معهد العراب العالي للتدريب

اساسيات الامن السيبرانى

م.سمر سعيد الهوارى

أمن السيبراني ▪ -عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، هدفها الوصول الى معلومات حساسة و تغييرها أو تدميرها.

التهديدات ▪ -احتمالية وجود خطر على امن المعلومات، قد يتشكل هذا التهديد كإنسان او فايروس او برامج ضارة او اي شي اخر .كالمقاطعة و الاعتراض و التلفيق و التعديل

الهجمات ▪ -هو الهجوم الفعلي المقصود بدون صلاحية على النظام لاستغلال نقاط ضعف نظام امن المعلومات.

الفرق بين التهديدات و الهجمات

/	التهديد	الهجمات
طبيعتها	غير متعمدة. يمكن ان تكون مقصودة (تنافس شرس)، غير مقصود (كوارث طبيعية)	متعمدة. صاحب الهجوم يملك دوافع و خطط للهجوم
الضرر	غالبًا لا	دائمًا ضارة
التعريف	حالة يمكن ان تسبب ضررًا للنظام مستقبلًا	حالة مهيئة لصنع الضرر في النظام
احتمالية التدمير	تختلف من عالية لمنخفضة	نسبة الضرر عالية
الكشف	صعب اكتشافه	من السهل نسبيًا اكتشافه
المنع	يمكن التحكم بنسبة حدوثه	لا يمكن منعه بالتحكم به. يمكن حمايته بالنسخ الاحتياطي
انطلاقها	تُشغل بواسطة النظام او شخص خارجي	تُشغل بواسطة شخص خارجي

اهداف الامن السيبرانى

CIA

- **الخصوصية:** "هل نظامي محمي من هجمات العالم الخارجي، و الدخول الغير مصرح؟"
  - حماية البيانات من الوصول الغير مصرح لها، فقط من يملكون الصلاحية يستطيعون رؤيتها.

- **النزاهة:** "هل تم التلاعب في بياناتي أو إفسادها أو تأثرها من تهديد خارجي؟"
  - التأكد من صحة المعلومات و عدم التحريف فيها وأن مصدر المعلومات حقيقي.

- **الإتاحة:** "هل يمكن الوصول بسهولة الى أنظمتي وبياناتي للإستخدام اليومي؟"
  - المعلومات متاحة للأشخاص المصرح لهم.

الخصوصية	النزاهة	الإتاحة
Encryption - التشفير إدارة عملية الدخول: • المعرف - الأسم • المصادقة - الرقم السري • تفويض - الإذن Steganography - اخفاء البيانات: • الرسائل الخفية داخل الموقع • الرسائل الخفية داخل الملفات و الصور	**التأكد من عدم العبث بالبيانات** **التشفير** إنشاء كود مشتق من خلال خوارزمية، اذا تم تغيير البيانات، فسيتم تغيير الكود في المستقبل ايضًا **توقيع رقمي، شهادة** ارسال توقيع رقمي فريد، بتوضيح من ارسل الرسالة ومن يسمح للمستلم بقراءتها	**ضمان إمكان استرداد البيانات عند الحاجة إليها** • أي فشل في SPOF يتوقف النظام بإكمله عن العمل • تكرار القرص • تكرار الخوادم • النسخ الإحتياطية • الطاقة البديلة • التوقي

الهجمات وأنواعها وطرقها

عن طريق البشر:

- هجوم الوسيط (Man-in-the-Middle): يدخل المهاجمون أنفسهم ضمن معاملة ثنائية الأطراف، يمكنها الآتي:
  - التنصت على المعلومات المرسلة بين الطرفين دون معرفتهم

- هجوم رفض الخدمة (DDoS): إغراق النظام بالعديد من رسائل طلبات المرور حتى تنفذ الموارد، عندها ينهار الخادم ويتعذر عن الرد على باقي الطلبات.

- الهجوم دون إنتظار: بعد إكتشاف ثغرة أمنية بالنظام وقبل تحديث الثغرة يستهدف المهاجم الثغرة

- التصيد (Phishing): يحدث عندما يحصل المجرمون على معلومات عنك من مواقع الويب أو مواقع الشبكات الاجتماعية، ويقومون بتخصيص مخطط تصيد لك.

