقمية، وقضاء وقت طويل في استخدامها.
- التركيز على أهمية الانغماس بشـكل مُفرط في اسـتخدام التكنولوجيا، وتحويل الاتجاهات الفكرية إلى اســـتغلال الوقت في أنشـــطة ذات انعكاس مُفيد على طلاب المدارس والجامعات.
- تنظيم ورش عمل في المدارس لأولياء الأمور والطلاب، وعرض الأســـاليب المُختلفة التي يتبعها المُهندسون الاجتماعيون سواء من خلال أجهزة الكمبيوتر

أو بشكل شخصي، ويجب التركيز على الأمور التي لا يجب الإفصاح عنها للمهندسين الاجتماعيين، ونوع الضرر الذي يقع على سمعة عائلاتهم ووضعهم المالي.

محمد المري, ر., & راشد. (2023). أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية| The Impact of Information Technology on the Security System and Internal Control. مجلة البحوث الفقهية والقانونية, 40(40), 1303-1373.

تدريبات

أسئلة اختيار من متعدد:

1. ما هو الهدف الرئيسي للهندسة الاجتماعية في مجال الأمن السيبراني؟
   - أ) تشفير البيانات
   - ب) السيطرة على الأجهزة الذكية
   - ج) الحصول على معلومات أو تصرفات من الأفراد
2. أي الخيارات التالية يمثل مثالًا على هندسة اجتماعية؟
   - أ) تشفير الرسائل الإلكترونية
   - ب) تلاعب المهاجمين بالعناصر البشرية للحصول على معلومات
   - ج) استخدام جدران الحماية لحماية البيانات
3. ماذا يشمل دور العنصر البشري في استراتيجيات الأمن السيبراني؟
   - أ) الترميز السري
   - ب) التدريب والتوعية
   - ج) تطوير البرمجيات الخبيثة
4. ما هي واحدة من أساليب الهندسة الاجتماعية؟
   - أ) استخدام البرمجيات المكافحة للفيروسات
   - ب) انتحال هوية شخص موثوق به للوصول إلى معلومات
   - ج) تحليل البيانات الكبيرة
5. ما هي التقنية التي تتيح للمهاجم التنكر والاختباء وراء هويات مزيفة على الإنترنت؟
   - أ) VPN

- ب) الهندسة الاجتماعية
- ج) تقنية التشفير

6. ما هو التوعية بالأمان (Security Awareness) في سياق الأمن السيبراني؟
   - أ) تحليل سجلات الحوادث
   - ب) تعليم الموظفين والأفراد حول مخاطر الأمان
   - ج) استخدام الويب بأمان
7. ما هو الهدف الرئيسي للتوعية بالأمان؟
   - أ) تحسين الأمان فقط دون الحاجة للوعي البشري
   - ب) توجيه الأفراد والموظفين للتصرف بأمان والتعرف على مخاطر الأمان
   - ج) تشفير البيانات بشكل دائم
8. ماذا يشمل التدريب على الوعي بالأمان في الأمن السيبراني؟
   - أ) تدريب على استخدام البرمجيات المكافحة للفيروسات
   - ب) تعليم كيفية القراءة بسرعة
   - ج) توعية الموظفين بأهمية الأمان وكيفية التصرف بأمان
9. ما هو التصيد الاجتماعي (Phishing) في الأمن السيبراني؟
   - أ) تحليل سلوك المستخدمين
   - ب) استخدام تقنيات التشفير لحماية البيانات
   - ج) محاولة احتيال الأفراد عبر رسائل مزيفة للحصول على معلومات شخصية
10. ما هي واحدة من أساليب التوعية بالأمان؟

- أ) تجنب التواصل مع أي شخص غريب عبر الإنترنت
- ب) تعليم الأفراد عن كيفية التحدث بلطف
- ج) تعليم الأفراد كيفية الكشف عن محاولات الاحتيال عبر البريد الإلكتروني

أسئلة صواب أو خطأ:

1. صحيح أو خطأ: الهندسة الاجتماعية تهدف إلى الحصول على معلومات من الأفراد من خلال التلاعب بهم.
2. صحيح أو خطأ: دور العنصر البشري في استراتيجيات الأمن السيبراني يشمل التوعية والتدريب فقط.
3. صحيح أو خطأ: تقنية التصيد الاجتماعي تتضمن محاولات احتيال عبر رسائل مزيفة للحصول على معلومات شخصية.
4. صحيح أو خطأ: التوعية بالأمان تهدف إلى تعزيز الوعي بمخاطر الأمان وكيفية التصرف بأمان.

المراجع

- العتيبي, عبد الرحمن بن بجاد شارع المرشدي, علي, & إبراهيم ميرغني محمد. مشرف. (2020). دور الأمن السيبراني في تحقيق رؤية 2030 (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية).
- سعيد إسماعيل, & محمد. (2022). التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة–دراسة في القانون القطري والمقارن.
- بدر الحيمودي. (2023). الأمن السيبراني وحماية الأنظمة المعلوماتية. North African Journal of Scientific Publishing (NAJSP), 174-189.
- جمال الدين, ه. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية, 24(1), 189-230.
- حكمت اسماعيل, & ياسين. (2023). اداء طرق التشفير الكتلي وتحليل المخاطر. مجلة الرافدين لعلوم الحاسوب والرياضيات, 17(1), 23-33.
- زكي حسين متولي, م., مصطفى, عبد العال سالم غريب, & حسين. (2022). قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة الخارجية: دراسة تطبيقية. المجلة العلمية للدراسات المحاسبية, 4(4), 245-328.
- بودوشة, شاكر, بلجودي, & احلام/مشرف. (2017). حماية البيانات الشخصية في مجال التجارة الالكترونية (Doctoral dissertation, جامعة جيجل).
- الزهراني, عبد الله بن يحي سعيد الخزمري, الشهري, & حسن بن أحمد. مشرف. (2020). استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة: دراسة مقارنة (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية).
- موسى, ب. ح., & بوسي حمدي. (2023). العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة الدور المعدل لسمات منشاة المحاسبة والمراجعة: دراسة تجريبية. مجلة البحوث المحاسبية, 10(3), 387-458.
- جمال الدين, ه. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية, 24(1), 189-230.
- محمد المري, ر., & راشد. (2023). أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية| The Impact of Information Technology on the Security System and Internal Control. مجلة البحوث الفقهية والقانونية, 40(40), 1303-1373.

المحتويات