معهد العراب العالي للتدريب

١٠٨سايبر

إدارة امن المعلومات

م.نورة الحربي

نبذة عن المقرر

يهدف هذا المقرر الى التعرف على المهارات الأساسية في ادرة امن المعلومات وأيضا تقييم المخاطر وكيفية مواجهة هذه المخاطر وأيضا تفهم إدارة أنظمة امن المعلومات وكيفية إدارة مشاريع امن المعلومات وأيضا التعرف على اهم الممارسات والأساليب الأمنية التي تمكن من تامين المعلومات من التهديدات الالكترونية

معهد العراب العالي للتدريب

الأهداف العامة والتفصيلية من المقرر

مفهوم إدارة امن المعلومات
تقييم المخاطر في امن المعلومات
إدارة الجهود والمهام وحماية امن المعلومات
إدارة برامج ادرة امن المعلومات
فهم متطلبات وأنظمة المعلومات
إدارة المخاطر وبيان أهميتها
مخاطر امن المعلومات
السياسات و الإجراءات الخاصة بامن المعلومات
أنواع خطط الطوارئ و الخطوات المتبعة في تطوير كلا منها

الخبير العالمي في أمن المعلومات

ستيفان نابو : “إن أمن المعلومات أكبر بكثير من مجرد مسألة تقنية معلومات” .

مفهوم إدارة امن المعلومات

نظام إدارة أمن المعلومات ISMSهو مجموعة من السياسات المعنية بإدارة أمن المعلومات أو أنها ذات صلة بالمخاطر المتعلقة بالمعلومات.[1] المبدأ الذي يحكم نظام إدارة امن المعلومات هو أن المنظمة ينبغي عليها تصميم وتنفيذ والحفاظ على مجموعة مترابطة من السياسات والعمليات ونظم إدارة المخاطر لأصولها في مجال المعلومات الخاصة بها، وبالتالي ضمان مستويات مقبولة من مخاطر أمن المعلومات.

تقييم المخاطر في امن المعلومات

تعد تقنية المعلومات (تكنولوجيا المعلومات) متطورة بشكل لا متناهي. لقد قاد التعامل مع العديد من المقاولين والموردين، ومعماريات تقنية المعلومات المختلفة، وأحكام الاستضافة المتعددة الى استصعاب الحفاظ على رؤية متسقة للتهديد السيبراني على جميع المستويات. والتهديد يتطور باستمرار.

حتى عندما تعتقد أن النظام آمن، فإن الأساليب الأمنية الوقائية التقليدية قد لا تكشف أو تمنع عمليات الاحتيال والهجمات السيبرانية بشكل كامل. هذا هو السبب في أن الشركات لا تستطيع أن تدع هذه التهديدات تقف في طريق النمو والتوسع.

يعد تقييم أمان تكنولوجيا المعلومات، الذي يشمل التحقق من التطبيقات وأنظمة التشغيل وتكوينات الأجهزة بهدف الوصول إلى البيانات المحمية، وسيلة جيدة لتحديد نقاط الضعف الموجودة في البنية التحتية لتقنية المعلومات في المؤسسات.

هذه عي اول واهم الخطوات التي يمكن أن تتخذها المؤسسات للتخلص بشكل منهجي من مخاطر الاعدادات الخاطئة قبل أن يتمكن المهاجمون من استغلال الثغرات بها.

تقييم المخاطر في امن المعلومات

يعد تقييم أمان تكنولوجيا المعلومات ضروريًا في أي مؤسسة لأنه:

من خلال وضع التقييمات والتدقيقات الأمنية السيبرانية المناسبة، يمكن لمؤسستك تحديد الاستراتيجية الصحيحة ووضع برنامج النمو والتوسع لحماية بياناتك وأصولك الحساسة.

عن طريق القيام بما يلي:

1- التدقيق الأمني الاستباقي / الاختبار: هو أفضل وسيلة حماية ضد المتسللين والاحتيال الرقمي.

2- في حالة ما إذا كان احد الانظمة او البرامج قد تم اختراقها بالفعل

، وترغب المؤسسة في تحديد ما إذا كانت أي تهديدات لا تزال موجودة في الانظمة لتجنب(backdoor) الاختراق في المستقبل.

3- ترغب المؤسسات في تأمين بياناتها، كما أن التدقيق/الاختبار الأمني ضروري لضمان الأمان.

أهمية تقييم المخاطر في امن المعلومات

1- تحديد ما إذا كان المخترقين او المتطفلين يستطيعون الوصول غير المصرح به إلى الأصول التي تؤثر على الأمن الأساسي للانظمة والملفات والسجلات والبيانات.
2- لتأكيد أن الضوابط المطبقة، مثل النطاق، وإدارة الضعف والثغرات، والمنهجية، وتقسيم الشبكة، المطلوبة عامة في نظم الامتثال.