- إنتحال الشخصية (Spoofing): استخدام لجعله يبدو كما لو أن الرسالة واردة من مصدر موثوق به .عنوان بريد إلكتروني أو رقم هاتف مزيف

الهجمات وأنواعها وطرقها

عن طريق البرامج الضارة (Malware)

- فايروس (Various): برنامج صغير ينزل رفقة برنامج اخر يفسد المعلومات
- الدودة (Worm): برنامج صغير ينزل رفقة برنامج اخر يفسد المعلومات وينسخ نفسه بالجهاز، ينتقل عند إرسال الملفات
- حصان طروادة (Trojan): برنامج يخفي غرضه الحقيقي
- فيروس الفدية (Ransomware): فايروس يشفر المعلومات ولا تفتح حتى دفع المبلغ المطلوب

(AAA)المصادقة و القدرات والحدود

- **المصادقة (Authentication) :** هل شهد هي شهد؟
  - عملية التحقق من هوية المستخدم.
- **القدرات (Authorization) :** بينما نحن نعرف شهد، ماهو المصرح لشهد؟
  - عملية إعطاء الإذن للمستخدم ليستعمل المصادر المعينة او المهام.
- **الحدود (Accountability) :** بينما نحن نعرف شهد، ماذا فعلت شهد؟
  - أحدد ماهو ضمن صلاحيته و خارجها.

خدمات المصادقة

خدمات المصادقة : هي آلية مماثلة لإستخدام كلمات المرور في أنظمة مشاركة الوقت، تتم مقارنة بيانات المستخدم المقدمة بتلك الموجودة في ملف قاعدة بيانات لمعلومات المستخدم المصرح له على نظام تشغيل محلي او داخل خادم مصادقة.

أنواع الخدمات:

Kerberos

Asymmetric Encryption Key

Remote Access Service Authentication

SSO - Single Sign On

معهد العراب العالي للتدريب

مراجعة سريعة

2023

النـهايـة

سؤال و إجابة

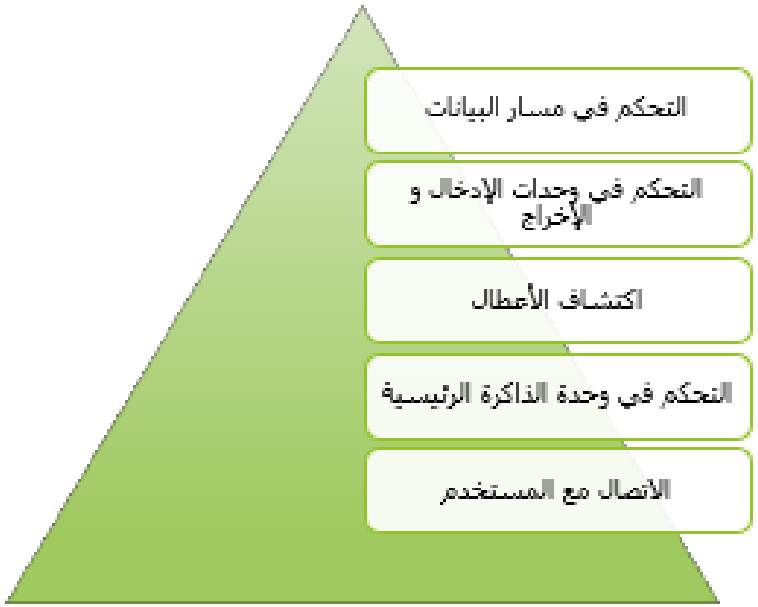
1- من البرامج الضارة
A. الدودة
B. الفيروس
C. الاثنان

2- من اهداف الامن السيبرانى
A. السرية
B. النزاهة
C. الاثنان

نظام التشغيل - Operating System :

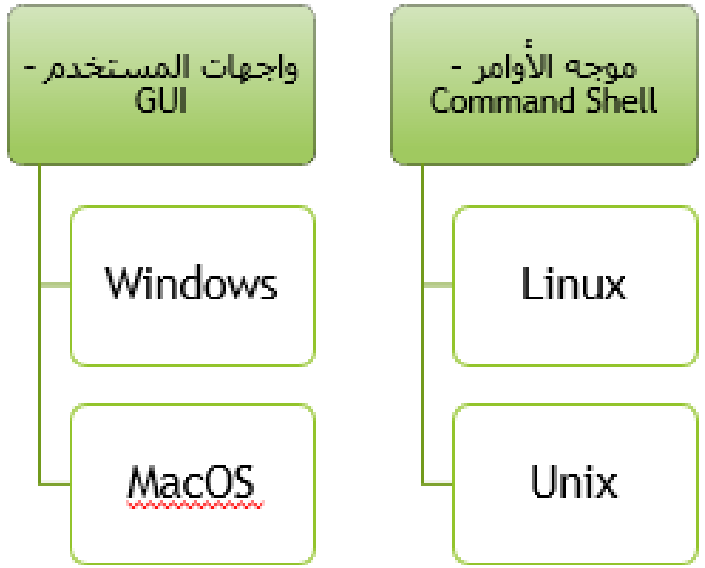
عبارة عن جُملةٍ من البرمجيات (Software)، وهو حلقة الوصل بين المستخدم وجهاز الحاسوب، كما يُعرَّف بأنّه المشغِّل الرئيسي لجهاز الحاسوب، والمنسّق بين أجزاء الحاسوب المادية (Hardware) والبرمجيّة (Software). أي أنّه المسؤول عن إدارة جهاز الحاسوب؛ حيثُ يُعدّ نظام التشغيل بمثابة مُترجِم أو وسيلة اتصال بين المُستخدِم والحاسوب.

