Kingdom of Saudi Arabia
Technical and Vocational Training Corporation
College of Telecom & Information
Department of Computer & Information

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

المملكة العربية السعودية
التقني والمهني المؤسسة العامة للتدريب
كلية الاتصالات والمعلومات بالرياض
قسم الحاسب والمعلومات

ترجمة

الأخلاقيات في تكنولوجيا المعلومات

الفصل الثالث

الهجمات السيبرانية والأمن السيبراني

جورج رينولدز

أهـداف التـعلم:

1. لماذا تنتشر هجمات الكمبيوتر إلى هذا الحد، وما أثارها؟
2. ما الذي يمكن فعله لتنفيذ برنامج أمني قوي لمنع الهجمات الإلكترونية؟
3. ما هي الإجراءات التي يجب اتخاذها في حالة نجاح الاختراق الأمني؟

توضيح التهديد:

يعد أمن البيانات وأنظمة المعلومات المستخدمة في الأعمال أمرًا في غاية الأهمية.

ملحوظة :يجب أن تكون بيانات العمل سرية ومعلومات العملاء والموظفين الخاصة مصونة، ويجب حماية الأنظمة من أعمال السرقة أو التعطيل الخبيثة.

ومع ذلك، فإن اتخاذ القرارات المتعلقة بأمن تكنولوجيا المعلومات ينطوي على تقييم المقايضات المعقدة على الرغم من أن الحاجة إلى الأمان واضحة، إلا أنه يجب في كثير من الأحيان موازنتها مع احتياجات العمل الأخرى.

يواجه مديرو الأعمال ومحترفو تكنولوجيا المعلومات ومستخدمو تكنولوجيا المعلومات عددًا من المقايضات المعقدة عند اتخاذ القرارات المتعلقة بأمن تكنولوجيا المعلومات، مثل ما يلي:

- ما مقدار الجهد والمال الذي ينبغي إنفاقه للحماية من جرائم الالكترونية ؟ وبعبارة أخرى، ما مدى الأمان الذي يعتبر آمنًا بدرجة كافية؟
- ما الذي يجب فعله إذا كانت ضمانات أمن تكنولوجيا المعلومات الموصى بها تجعل ممارسة الأعمال أكثر صعوبة للعملاء والموظفين، مما يؤدي إلى خسارة المبيعات وزيادة التكاليف؟

- إذا كانت إحدى الشركات ضحية لجريمة إلكترونية، فهل ينبغي عليها متابعة المجرمين قضائيًا، أو الابتعاد عن الأضواء لتجنب الدعاية السلبية، أو إبلاغ العملاء المتأثرين، أو اتخاذ بعض الإجراءات الأخرى؟

لماذا الهجمات الإلكترونية منتشرة إلى هذا الحد؟

الجزء الأول

- زيادة التعقيد تزيد من الضعف، ومع إضافة المزيد من الأجهزة، يزداد عدد نقاط الدخول إلى الشبكة، مما يزيد من المخاطر الأمنية.
- يؤدي توسيع الأنظمة وتغييرها إلى ظهور مخاطر جديدة: يجب على مؤسسات تكنولوجيا المعلومات:

1-مواكبة التغير التكنولوجي.

2-إجراء تقييمات أمنية مستمرة.

3-تنفيذ أساليب التعامل مع المخاطر الجديدة.

الجزء الثاني

- تزايد الاعتماد على البرامج التجارية ذات نقاط الضعف المعروفة:

1-يستغل: هجوم على نظام معلومات يستغل ثغرة أمنية معينة في النظام.

2-هجوم اليوم صفر: يحدث قبل أن يصبح مجتمع الأمان أو مطور البرامج على علم بذلك وإصلاح ثغرة أمنية.

- زيادة تطور أولئك الذين قد يلحقون الأذى وزيادة تعقيد الحوسبة، وتوسيع الأنظمة وتغييرها، وزيادة انتشار سياسات إحضار جهازك الخاص (BYOD)، والاعتماد المتزايد على البرامج ذات نقاط

الضعف المعروفة، والتطور المتزايد لأولئك الذين قد يلحقون الضرر com.mcause زيادة كبيرة في عدد وتنوع وشدة الحوادث الأمنية.