أهمية تقييم المخاطر في امن المعلومات

1- تحديد ما إذا كان المخترقين او المتطفلين يستطيعون الوصول غير المصرح به إلى الأصول التي تؤثر على الأمن الأساسي للانظمة والملفات والسجلات والبيانات.
2- لتأكيد أن الضوابط المطبقة، مثل النطاق، وإدارة الضعف والثغرات، والمنهجية، وتقسيم الشبكة، المطلوبة عامة في نظم الامتثال.

إدارة الجهود والمهام في حماية امن المعلومات

ادارة جهود تطوير برامج أمن المعلومات على مستوى الهيئة وتنفيذها، وقيادة الأنشطة المستمرة الرامية إلى الحفاظ على توافر مصادر معلومات الهيئة وصحتها وسريتها بما يتوافق مع سياسات ومعايير الأمن المتبعة.

الواجبات والمسؤوليات:

المسؤوليات الإدارية

* الإشراف على إعداد تقارير الأداء الدورية للإدارة
* إجراء تقييم الأداء السنوي للموظفين المرؤوسين.

المسؤوليات التشغيلية

*مراجعة البنية الأمنية وتقديم التوصيات الأمنية حول التصاميم المقترحة.
*المساهمة في إدارة المشاريع الأمنية والمساعدة في دمج أفضل الممارسات الأمنية في المشاريع الأخرى.
*تطوير سياسات وإجراءات ومعايير أمن المعلومات، وضمان توثيقها وتحديثها.
*المساهمة في تطوير سياسات وإجراءات ومعايير أمن المعلومات مع الإدارات المعنية، وضمان توثيقها وتحديثها.
*مراقبة الامتثال لجميع إجراءات وسياسات أمن المعلومات وإجراء عمليات مراجعة دورية بشأنها، والتأكد من اتساقها مع الضوابط الداخلية في جميع الإدارات.

إدارة الجهود والمهام في حماية امن المعلومات

*المساعدة في عملية تصميم وتنفيذ أنشطة مراقبة الامتثال والتحسين ذات الصلة، لضمان الامتثال مع كل من السياسات الأمنية الداخلية والقوانين واللوائح ذات الصلة.
*المساهمة في وضع خطة التعافي من مخاطر تقنية المعلومات بالتعاون مع الإدارات والأطراف الأخرى ذات العلاقة.
*رصد نقاط الضعف من خلال الفحوصات الداخلية والتقارير الخارجية، وتحليلها واقتراح المنهجيات العلاجية.
*توفير الرقابة وتولي مسؤولية الكشف عن محاولات التسلل ومتابعة معالجتها.
*تطبيق ومراعاة معايير الأمن والحماية العالمية لشبكات وأنظمة نظم المعلومات مع مراعاة المستجدات والعمل بها.
*المساهمة في تصميم امن الشبكات والمساهمة في وضع حلول تصحيحية للمشاكل المتعلقة بها.
*وضع الخطط الدفاعية لردع ومنع التسلل وحماية امن معلومات الهيئة من سرقة الهوية والبيانات، والقرصنة والتعدي على الخصوصية.
*مراقبة الشبكة للكشف عن محاولة الاختراقات

إدارة الجهود والمهام في حماية امن المعلومات

إعداد دراسة للأنظمة العاملة والتأكد من التزامها بالمعايير الأمنية المعتمدة.
*إعداد البرامج لرفع مستوى الوعي الأمني للموظفين.
*حوكمة امن المعلومات في الهيئة.
*وضع المعايير الأمنية للأنظمة.
*اعتماد منح الصلاحيات على الأنظمة.
*اعداد المراجعة الداخلية الأمنية للأنظمة.
*وضع الاختبارات الأمنية للتأكد من التزام الأنظمة بالمعايير الامنية والمستخدمين بالسياسات الأمنية
*اختبار الشبكة بشكل دوري وذلك للبحث عن نقاط ضعف.

إدارة برامج امن المعلومات

أدوات مراقبة امن الشبكات

Argus

واحدة من أفضل الأدوات المجانية والمفتوحة المصدر المتاحة لتحليل حركة
مرور الشبكة.
هي اختصار لـ "نظام إنشاء واستخدام سجلات التدقيق".Argus
يقوم البرنامج فقط بما يقوله الاختصار. تحليل فعال ومتعمق لبيانات الشبكة ،
وغربلة أجزاء كبيرة من حركة المرور بتقارير سريعة وشاملة.
سواء كانت الأداة الوحيدة التي
يحتاجها المستخدمون لمراقبة حركة المرور أم لا ، فإنها توفر أساسًا متينًا.