مهام نظام التشغيل:



- ينقسم نظام التشغيل لقسمين للتعامل معه :

- واجهة مستخدم نظام التشغيل هي الواجهة المرئية لمستخدمي النظام. وهي عبارة قشرة (shell) و غلاف لنظام التشغيل. تتفاعل مع المستخدم بضغطة زر على الفارة.
- موجه الأوامر أو CMD، هو مترجم سطر الأوامر لأنظمة التشغيل. يتفاعل مع المستخدم بأوامر كتابية.



امن الشبكات

المصادقة

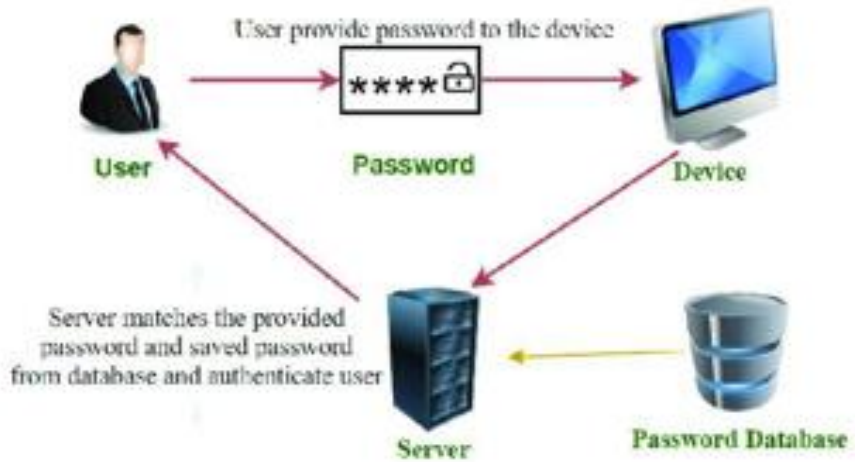
- هي عملية فحص المستخدمين الذين يطلبون الوصول الآمن إلى الشبكات أو الأنظمة أو الأجهزة. تحدد هذه العملية هوية المستخدم ويمكن العثور عليها من بيانات اعتماد اسم المستخدم وكلمة المرور والتقنيات الأخرى مثل تطبيقات المصادقة أو القياسات الحيوية.

- طرق زيادة الأمان في مصداقية الشبكات:

1. **المصادقة لكلمة المرور - Password-based authentication**
2. **المصادقة الثنائية - Two-factor authentication**
3. **CAPTCHAs**
4. **مصادقة العلامات الحيوية - Biometrics authentication**
5. **مصادقة التوقيع - Certificate-based authentication**

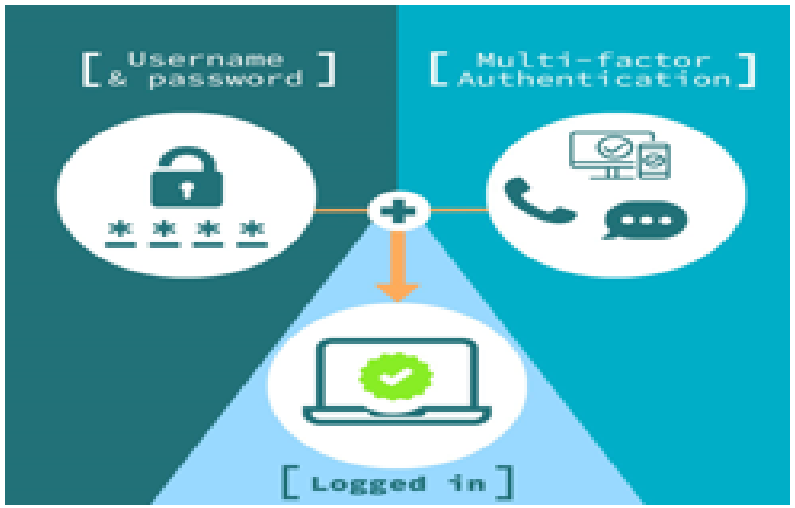
المصادقة لكلمة المرور

- يدخل المستخدم كلمة المرور ولا يستطيع الدخول الا بعد مطابقة رقمه السري
- يتحقق الخادم من كلمة المرور المدخلة وكلمة المرور المرتبطة بإسم المستخدم في قاعدة البيانات
- مثل/ البريد الإلكتروني