تصنيف مرتكبي الجرائم الحاسوبية

اليوم يعد التهديد الحاسوبي الخاص هو أفضل تنظيمًا وقد يكون جزءًا من مجموعة منظمة على سبيل المثال:

Anonymous) Lizard Squad, Chaos Computer Club,

، فريق تسلا وفرق القرصنة الذي ترعاها الحكومات الوطنية (والتي لديها أجندة وتستهدف منظمات ومواقع ويب محددة، وتمتلك بعض هذه المجموعات موارد وافرة، بما في ذلك الأموال والأدوات المتطورة لدعم جهودها. اليوم يتمتع مهاجم الكمبيوتر لديك بقدر أكبر من المعرفة والخبرة في الالتفاف حول ضمانات أمان الكمبيوتر والشبكات. يلخص الجدول ادناه

الوصف	نوع مرتكب الجريمة
شخص ينتهك أمن الكمبيوتر أو الإنترنت بشكل ضار أو لتحقيق مكاسب شخصية غير قانونية	قرصنة القبعة السوداء
الشخص الذي يسبب المشاكل ويسرق البيانات ويفسد الأنظمة	العابث
موظف أو مقاول يحاول تحقيق مكاسب مالية و/أو تعطيل أنظمة معلومات الشركة	برامج خبيثة داخلية
الفرد الذي يلتقط الأسرار التجارية للحصول على ميزة تنافسية غير عادلة	جاسوس صناعي
شخص يهاجم نظام الكمبيوتر لتحقيق مكاسب مالية	مجرم إلكتروني
فرد هدفه هو تعزيز أيديولوجية سياسية	هاكر ناشط
شخص يحاول تدمير البنية التحتية الحكومية والمؤسسات المالية وغيرها الشركات والمرافق ووحدات الاستجابة للطوارئ	إرهابي الإنترنت

أنواع مرتكبي الأذى والجريمة والأضرار الحاسوبية.

أنواع الثغرات ومصادر التهديدات السيبرانية

الجزء الأول

هناك أنواع عديدة من الهجمات الحاسوبية، ويتم اختراع أنواع جديدة منها طوال الوقت مثل:

1- برامج الفدية: البرامج الضارة التي تمنعك من استخدام جهاز الكمبيوتر الخاص بك أو الوصول إلى بياناتك حتى تلبي متطلبات معينة، مثل دفع فدية.
2- فايروس: قطعة من تعليمات برمجية متخفية في هيئة شيء آخر، تجعل الكمبيوتر يتصرف بطريقة غير متوقعة وغير مرغوب فيها عادةً.
3- دُودَة: برنامج ضار موجود في الذاكرة النشطة للكمبيوتر ويكرر نفسه.
4- حصان طروادة: برنامج يتم فيه إخفاء تعليمات برمجية ضارة داخل برنامج يبدو غير ضار.
5- قنبلة المنطق: يتم تنفيذه عند تشغيله بواسطة حدث معين.
6- التهديد المختلط: هجوم يجمع بين ميزات الفيروسات والديدان وحصان طروادة وغيرها من التعليمات البرمجية الضارة في حمولة واحدة.

الجزء الثاني

هناك أنواع عديدة من الهجمات الحاسوبية، ويتم اختراع أنواع جديدة منها طوال الوقت مثل:

1- رسائل إلكترونية مزعجة: استخدام أنظمة البريد الإلكتروني لإرسال بريد إلكتروني غير مرغوب فيه إلى أعداد كبيرة من الأشخاص.

2- قانون مكافحة الاعتداء على المواد الإباحية والتسويق غير المرغوب فيه (CAN-SPAM):يجعل البريد العشوائي قانونيًا مع بعض القيود - يجب أن يتضمن البريد الإلكتروني ما يلي: عنوان إرجاع حقيقي، وعلامة تحدد أنه إعلان أو طلب، وطريقة للمستلمين لإلغاء الاشتراك في رسائل البريد الإلكتروني المستقبلية.

3- (CAPTCHA) اختبار تورينج العام الآلي بالكامل للتمييز بين أجهزة الكمبيوتر والبشر: برنامج يقوم بإنشاء وتصنيف الاختبارات التي يمكن للبشر اجتيازها ولكن برامج الكمبيوتر لا تستطيع ذلك.