P0f

شائعًا على الرغم من نقص التحديثات. نادرًا ما تغير البرنامج منذ أكثر من عقد لأنه كان مثاليًا عند الإصدار. P0fلا يزال
P0fمبسطة وفعالة ، لا يولد
أي حركة مرور إضافية. يمكن استخدامه لتحديد نظام التشغيل لأي مضيف يتفاعل معه.
تقوم العديد
خفيف وسريع ونظيف. P0fمن الأدوات في هذه الفئة بإنشاء تحقيقات وعمليات بحث عن الأسماء واستعلامات متنوعة وما إلى ذلك.
لا غنى عنه للمستخدمين المتقدمين ، ولكن ليس من الأسهل تعلمه للمبتدئين في الفريق.

إدارة برامج امن المعلومات

تابع أدوات أمن الشبكات :

Splunk

مصمم لكل من التحليل في الوقت الفعلي وعمليات البحث عن البيانات التاريخية.
هي أداة مراقبة شبكة سريعة ومتعددة الاستخدامات. Splunk
أحد البرامج الأكثر سهولة في الاستخدام مع واجهة موحدة. تعمل وظيفة البحث القوية
هو تطبيق مدفوع مع توفر Splunkعلى تسهيل مراقبة التطبيقات. Splunkفي
إصدارات مجانية. النسخة المجانية محدودة. هذه أداة ممتازة لوضعها في القائمة
لأولئك الذين لديهم ميزانية للعمل . يميل المقاولون المستقلون إلى توخي الحذر بشأن
تستحق التكلفة. يجب على أي متخصص Splunkالأدوات المتميزة التي يشترونها.
.Splunkفي أمن المعلومات لديه قاعدة عملاء قوية بما يكفي أن يستثمر في

إدارة برامج امن المعلومات

تابع أدوات أمن الشبكات :

OSSEC

تحليلات في الوقت الفعلي لأحداث أمن النظام. OSSECتوفر خدمة اكتشاف التسلل مفتوحة المصدر يمكن تكوينه ليراقب باستمرار جميع المصادر المحتملة للدخول والوصول ، بما في ذلك الملفات ، والجذور الخفية ، والسجلات ، والسجلات ، والعمليات. وهو متاح أيضًا لمجموعة متنوعة من الأنظمة الأساسية ، مثل جيدًا أيضًا في OSSECيعتبر مجتمع مستخدمي .VMWare ESXو BSDو Macو Windowsو Linux مشاركة الاستراتيجيات والتعديلات والدعم والمعلومات المفيدة الأخرى. تشمل الأدوات الأخرى المتاحة الذي يقدم التدريب Wazuhالتي توفر "الشفاء الذاتي" لإصلاح الثغرات المكتشفة تلقائيًا ، و "Atomicorp" والدعم.

إدارة برامج امن المعلومات

أدوات التشفير :

KeePass

في إدارة الهوية ، وهي ضرورية للعديد من إعدادات المكتب. نظام بسيط لإدارة كلمات المرور. يسمح KeePassتُستخدم للمستخدمين بالوصول إلى جميع حساباتهم بكلمة مرور واحدة. من خلال الجمع بين الراحة والأمان ، يتيح KeePass للمستخدمين تعيين كلمات مرور فريدة لحسابات مختلفة مع وظيفة الملء التلقائي عند كتابة كلمة المرور KeePass لأكثر من يوم يعرفون مدى أهمية ذلك. في بعض الأحيان ، ترجع مشكلة InfoSecالرئيسية. أولئك الذين تعاملوا مع ضباط أمن الشبكات في إدارة العنصر البشري للوظيفة. KeePassالأمان إلى إدارة كلمات المرور السيئة. يساعد

TrueCrypt

من قبل مطوره TrueCryptمشهورًا على الرغم من مرور سنوات بدون تحديثات. تم التخلي عن TrueCryptلا يزال بتشفير المحتوى ذي TrueCryptفي عام 2014 ، وهو قديم تقنيًا ، لكنه لا يزال أداة قوية. نظام تشفير القرص ، يسمح الطبقات مع مستويين من التحكم في الوصول. برنامج مجاني وقوي ومفتوح. من السهل معرفة سبب استمرار شعبية على الرغم من عدم تحديثها منذ أربع سنوات. أحد أفضل برامج الأمان مفتوحة المصدر المتاحة. TrueCrypt

إدارة برامج امن المعلومات

أدوات فحص ثغرات الويب:

KeePass

في إدارة الهوية ، وهي ضرورية للعديد من إعدادات المكتب. نظام بسيط لإدارة كلمات المرور. يسمح KeePassتُستخدم للمستخدمين بالوصول إلى جميع حساباتهم بكلمة مرور واحدة. من خلال الجمع بين الراحة والأمان ، يتيح KeePass للمستخدمين تعيين كلمات مرور فريدة لحسابات مختلفة مع وظيفة الملء التلقائي عند كتابة كلمة المرور KeePass لأكثر من يوم يعرفون مدى أهمية ذلك. في بعض الأحيان ، ترجع مشكلة InfoSecالرئيسية. أولئك الذين تعاملوا مع ضباط أمن الشبكات في إدارة العنصر البشري للوظيفة. KeePassالأمان إلى إدارة كلمات المرور السيئة. يساعد