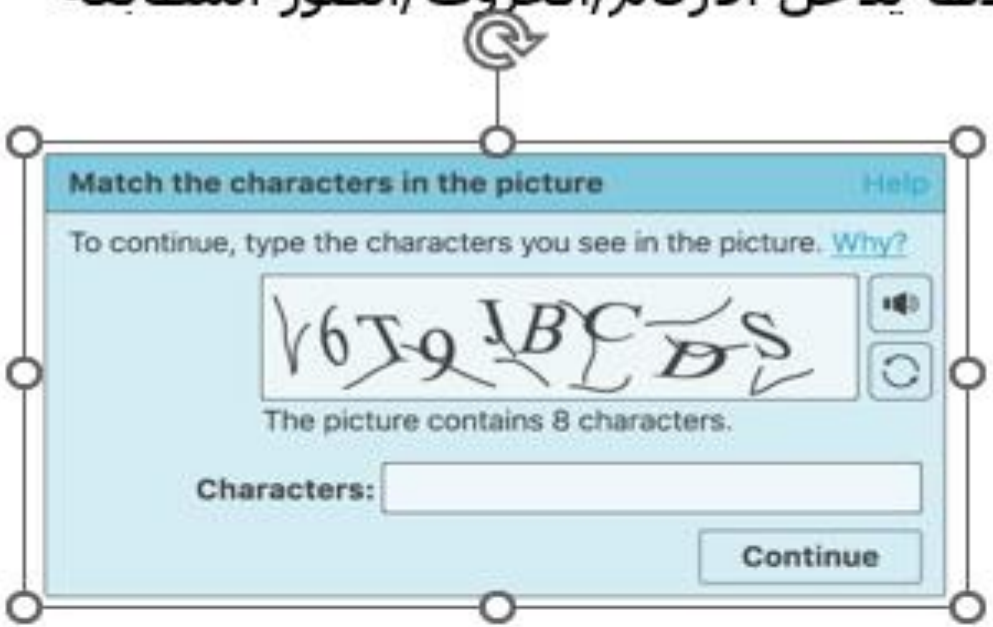
المصداقية الثنائية

- يدخل المستخدم كلمة المرور ولا يستطيع الدخول الا بعد مطابقة رقمه السري
- بعد التأكد من كلمة المرور المدخلة رفقة قاعدة البيانات، يُرسل رقم قصير على البريد الإلكتروني/الهاتف
- يدخل المستخدم الرقم القصير وعندها يستطيع تسجيل الدخول
- مثل/ تسجيل دخول موقع أبشر



CAPTCHA

- يأكد ما إن كان الذي يسجل الدخول إنسان او ألي
- يدخل معلومات التسجيل بعدها يدخل الأرقام/الحروف/الصور المطابقة

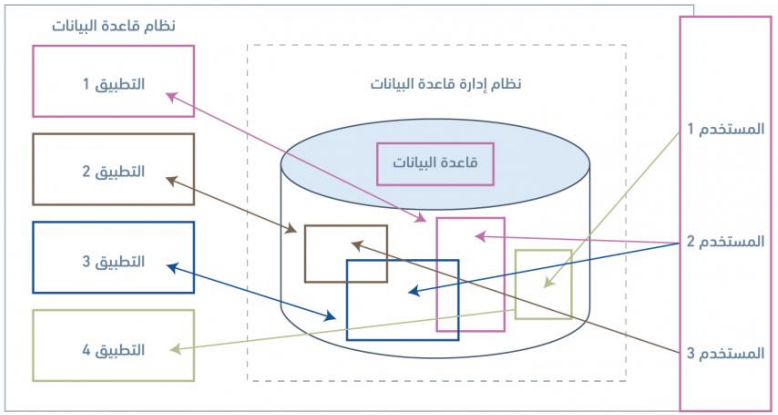


مصادقه العمليات الحيوية

- يدخل كلمة السر وتراجع عن طريق قواعد البيانات
- يدخل رقم الهاتف/البريد الالكتروني ويدخل الرقم الخاص للتحقق
- يستعمل نظام البصمة للتأكد من هوية الشخص
- مثل/ تطبيق نفاذ

امن قواعد البيانات

- هي عبارة عن مجموعة من المعلومات المُنظّمة بطريقة تسمح الوصول إليها، وتعديلها، وإدارتها بسهولة. يتم استخدام قواعد البيانات من قِبَل المنظّمات من أجل تخزين المعلومات، واسترجاعها، وإدراتها.