الجزء الثالث

هناك أنواع عديدة من الهجمات الحاسوبية، ويتم اختراع أنواع جديدة منها طوال الوقت مثل:

1- هجوم حجب الخدمة الموزعة (DDoS): هجوم يسيطر على أجهزة الكمبيوتر عبر الإنترنت، مما يؤدي إلى إغراق الموقع المستهدف بالطلبات على البيانات والمهام الصغيرة الأخرى.

2- الجذور الخفية: مجموعة من البرامج التي تمكن مستخدمها من الوصول إلى مستوى المسؤول إلى جهاز كمبيوتر دون موافقة المستخدم النهائي أو علمه.

3- التهديد المستمر المتقدم (APT):هجوم يتمكن من خلاله أحد المتسللين من الوصول إلى الشبكة والبقاء هناك - دون أن يتم اكتشافه - بهدف سرقة البيانات على مدار فترة أسابيع أو أشهر.

الجزء الرابع

هناك أنواع عديدة من الهجمات الحاسوبية، ويتم اختراع أنواع جديدة منها طوال الوقت مثل:

1- التصيد الاحتيالي: عملية استخدام البريد الإلكتروني بشكل احتيالي لمحاولة إقناع المستلم بالكشف عن بياناته الشخصية.
2- التصيد بالحربة: نوع مختلف من التصيد الاحتيالي حيث يرسل المخادع رسائل بريد إلكتروني احتيالية إلى موظفي المؤسسة.
3- التصيد الاحتيالي عبر الهاتف: أحد أشكال التصيد الاحتيالي حيث يتلقى الضحايا رسالة نصية ذات مظهر شرعي تطلب منهم الاتصال برقم هاتف محدد أو تسجيل الدخول إلى موقع ويب.
4- التصيد الاحتيالي: نوع مختلف من التصيد الاحتيالي حيث يتلقى الضحايا رسالة بريد صوتي تطلب منهم الاتصال برقم هاتف أو الوصول إلى موقع ويب.

الجزء الخامس

هناك أنواع عديدة من الهجمات الحاسوبية، ويتم اختراع أنواع جديدة منها طوال الوقت مثل:

1- التجسس الإلكتروني: نشر البرامج الضارة التي تسرق البيانات من الوكالات الحكومية، أو المقاولين العسكريين أو المنظمات السياسية أو شركات التصنيع.

2- الإرهاب الإليكتروني: ترهيب الحكومة أو السكان المدنيين باستخدام تكنولوجيا المعلومات لتعطيل البنية التحتية الوطنية الحيوية.

- وزارة الأمن الداخلي (DHS): وكالة فيدرالية هدفها توفير أمريكا أكثر أمانًا ومرونة ضد الإرهاب والتهديدات المحتملة الأخرى.
- فريق الاستعداد لطوارئ الكمبيوتر الأمريكي (US-CERT): شراكة بين وزارة الأمن الوطني والقطاع العام/الخاص؛ US-CERT مسؤول عن تحليل وتقليل التهديدات السيبرانية ونقاط الضعف ونشر معلومات التحذير من التهديدات السيبرانية وتنسيق أنشطة الاستجابة للحوادث.

القوانين الفيدرالية لملاحقة هجمات الكمبيوتر

(خاص بالولايات المتحدة)

على مر السنين تم سن العديد من القوانين للمساعدة في ملاحقة المسؤولين عن الجرائم المتعلقة بالكمبيوتر، وتتلخص هذه القوانين في التالي:

1-قانون الاحتيال وإساءة استخدام الكمبيوتر:

- يتناول الاحتيال والأنشطة ذات الصلة المرتبطة بأجهزة الكمبيوتر، بما في ذلك:
  - الوصول إلى جهاز كمبيوتر دون تصريح.
  - نقل التعليمات البرمجية التي تسبب ضررا لجهاز الكمبيوتر.
  - الاتجار بكلمات مرور الكمبيوتر.
  - التهديد بإحداث ضرر لجهاز كمبيوتر محمي.

2-الاحتيال والأنشطة ذات الصلة فيما يتعلق بالوصول للنظام الأساسي للأجهزة.