TrueCrypt

من قبل مطوره TrueCryptمشهورًا على الرغم من مرور سنوات بدون تحديثات. تم التخلي عن TrueCryptلا يزال بتشفير المحتوى ذي TrueCryptفي عام 2014 ، وهو قديم تقنيًا ، لكنه لا يزال أداة قوية. نظام تشفير القرص ، يسمح الطبقات مع مستويين من التحكم في الوصول. برنامج مجاني وقوي ومفتوح. من السهل معرفة سبب استمرار شعبية على الرغم من عدم تحديثها منذ أربع سنوات. أحد أفضل برامج الأمان مفتوحة المصدر المتاحة. TrueCrypt

إدارة برامج امن المعلومات

اختبار الاختراق

Metasploit

هذا. متوفر في إصدارات مفتوحة المصدر Metasploitإذا كنت تبحث عن أداة اختبار الاختراق ، فستقدر إطار عمل . Proللمطورين / موظفي الأمن أو إصدار
للبحث عن أكثر من 1500 اختراق ، بما في ذلك أمان تجزئة Rapid7يمكن للمستخدمين استخدام أداة أمان الشبكة من الشبكة. كما يسمح للشركات بإجراء تقييمات أمنية متنوعة وتحسين دفاعات الشبكة الشاملة ، بحيث تكون أكثر شمولاً واستجابة

Kali Linux

Linuxنظام تشغيل ومجموعة أدوات للتدقيق الأمني مع أكثر من 300 تقنية لضمان بقاء مواقعك وخوادم Kali Linuxيقدم في مأمن من الهجوم.
، والذي يعمل أيضًا على إدارة مجتمع مستخدم نشط وقاعدة بيانات Offensive Securityيتم تمويلها وصيانتها بواسطة شاملة للتهديدات وعمليات الاستغلال. يتضمن جزء من قاعدة المعرفة هذه شهادة في اختبارات القلم ودورة تدريبية مجانية ميم مجموعة الأدوات لجميع مستويات مهارات الأمان .Metasploit Unleashedعبر الإنترنت تسمى امها ، وليس فقط محترفي تكنولوجيا المعلومات المتقدمين.

مفهوم متطلبات أنظمة امن المعلومات

مهارات رئيسية يجب أن يملكها مدير الأمن السيبراني

أهم ست مهارات يملكها مدراء الأمن السيبراني، والتي ستساعدك في شق طريقك بهذا المجال بحال كنت تسعى للعمل كمدير أمن سيبراني في مؤسسة مرموقة.

1. عادات العمل

أولاً، ستحتاج إلى بعض عادات العمل الأساسية، بما في ذلك القدرة على العمل بشكل منهجي (وبطريقة تركز على التفاصيل).

القدرات التالية ستكون مفيدة أيضًا:

الحرص على البحث في الأسئلة الفنية وفحصها من جميع الجوانب.•

الحماس ودرجة عالية من القدرة على التكيف.•

مهارات تحليلية وتشخيصية قوية.•

21المهارات اللينة•

3. القدرة والفهم واستخدام مهارات الاستماع النشط (خاصة مع العملاء!).

. 4.مهارات تقنية

التعرف علي كيفية إدارة امن المعلومات بطريقة صحيحة

يجب أن يكون لنظام أمن المعلومات عدة محاور يجب إنشاءها وتوثيقها وتطبيقها وصيانتها في كل منشأة تريد أن تطبّق نظاما سليما متكاملا لأمن المعلومات لديها؛ ومن هذه المحاور:

- **سياسة أمن المعلومات** Security Policy : فيجب على الشركة أو المنشأة أن تكون لديها سياسة أمن المعلومات معتمدة من الإدارة وموثقة ومتاحة لكل العاملين المسئولين عن نظام أمن المعلومات. وكذلك الأطراف الخارجية المرتبطة الشركة

- **الهيكل التنظيمي لـ أمن المعلومات** Organization of Information Security: داخل أو خلال المؤسسة، وذلك لتحديد التزامات الإدارة العليا لتأمين المعلومات، وتنسيق أمن المعلومات، وتحديد المسئوليات، وعمليات التفويض لأماكن عمليات المعلومات، واتفاقيات الحفاظ على السرية، والاتصال والتعاون بين الهيئات، والأطراف الخارجية.

التعرف على كيفية إدارة امن المعلومات بطريقة صحيحة

إدارة الأصول :Asset Management
وذلك للوصول والتعامل مع الحماية المناسبة لأصول المؤسسة، وتحديد قائمة جرد الممتلكات، وملكية هذه الأصول، والاستخدام المقبول لها، وتصنيف وتمييز وتداول المعلومات.