تملك قاعدة البيانات الخصائص التالية:

1. تُعَدّ قاعدة البيانات منطقيةً، ومتماسكةً، ومُتسقةً داخليًا.
2. صُممَت قاعدة البيانات وبُنيت ومُلِئت بالبيانات لخدمة غرض معيّن.
3. يُخزَّن كل عنصر بيانات في حقل field.
4. تُكوِّن مجموعة الحقول جدولًا table، فمثلًا، يحتوي كل حقل في جدول الموظف على بيانات حول موظف فردي.

متطلبات الامان

- **الإستباق مع إدارة التصحيح**

تعد إدارة التصحيح ممارسة أساسية للحفاظ على أمان قاعدة البيانات الخاصة بك. لا يضمن تحديث برنامج قاعدة بياناتك بانتظام بأحدث التصحيحات أنك تستفيد من أحدث الميزات وإصلاحات الأخطاء فحسب، بل إنه يعالج أيضًا الثغرات الأمنية التي يمكن أن يستخدمها مجرمون الإنترنت للتسلل إلى أنظمتك واختراقها.

- **تنفيذ ضوابط قوية للمصادقة والترخيص**

يعد استخدام عناصر التحكم في المصادقة والترخيص أمرًا ضروريًا لتأمين الوصول إلى قاعدة البيانات الخاصة بك وحماية البيانات الحساسة. تساعد عناصر التحكم هذه على ضمان أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى النظام وتنفيذ إجراءات محددة وفقًا للأدوار والأذونات المخصصة لهم.

- **تأمين اتصالات قاعدة البيانات الخاصة بك**

لضمان الأمان العالي وحماية البيانات، يعد تأمين جميع اتصالات قاعدة البيانات أمرًا ضروريًا. يساعد الحفاظ على قنوات اتصال آمنة على منع الوصول غير المصرح به أو تسرب البيانات أو هجمات الوسيط التي قد تؤدي إلى تعرض المعلومات الحساسة للخطر.

- **تشفير البيانات الحساسة**

يعد تشفير البيانات الحساسة أمرًا بالغ الأهمية لحماية مؤسستك من الوصول غير المصرح به والتهديدات السيبرانية وانتهاكات البيانات. يضمن تشفير البيانات أن تظل سرية وغير قابلة للقراءة، حتى إذا تمكن المهاجم من الوصول إلى قاعدة البيانات الخاصة بك.

معهد العراب العالي للتدريب

مراجعة سريعة

2023

النـهايـة

سؤال و إجابة

1- من اقسام الامن السيبرانى

A. امن الشبكة
B. امن البيانات
C. الاثنان

2- من اهداف الامن السيبرانى

A. السرية
B. النزاهة
C. الاثنان

إدارة مخاطر الامن السيبرانى

- تعرّف **إدارة مخاطر الأمن السيبراني** على أنها مجموعة خطوات تتُخذ بشكل دوري لمواجهة التهديدات الإلكترونية ومعالجتها من خلال رصدها وتحديدها وتقييمها، ومن أجل إدارتها بفاعلية فإن ذلك يتطلب نظرة شاملة لهذه المخاطر وتعاون من كافة أفراد العمل.

- تعتمد إدارة مخاطر الأمن السيبراني على استراتيجيات تساعد على ترتيب أولويات المخاطر المطلوب معالجتها؛ لرصد التهديدات الأكثر ضررًا والمطلوب مواجهتها في الوقت المطلوب.

عوامل زيادة مخاطر الأمن السيبراني

عند البحث عن الأسباب التي تزيد من وقوع المخاطر الإلكترونية نجد أن بعضها يكون بسبب أخطاء تحدث من الأفراد العاملين بالمؤسسة ومشكلات تقنية، العوامل:

- وقوع عطل في الشبكات ينجم عنه فقدان بيانات هامة.
- استخدام أجهزة المؤسسات من أماكن بعيدة عند السفر أو من المنازل.
- عدم الاطلاع على سياسات الأمن السيبراني ومراجعتها خلال عام.
- دخول أحد الموظفين غير المختصين على نظام الأمن السيبراني ووصوله إلى الخيارات الإدارية الخاصة به.
- استخدام أجهزة المؤسسات في إجراء المعاملات البنكية مثل تحويل الأموال.