يغطي المطالبات الكاذبة المتعلقة بالاستخدام غير المصرح به لبطاقات الائتمان.

3-قوانين الوصول إلى الاتصالات السلكية والإلكترونية وسجلات المعاملات المخزنة.

يركز على الوصول غير القانوني إلى الاتصالات المخزنة للحصول على أو تغيير أو منع الوصول المصرح به إلى الاتصالات السلكية أو الإلكترونية أثناء وجودها في المخزن الإلكتروني.

4-الولايات المتحدة الأمريكية قانون باتريوت.

تعريف الإرهاب السيبراني والعقوبات المرتبطة به.

الثالوث الأمني CIA لحماية الفضاء الرقمي (السيبراني)

تركز ممارسات أمن تكنولوجيا المعلومات للمؤسسات في جميع أنحاء العالم على ممارسة تستهدف CIA: ضمان السرية والحفاظ على نظام المعلومات البيئي وضمان توافر الأنظمة والبيانات.

الثالوث الأمني CIA: سرية وسلامة وتوفر الأنظمة والبيانات

تركز ممارسات أمن تكنولوجيا المعلومات على ثالوث أمان وكالة المخابرات المركزية:

- سرية يضمن أن الأفراد الذين يتمتعون بالسلطة المناسبة فقط هم من يمكنهم الوصول إلى البيانات الحساسة، مثل: البيانات الشخصية للموظفين، وبيانات مبيعات العملاء والمنتجات، والمنتجات الجديدة والخطط الإعلانية.

- نزاهة يضمن أنه لا يمكن تغيير البيانات إلا من قبل المستخدمين المصرح لهم، بحيث يتم ضمان دقة البيانات واتساقها ومصداقيتها.
- التوفر يضمن إمكانية الوصول إلى البيانات متى وأينما دعت الحاجة، بما في ذلك خلال أوقات العمليات العادية وعمليات التعافي من الكوارث.

يُعرف معيار التوفر المنتشر على نطاق واسع ولكن يصعب تحقيقه لنظام أو منتج باسم"خمسة 9S " أو توفر 99.999 بالمائة. بالنسبة للعملية التي تستمر 365 يومًا في السنة، 24 ساعة في اليوم، فإن هذا يترجم إلى أقل من ساعة واحدة من عدم التوفر سنويًا.

لا يمكن لأي منظمة أن تكون مؤمنة بشكل كامل من أي هجوم. إن مفتاح منع وقوع حادث يتعلق بأمن الكمبيوتر هو تنفيذ حل أمني متعدد الطبقات لجعل عمليات اقتحام الكمبيوتر صعبة للغاية بحيث يستسلم المهاجم في النهاية أو يتم اكتشافه قبل إلحاق الكثير من الضرر.