أمن الموارد البشرية Human Resources Security
:وذلك لضمان تفهم الموظفين والمقاولين ومستخدمي الطرف الثالث لمسئولياتهم وأنها مناسبة لدورهم. ولتقليل مخاطر السرقة والخداع وسوء استخدام الموارد والأماكن. كما يجب التحري ووضع اشتراطات للتعيين، والتدريب على أمن المعلومات، وإجراءات إنهاء التعيين وغير ذلك.

تأمين المناطق والظروف المناخية :Physical and Environmental Securityوذلك بهدف منع من ليس لهم سلطة اختراق وإتلاف المباني التي تحتوي على مراكز معلوماتية للمؤسسة، فيجب تأمين المناطق، والتحكم في عملية الدخول إليها، وتأمين المكاتب والغرف والمعدات، والتأمين ضد التهديدات الخارجية والبيئية، والعمل في المناطق الآمنة، ومناطق، وتأمين الكوابل، وصيانة الأجهزة، وتأمين عملية التخلص من الأجهزة أو إعادة استخدامها، وكيفية إزالة الممتلكات

التعرف على كيفية إدارة امن المعلومات بطريقة صحيحة

إدارة الاتصالات والعمليات : Communication and Operation Management

وذلك بهدف التأكد من التشغيل الصحيح والآمن لوسائل معالجة المعلومات. بوضع إجراءات التشغيل الموثقة، وكيفية إدارة تعديلات التشغيل، وعمليات الفصل للواجبات ولوسائل التشغيل والتطوير، وإدارة توصيل خدمات الطرف الثالث، وتوصيل الخدمات، وعملية مراقبة ومراجعة خدمات الطرف الثالث، وعمليات تخطيط وقبول النظام، والضوابط الأمنية ضد البرامج والأكواد المنقولة، والنسخ الاحتياطية للمعلومات، وإدارة أمن الشبكات، وأمن وثائق النظام، وسياسة وإجراءات تبادل المعلومات

التعرف على كيفية إدارة امن المعلومات بطريقة صحيحة

مراقبة الدخول :Access control

وذلك بهدف ضبط والتحكم في الدخول على المعلومات، وكيفية اعتماد وتسجيل المستخدم، وإدارة حقوق الامتياز وكلمة السر، ومراجعة الحقوق والمسئوليات للمستخدمين، ومراقبة الدخول، وخطط العمل عن بعد، وغير ذلك.

تطوير وصيانة نظم المعلومات :Information Systems development and maintenance

وذلك بهدف التأكيد على أن المطالب الأمنية جزء متكامل من نظم المعلومات، وتحليل وتوصيف المتطلبات الأمنية، وتحديد العمليات الصحيحة في التطبيقات، لمنع أخطاء وفقد التعديلات غير المصرح بها، وضوابط التشفير، وضبط الأضرار الفنية.

التعرف على كيفية إدارة امن المعلومات بطريقة صحيحة

إدارة حوادث أمن المعلومات :Information security incident management

وذلك بهدف ضمان أن أحداث أمن المعلومات ونقاط الضعف المرتبطة بنظم المعلومات تكون متصلة بشكل يسمح باتخاذ الإجراءات التصحيحية في الوقت المناسب.

إدارة استمرارية العمل :Business continuity management

بهدف إبطال العوائق لنشاط المؤسسة ولحماية سير العمل الأساسي من تأثير الكوارث او الأعمال الفاشلة الضخمة لنظام المعلومات لضمان استعادتها في الوقت المناسب.

التطابق مع القوانين والتشريعات :Compliance

وذلك لتحاشى مخالفة كل من القوانين الجنائية والمدنية والتشريعات والارتباطات التعاقدية التي تشمل متطلبات أمنية. والتعرف على التشريعات السارية وحقوق الملكية الفكرية، وغير ذلك

التعرف على كيفية ادرة المخاطر وأهميتها

أهمية إدارة المخاطر في العديد من النقاط نوضحها فيما يلي:

1- توقع المشكلات المُحتملة
2- تجنب الأحداث الكارثية
3- اتخاذ قرارات أفضل
4- بقاء الشركات قادرة **على** المنافسة
5- تحسين أساليب العمل
6- وضع ميزانية أفضل
7- التأثير الإيجابي **على** مستوى الشركة

التعرف على كيفية ادرة المخاطر وأهميتها

خطوات ومراحل إدارة المخاطر:

تحديد المخاطر

عملية تحديد المخاطر يقوم بها فريق العمل القائم على إدارة المخاطر، وذلك من خلال العصف الذهني أو التحليل

2- تحليل المخاطر

في هذه الخطوة يقوم قسم إدارة المخاطر بتحليل التهديدات المحتملة على المؤسسة أو المشروع لقياس مدى شدتها، بالإضافة الكشف عن الصلة بينها وبين والأسباب المؤدية لحدوثها والمرتبطة بالمؤسسة، تُنفذ هذه العملية بشكل يدوي وعلى إثرها تُحدد السياسات والإجراءات التي ترسم إطار إدارة المخاطر.