مراحل عملية إدارة مخاطر الأمن السيبراني قبل وقوع المخاطر

تعتمد إدارة مخاطر الأمن السيبراني على **خمسة خطوات رئيسة** والتي تشمل ما يلي:

1- تحديد الأصول وبيئة تكنولوجيا المعلومات

لا بد من تحديد الأصول قبل حمايتها، فيتم تحديد جميع التطبيقات والخدمات والأجهزة، المُستخدمة في مختلف الأعمال، أو التي تدعم أهم عملياتها.

2- تحديد المخاطر وتقييمها

إذ يتم تعيين مستوى تهديد لكل برنامج وجهاز كمبيوتر محمول وخادم وجهاز نقاط البيع وجهاز محمول، اعتمادًا على مدى تعرضه للتهديدات، والوقوف على مدى تأثير تلك التهديدات على الأداء العام للعملية الأساسية للأعمال.

3- وضع استراتيجية قوية لإدارة مخاطر الأمن السيبراني

بعد ذلك يتم وضع استراتيجية وخطة مدروسة وقوية لإدارة مخاطر الأمن السيبراني، تلك الاستراتيجية التي تحتاج إلى تطوير وتخطيط مناسبين، ومواصلة تحديثها من قِبل المؤسسة.

ويمكن القول أن جعل الأمن السيبراني مسؤولية الجميع، هو شيء لا غنى عنه ويجب إدراجه في استراتيجية إدارة المخاطر.

4- تحديد الحلول للتغلب على مخاطر الأمن السيبراني:

تتمثل هذه الخطوة في الوصول إلى حلول مؤقتة (قصيرة الأجل)، وحلول دائمة (طويلة الأجل)، لمنع تهديدات الأمن السيبراني، وهناك 4 استراتيجيات تُتبع للوصول إلى الحل الأمثل وهي:

5- تنفيذ الحلول ورصد الفاعلية

الخطوة الأخيرة في إدارة مخاطر الأمن السيبراني هي تنفيذ القرارات التي جرى اتخاذها في أقرب وقت ممكن، ومن ثم البدء في الحماية من التهديدات.

ومعظم الحلول البرمجية لمراقبة مخاطر الأمن السيبراني، تحتوي على لوحات معلومات تظهر مستويات التعرض للمخاطر، وذلك للتأكد من أن الحلول المقدمة تساعد بالفعل في حل التهديدات.

وفي حال وجود ثغرات في السياسات، أو دفاعات ضعيفة، أو تم تحديد مخاطر جديدة غير متوقعة؛ فإن العملية برمتها تعود إلى الخطوة الأولى، وتبدأ عملية إدارة مخاطر الأمن السيبراني من جديد.

- ويجدر التنويه إلى أن تلك الخطوات الخمس هي جزء من دورة إدارة المخاطر التي لا نهاية لها والتي تتكرر حتى يتم حل جميع التهديدات المُحددة، وهذه العملية بحاجة إلى تشغيل وتطوير مستمرين، للتأكد من عدم ظهور مشكلات جديدة في المستقبل

مراحل عملية إدارة مخاطر الأمن السيبراني بعد حدوث مخاطر سيبرانية

1- تحديد المخاطر:
يعمل القائمون على إدارة المخاطر في تلك المرحلة على تحديد التهديدات المحتملة سواء في الوقت الحالي أو في المستقبل، كما أن هذه المرحلة تتطلب معرفة وتحديد بيانات وبرامج وأجهزة المنظمة.

2- الحماية من المخاطر:
تستهدف هذه المرحلة حماية البيانات والبرامج والأجهزة الخاصة بالمنظمة، وذلك من خلال تطبيق وسائل الحماية من أبرزها استخدام برامج مكافحة الفيروسات.

3- كشف المخاطر
تتطلب هذه المرحلة الكشف عن المخاطر المحتملة عبر تنفيذ أنظمة رصد التهديدات الإلكترونية.

4- الاستجابة للمخاطر:
عقب الانتهاء من مرحلة رصد المخاطر تأتي مرحلة الاستجابة والتي تُطبق فيها استراتيجيات بالاستجابة للمخاطر والتي تتضمن الاتصال والتعافي والاستجابة للتهديدات.

5- التعافي من المخاطر:
العودة إلى الوضع الافتراضي قبل التعرض للتهديدات الإلكترونية هو ما تتطلبه هذه المرحلة من أجل سير العمل من جديد، كما أنها خطوة تستهدف الحد من حوادث الهجوم الإلكتروني فيما بعد من خلال تطوير البرامج الخاصة بالأمن السيبراني.

خطوات تقييم المخاطر السيبرانية

الخطوة الأولى: تحديد قيمة المعلومات

لا يمكنك حماية ما لا تعرفه، فالمهمة الأولى هي تحديد البيانات ومعرفة البنية التحتية التي تمتلكها وقيمة هذه البيانات. يساعد تلخيص هذه المعلومات في فهم المخاطر التي تواجه فرق الأمان لتحديد أفضل الممارسات لتجنب المخاطر.