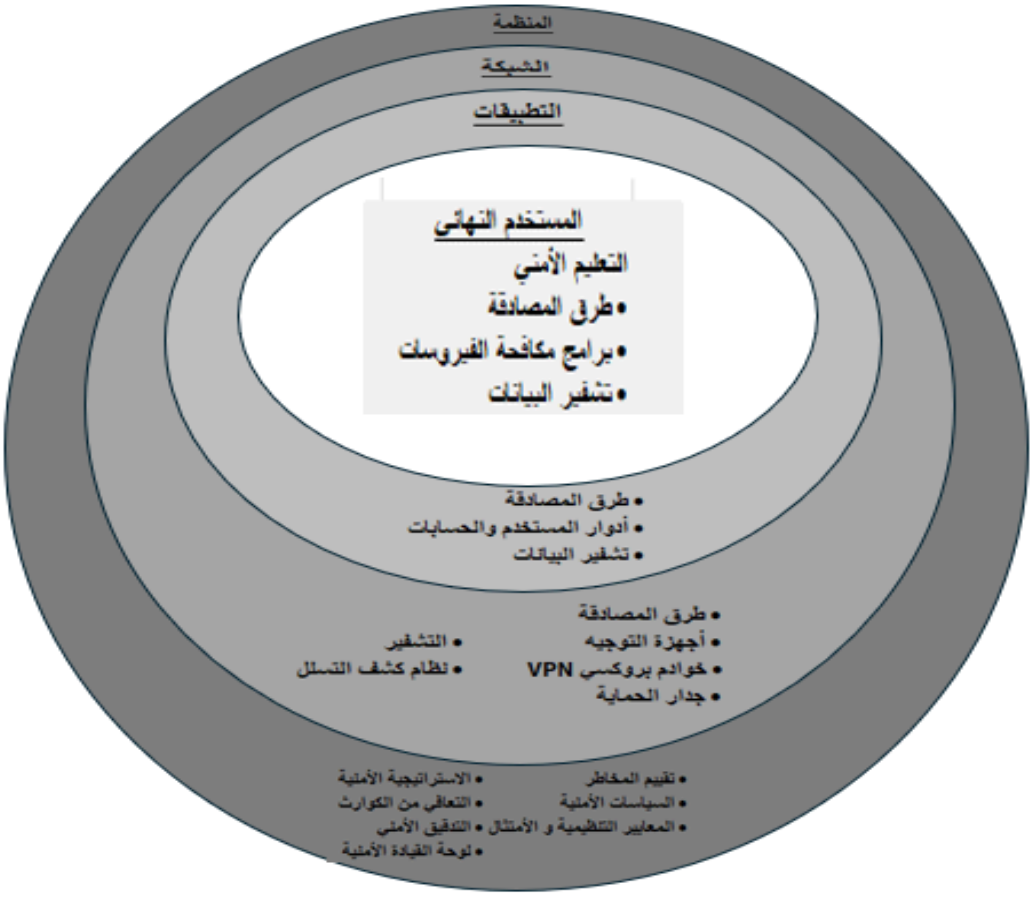
تنفيذ أمان CIA في الفضاء الرقمي (السيبراني)

يجب تنفيذ أمان CIA على مستوى المنظمة والشبكة والتطبيقات والمستخدم النهائي

في حل متعدد الطبقات، إذا انكسر المهاجم ومن خلال طبقة واحدة من الأمان، يجب بعد ذلك التغلب على طبقة أخرى. تدابير أمنية

يجب التخطيط لها وتصميمها وتنفيذها واختبارها وصيانتها في المنظمة، مستويات الشبكة والتطبيقات والمستخدم النهائي لتحقيق أمان CIA الحقيقي

(انظرالشكل) يتم شرح طبقات التدابير الوقائية هذه بمزيد من التفصيل في الأقسام التالية.



تنفيذ CIA على مستوى المنظمة

يتطلب تنفيذ وكالة المخابرات المركزية استراتيجية أمنية قائمة على المخاطر مع عملية إدارة نشطة وخطة واضحة المعالم للتعافي من الكوارث.

يبدأ تنفيذ CIA على مستوى المؤسسة بتعريف استراتيجية أمنية شاملة، وأداء تقييم المخاطر، ووضع خطط للتعافي من الكوارث، ووضع سياسات أمنية، وإجراء عمليات تدقيق أمنية، وضمان الامتثال للمعايير التنظيمية، وإنشاء لوحة معلومات أمنية.

إن إكمال هذه المهام على المستوى التنظيمي سيضع أساسًا سليمًا واتجاهًا واضحًا للإجراءات المستقبلية المتعلقة بوكالة المخابرات المركزية.

تقييم المخاطر

تقييم المخاطر:عملية تقييم المخاطر المتعلقة بالأمن على أجهزة الكمبيوتر والشبكات الخاصة بالمؤسسة من التهديدات الداخلية والخارجية.

يحدد تقييم المخاطر المكتمل أكبر التهديدات التي تواجه الشركة ويساعد في تركيز الجهود الأمنية على المجالات ذات العائد الأعلى.

عملية تقييم المخاطر العامة

خطوات العملية:

1- تحديد مجموعة أصول تكنولوجيا المعلومات الأكثر أهمية.
2- تحديد أحداث الخسارة أو المخاطر / التهديدات التي يمكن ان تحدث.
3- تقييم تكرار الأحداث أو احتمالية كل تهديد محتمل.
4- تحديد تأثير كل تهديد يحدث.
5- تحديد كيفية التخفيف من كل تهديد.
6- تقييم جدوى تنفيذ خيارات التخفيف.
7- قم بإجراء تحليل التكلفة والعائد للتأكد من أن جهودك ستكون فعالة من حيث التكلفة.
8- قرر ما إذا كنت تريد تنفيذ الإجراء المضاد أم لا.