3- تقييم المخاطر

وفي تلك المرحلة تتحدد المخاطر الأكثر شدة والأقل شدة من أجل ترتيب الأولويات في التهديدات التي تتطلب إداراتها أولاً وبشكل عاجل وتدخل من الإدارة العليا

4- معالجة المخاطر

تأتي خطوة التعامل مع المخاطر من خلال إتخاذ الإجراءات المطلوبة لتجنب حدوثها أو التقليل من شدة أضرارها،

5- رصد المخاطر

التعرف على كيفية ادرة المخاطر وأهميتها

أنواع إدارة المخاطر

إدارة المخاطر تنقسم أساسًا إلى أربعة أنواع تعبر عن الاستراتيجيات المتبعة للتعامل مع المخاطر. تتضمن هذه الأنواع :

تجنب المخاطر :حيث يتجنب اتخاذ القرارات التي قد تزيد من احتمالية حدوث مخاطر معينة

تقليل من المخاطر: حيث يُتخذ إجراءات لتقليل الآثار السلبية للمخاطر على المشروع أو المؤسسة. استراتيجية

تحويل المخاطر: تعتمد على تحويل المسؤولية عبر توقيع عقد مع جهة أخرى تتحمل المخاطر.

تقبل المخاطر: ، فيتمثل في قبول المخاطر دون اتخاذ إجراءات لتقليل آثارها، وغالباً تستخدم عندما تكون تكاليف التقليل أعلى من قيمة المخاطر.

التعرف على كيفية ادارة المخاطر وأهميتها

أنواع إدارة المخاطر

إدارة المخاطر تنقسم أساسًا إلى أربعة أنواع تعبر عن الاستراتيجيات المتبعة للتعامل مع المخاطر. تتضمن هذه الأنواع :

تجنب المخاطر :حيث يتجنب اتخاذ القرارات التي قد تزيد من احتمالية حدوث مخاطر معينة

تقليل من المخاطر: حيث يُتخذ إجراءات لتقليل الآثار السلبية للمخاطر على المشروع أو المؤسسة. استراتيجية

تحويل المخاطر: تعتمد على تحويل المسؤولية عبر توقيع عقد مع جهة أخرى تتحمل المخاطر.

تقبل المخاطر: ، فيتمثل في قبول المخاطر دون اتخاذ إجراءات لتقليل آثارها، وغالباً تستخدم عندما تكون تكاليف التقليل أعلى من قيمة المخاطر.

مخاطر امن المعلومات

١. **الأخطاء:** سواء كانت أخطاءً في إدخال البيانات يدويًا أو في استخدام بيانات قديمة، تعد التحليلات المستندة إلى جداول البيانات عرضة للأخطاء، خاصةً عندما تستند التحليلات إلى مجموعات بيانات كبيرة ومعقدة. حتى خطأ صغير يمكن أن يكون له عواقب كبيرة، خاصة إذا لم يتم الكشف عنه لفترة طويلة. كما يمكن تقديم الأخطاء عند معالجة البيانات لأغراض مثل التحليلات.

2. **انعدام أمان البيانات:** يمكن نسخ جداول البيانات ومشاركتها وتوزيعها بسهولة، مما يزيد من خطر الوصول غير المصرح به أو انتهاكات البيانات(كما يمكن اختراق البيانات الحساسة المُخزنة في جداول البيانات عند نقلها إلى أنظمة أخرى للقيام بمهام مثل التحليلات والتمثيل المرئي.

3. **قابلية محدودة للتوسع:** يمكن لجداول البيانات إدارة عدد كبير من التقارير والمستخدمين بسهولة، لكنها غير مجهّزة للتعامل مع كميات كبيرة من البيانات أو العمليات الحسابية المعقدة وتحليل الأعمال، مما يؤدي إلى عجز في الأداء وأخطاء به.

مخاطر امن المعلومات

الافتقار إلى الشفافية: قد يكون من الصعب تتبع أصل البيانات أو فهم المنطق وراء العمليات الحسابية في جدول بيانات، خاصة إذا تم إنشاؤه بواسطة شخص آخر باستخدام بيانات من مصادر متعددة.