الخطوة الثانية: تحديد أولويات الأصول

بعد تحديد الأصول وتقييم المخاطر، سيسمح لك بتحديد أولويات الأصول التي يجب تقييمها، بالتالي تحتاج إلى العمل مع رجال الأعمال والإدارة لإنشاء قائمة جرد الأصول، حيث إنها طريقة أفضل لتصور مسارات الترابط بين الأصول والعمليات هناك بعض التهديدات التي ستكون في كل تقييم للمخاطر، وتشمل أنواع التهديدات الشائعة الوصول غير المصرح به أو إساءة استخدام المعلومات أو تسرب البيانات.

الخطوة الثالثة: تحليل التاثير

يشير إلى الضرر الذي يلحق بالمنظمة نتيجة التهديد باستغلال ثغرة أمنية، لذلك يجب أن تتوفر لديك ضوابط أمان قوية لتكنولوجيا المعلومات بما في ذلك النسخ الاحتياطي للبيانات ووضع كلمات المرور وما إلى ذلك.

الخطوة الرابعة: تحديد نقاط الضعف

الثغرة الأمنية هي تهديد يمكن استغلاله لإلحاق الضرر بمنظمتك أو سرقة بياناتها وتم العثور عليها من خلال تحليل نقاط الضعف وتقارير البائعين وتحليل الأمان.

الخطوة الخامسة: تحليل الضوابط

يجب أن تحدد الآن احتمالية الاستغلال مع الأخذ في الاعتبار بيئة المؤسسة المعمول بها، حيث يمكنك تحليل الضوابط الموجودة لتقليل الضعف أو تنفيذ الضوابط من خلال التشفير أو آليات كشف التسلل أو المصادقة الثنائية.
تحاول الضوابط الوقائية تطبيق التشفير أو مكافحة الفيروسات أو المراقبة الأمنية المستمرة، وتحاول الضوابط الاستقصائية اكتشاف وقت حدوث هجوم مثل الكشف المستمر عن البيانات.

أهمية المخاطر الأمنية والامتثال

تحقق المخاطر الأمنية والامتثال العديد من الفوائد الهامة للمؤسسات والتي تشمل ما يلي:

- التخفيف من المخاطر المرتبطة بالأعمال وخاصةً المخاطر التجارية، إلى تجنب تبعاتها.
- حماية المؤسسات من التعرض لخسائر مالية والمشكلات القانونية والإضرار بالسمعة، وذلك من خلال حماية بياناتها وبرامجها وأجهزتها.
- توفير الحماية من التعرض للمسائلات القانونية بسبب الإخلال باللوائح وعدم الامتثال للقوانين.
- تضمن للمؤسسات توفير المتطلبات القانونية والتنظيمية للشركاء والعملاء الذين يلتزمون باللوائح.

معهد العراب العالي للتدريب

مراجعة سريعة

2023

النهاية

سؤال و إجابة

1- من خطوات إدارة مخاطر الامن السيبرانى

A. تحديد الاصول

B. تحديد المخاطر

2- ما يقع ضرر امنى

A. مخاطر الامن السيبرانى

B. تهديدات الامن السيبرانى

معهد العراب العالي للتدريب

شكرا

حماية البرامج والبيانات

- البيانات: مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو أو التسجيلات الصوتيه أو الرموز التعبيرية
- الوصول للبيانات: القدرة على الوصول المنطقى والمادي الى البيانات والموارد التقنية للجهة لغرض استخدامها
- توفر البيانات: ضمان إمكانية الوصول المناسب والموثق للبيانات واستخدامها عند الحاجة
- سرية البيانات: الحفاظ على القيود المصرح بها للوصول للبيانات او الافصاح عنها
- سلامة البيانات: حماية البيانات من أي تعديلات او إتلاف غير مصرح به
- مستخدم البيانات: اي شخص يمنح صلاحية الوصول الى البيانات بغرض الاطلاع عليها او استخدامها او تحديثها وفقًا لمهام مصرح بها من قبل ممثل البيانات

❖ الحقوق المكفولة لأصحاب البيانات الشخصية وفقاً لنظام حماية البيانات الشخصية

الحق في العلم

ويشمل معرفة المسوغ النظامي أو العملي لمعالجة البيانات

الحق في الوصول إلى البيانات الشخصية

ويشمل الاطلاع عليها والحصول على نسخة منها دون مقابل مادي.

الحق في طلب تصحيح البيانات الشخصية

يحق لصاحب البيانات الشخصية أن يطلب تصحيح بياناته الشخصية التي يرى أنها غير دقيقة أو غير صحيحة أو غير مكتملة.

الحق في إتلاف البيانات الشخصية

يحق لصاحب البيانات الشخصية أن يطلب إتلاف بياناته الشخصية وفق ما نص عليه النظام.

قوانين جرائم الحاسب الآلي والإجراءات الشرعية

.

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

المساعدة على تحقيق الأمن المعلوماتي

حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية

حماية المصلحة العامة ، والأخلاق، والآداب العامة.

حماية الاقتصاد الوطني.

❖ يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1. الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية ، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات ، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

❖ يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1. التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.

❖ يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1. الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
2. إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
3. إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

❖ يعاقب كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيّ من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

الرقمية

❖ تاريخ التحول الرقمي

يبدأ التاريخ الطويل للتحول الرقمي بأول أجهزة كمبيوتر، والتي حولت الملاحظات المكتوبة بخط اليد إلى معلومات محوسبة يمكن معالجتها وتحليلها ومشاركتها. ومع ظهور الشبكات والإنترنت، أصبحت هذه القدرات متقدمة ومجموعات البيانات كبيرة للغاية. تتطلب البيانات الكبيرة عمليات إدارة وتحليل بيانات رقمية أكثر قوة، مدعومة من مراكز البيانات ومستودعات البيانات وحاليًا بحيرات البيانات.

كان تطوير السحابة في جزء منه استجابة لكميات ضخمة بشكل متزايد من البيانات والحاجة إلى قدرات توسعة دائمة لإدارة هذه البيانات وتحليلها ومعالجتها. IoT، تقدم الذكاء الاصطناعي والتعلم الآلي خيارات تقنية أكثر تطورًا للمؤسسات التي تسعى إلى تحويل عملياتها لتحقيق نتائج أفضل. الواقع الافتراضي والمعزز، جنبا إلى جنب مع التقنيات القائمة على تحليلات الفيديو، هي جزء من مزيج من القدرات المبتكرة التي تسهم في التحول الرقمي على نطاق واسع.

لماذا نتحوّل إلى التكنولوجيا الرقمية؟

لتحسين المصداقية

زد من مصداقيتك، أو مصداقية مؤسستك، من خلال مشاركة السجلات الرقمية المصادق عليها أو إصدارها أوتلقيها بثقة.

لتعزيز السرّية

قم بإصدار وإدارة ومشاركة بيانات الاعتماد الأكاديمية الرقمية التي تم التحقق منها باستخدام تقنية بلوك

مشاركة أوراق الاعتماد بكفاءة

تخلص من وقت الانتظار الممل من خلال مشاركة مستنداتك المعتمدة خلال ثوانٍ، دون الحاجة إلى الاتصالبالجهة المصدرة، وفي أي وقت من اليوم.

وفّر أكثر، واهدر أقل

خفّض التكاليف الإدارية بنسبة تزيد عن 83% من خلال الاستغناء عن الأوراق والمساهمة في مستقبل أكثراستدامة.

مزايا للأشياء الرقمية

❖ زيادة التنافسية في العمل

-ستعمل التكنولوجيا على زيادة المرونة والكفاءة والإنتاجية في العمل، وكلما تبنت الشركة تقنيات جديدة كلما زادت صداراتها في السوق، فيصبح هناك تنافس أكبر بين الشركات.

❖ زيادة إنتاجية الموظفين

-بحيث يصبح الوصول إلى المعلومات أسهل، مثل استخدام برامج المحاسبة والبرامج المكتبية، مما يمنحهم القدرة على تحقيق إمكاناتهم،

❖ خدمة العملاء بشكل أفضل

-تتيح عمليات التحول الرقمي تلبية احتياجات العملاء بشكل أفضل، مثل استخدام مواقع وتطبيقات الويب للشراء، فيسهل على العملاء التجربة مع منصات الشركة الرقمية، وخدمتهم بشكل أسهل.

❖ سهولة الدخول إلى المعلومات

-يساعد التحول الرقمي على الحصول على المعلومات بسهولة ويسر، فمن الممكن الوصول إلى الكتب، والأفلام، وغيرها بدون متاعب، فقط من خلالى الإنترنت.

معهد العراب العالي للتدريب

مراجعة سريعة

2023

النـهايـة

سؤال و إجابة

1- من الحقوق المكفولة لأصحاب البيانات

A. الحق في اتلاف البيانات
B. الحق في الوصول
C. الاثنان

2- من اهداف الامن السيبرانى

A. السرية
B. النزاهة
C. الاثنان

معهد العراب العالي للتدريب

شكرا