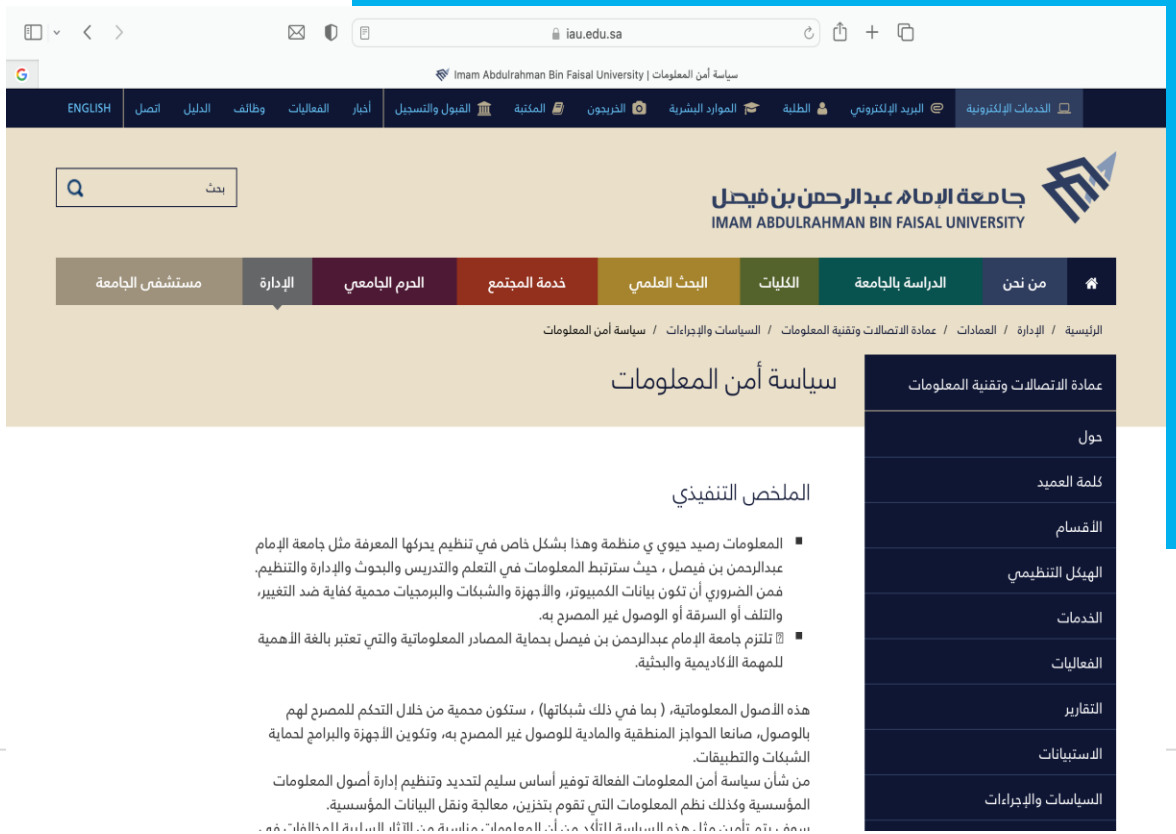
5. **كفاءة سير العمل:** نظرًا لوجود مشكلات وقيود في مشاركة البيانات عبر جداول البيانات، يمكن أن يؤدي استخدامها إلى عمليات يدوية ومتكررة عبر الأعمال ويتسبب في قيام الأشخاص ببذل جهود متكررة في محاولة حل نفس المشكلات أو المماثلة لها.
6. **مستودعات العمل:** يتم في العادة إنشاء جداول البيانات واستخدامها بواسطة أفراد أو فِرق، مما قد يؤدي إلى إنشاء مستودعات معلومات ويؤدي إلى عدم اتساق وأخطاء في البيانات.

مخاطر امن المعلومات

7. **التحكم في الإصدار:** مع تحرير مستخدمين متعددين جدول بيانات واحد، قد يكون تتبع أحدث إصدار صعبًا في حالة استخدام جدول البيانات بشكل غير صحيح. قد يؤدي ذلك إلى التشوش، وقد ينتهي الأمر بالأشخاص الذين يعملون باستخدام إصدارات جداول بيانات مختلفة. يمكن أن تدعم جداول البيانات التعاون في الوقت الفعلي باستخدام الإصدارات السحابية، لكن يُفضل العديد من المستخدمين إصدارات سطح المكتب التي تسبب هذه المشكلات.
8. **إضاعة الوقت:** يمكن أن يستهلك الحفاظ على جداول البيانات وتحديثها وقت الموظف، خاصة عند التعامل مع كميات كبيرة من البيانات، والتي يمكن أن تحول الموارد والوقت من أنشطة أعمال أكثر أهمية.
9. **نطاق البيانات المحدود:** تقتصر جداول البيانات على التعامل مع أنواع البيانات المهمة لجهود التحليلات، خاصةً البيانات غير المنظمة، مثل المستندات النصية الكبيرة.
10. **انعدام الثقة:** يمكن لأي من هذه العوامل أن يدفع قادة الأعمال إلى الاعتقاد بأن المعلومات التي يعتمدون عليها لاتخاذ القرار قديمة أو غير دقيقة أو متحيزة. يعود القادة الذين لا يثقون في بياناتهم إلى اتخاذ القرارات الجريئة القائمة على الخبرة بدلاً من الاعتماد على البيانات فعليًا.

السياسات والإجراءات الخاصة بمخاطر امن المعلومات

أمثلة على سياسة واجراءات امن المعلومات بجامعات المملكة العربية السعودية :



https://www.iau.edu.sa/ar/administration/deanships/deanship-of-information-and-communication-technology/policies-and-procedures/information-security-policy

سؤال وإجابة

1- من مخاطر امن المعلومات :

A. الأخطاء
B. خطة الطوارئ
C. الاثنان معا

تطبيق عملي !!

الرجاء كتابة سياسة امن المعلومات لمعهد العراب ..

فعالية عملية ادارة امن المعلومات

هدف إدارة أمن المعلومات الى توفير بيئة عمل آمنة لكافة أصول المعلومات بالجامعة وضمان سريتها وسلامتها وعملها المستمر من خلال المهام التالية:

- انشاء سياسات واجراءات أمن المعلومات التي توفر البيئة الآمنة بالجامعة والعمل على الالتزام بها مع تحسينها وتطويرها بشكل دوري.
- العمل على أمن وسرية أصول الجامعة وحفظ حقوق الملكية للجامعة والمستخدمين.
- مراقبة شبكة الجامعة بشكل مستمر وكشف أي هجوم داخلي او خارجي.
- تطبيق المعايير الدولية التي توفر أمن المعلومات المثالي، مثل **ISO** 27001.

فعالية عملية ادارة امن المعلومات

- منع الدخول الغير مصرح إلى مناطق العمل الحساسة وحماية الموارد الفيزيائية في الجامعة.
- حذف الحسابات الغير مستخدمه والتحكم في عملية الدخول لمنسوبي الجامعة مع تقليل الصلاحيات الغير ضرورية.
- المراقبة المستمرة لكافة الأحداث الأمنية للمستخدمين والتطبيقات والنظم وتوثيق الأحداث الغير عادية لمراجعتها.
- تقديم برامج التدريب والتوعية لمنسوبي الجامعة من طلاب، وأعضاء هيئة تدريس، وموظفين.
- التقييم الدوري للمخاطر ووضع خطط شاملة للاستجابة لأي الهجمات المحتملة واختبار مدى فاعلية هذه الاستجابة.

خطط الطوارئ والخطوات المتبعة في التطوير

خطط الطوارئ هي مجموعة من القوانين والإجراءات يتم اتخاذها عند حدوث أمر معين. ولا يمكن لأي شركة أو منظمة أن تكون قادرة على تحقيق أهدافها على أكمل وجه وفي أسرع وقت إلا بالتخطيط المدروس لكل حدث أو عارض قد يعرض لها أثناء مسيرتها في تحقيق أهدافها. ولعل المخاطر بجميع أنواعها من كوارث طبيعية أو سرقات أو احتيال من قبل البشر تكون من أهم ما يجب على المنظمات التخطيط له ولمواجهته بأتم استعداد

خطط الطوارئ والخطوات المتبعة في التطوير

الاستجابة لحوادث الأمن السيبراني: هي خطة موثقة ومكتوبة، تتألف من ست مراحل متميزة، تساعد متخصصي تقنية المعلومات والموظفين في التعرف على حادثة الأمن السيبراني والتعامل معها مثل خرق البيانات أو الهجوم السيبراني.

لضمان إنشاء وإدارة خطة الاستجابة للحوادث بشكل صحيح، يجب على مدراء الأمن السيبراني إجراء تحديثات وتدريب منتظم.

خطط الطوارئ والخطوات المتبعة في التطوير

- اختبار خطة الاستجابة للحوادث على الأقل سنويًا
- تعيين موظفين معينين ليكونوا متاحين على مدار الساعة للتعامل مع الحوادث
- تدريب الموظفين بشكل صحيح ومنتظم على مسؤوليات الاستجابة للحوادث
- إعداد التنبيهات من كشف التسلل ومنع التطفل وأنظمة مراقبة سلامة الملفات
- تنفيذ عملية لتحديث وإدارة خطة الاستجابة للحوادث حسب الصناعة والتغييرات التنظيمية

خطط الطوارئ والخطوات المتبعة في التطوير

مراحل الاستجابة للحوادث هي:

- **التحضير**
- **التعريف**
- **الاحتواء**
- **الاستئصال**
- **الاستعادة**
- **الدروس المستفادة**

سؤال وإجابة

1- من مراحل الاستجابة للحوادث :

A. التحضير
B. الاحتواء
C. الاثنان معا