التعافي من الكوارث

خطة التعافي من الكوارث: عملية موثقة لاستعادة أصول نظام معلومات الأعمال الخاص بالمؤسسة -بما في ذلك الأجهزة والبرامج والبيانات والشبكات والمرافق - في حالة وقوع كارثة.

العمليات الحرجة للمهمة: العمليات التجارية الأكثر أهمية لاستمرار العمليات وتحقيق الأهداف من غيرها.

السياسات الأمنية والتدقيق الأمني

السياسة الأمنية: سياسة تحدد المتطلبات الأمنية للمؤسسة، بالإضافة إلى الضوابط والعقوبات اللازمة لتلبية تلك المتطلبات تحدد السياسة الأمنية الجيدة المسؤوليات والسلوك المتوقع من أعضاء المنظمة.

التدقيق الأمني: عملية تدقيق تقيم ما إذا كانت المنظمة لديها سياسة أمنية مدروسة جيدًا وما إذا كان يتم اتباعها.

أداة وقائية مهمة أخرى هي التدقيق الأمني الذي يقيم ما إذا كانت المنظمة لديها سياسة أمنية مدروسة جيدًا وما إذا كان يتم اتباعها. على سبيل المثال: إذا كانت إحدى السياسات تنص على أنه يجب على جميع المستخدمين تغيير كلمات المرور الخاصة بهم كل 30 يومًا، فيجب أن تتحقق عملية التدقيق من مدى جودة تنفيذ هذه السياسة. يجب أن تقوم عملية التدقيق أيضًا بمراجعة من يمكنه الوصول إلى أنظمة وبيانات معينة ومستوى السلطة الذي يتمتع به كل مستخدم. ليس من غير المعتاد أن تكشف عملية التدقيق أن عددًا كبيرًا جدًا من الأشخاص لديهم إمكانية الوصول إلى البيانات المهمة وأن العديد من الأشخاص لديهم قدرات تتجاوز تلك اللازمة لأداء وظائفهم. إحدى نتائج التدقيق الجيد هي قائمة العناصر التي تحتاج إلى معالجة لضمان تلبية سياسة الأمان.

يجب أن يقوم التدقيق الأمني الشامل أيضًا باختبار ضمانات النظام للتأكد من أنها تعمل على النحو المنشود. قد تتضمن مثل هذه الاختبارات تجربة كلمات مرور النظام الافتراضية التي تكون نشطة

عند استلام البرنامج لأول مرة من البائع. الهدف من هذا الاختبار هو التأكد من تغيير جميع كلمات المرور المعروفة.

ستقوم بعض المنظمات أيضًا بإجراء اختبار اختراق لشبكاتها لدفاعات. ويستلزم ذلك تكليف أفراد بمحاولة اختراق التدابير وتحديد نقاط الضعف التي لا تزال بحاجة إلى المعالجة. يتمتع الأفراد المستخدمون في هذا الاختبار بالمعرفة ومن المرجح أن يتبعوا أساليب فريدة في اختبار الإجراءات الأمنية.

الامتثال للمعايير التنظيمية (خاص بالولايات المتحدة الامريكية)

قد يُطلب من المنظمة الالتزام بالمعايير الخارجية، تشمل:

1- **قانون السرية المصرفية لعام 1970**

يتطلب من المؤسسات المالية في الولايات المتحدة مساعدة الوكالات الحكومية الأمريكية في اكتشاف ومنع غسيل الأموال.

2- **القانون الفيدرالي لإدارة أمن المعلومات**

يتطلب من كل وكالة اتحادية توفير أمن المعلومات لأنظمة البيانات والمعلومات التي تدعم عمليات الوكالة وأصولها.

3- **قانون قابلية نقل التأمين الصحي والمساءلة**

ينظم استخدام والإفصاح عن المعلومات الصحية للفرد.

لوحات المعلومات الأمنية

برنامج لوحة القيادة الأمنية

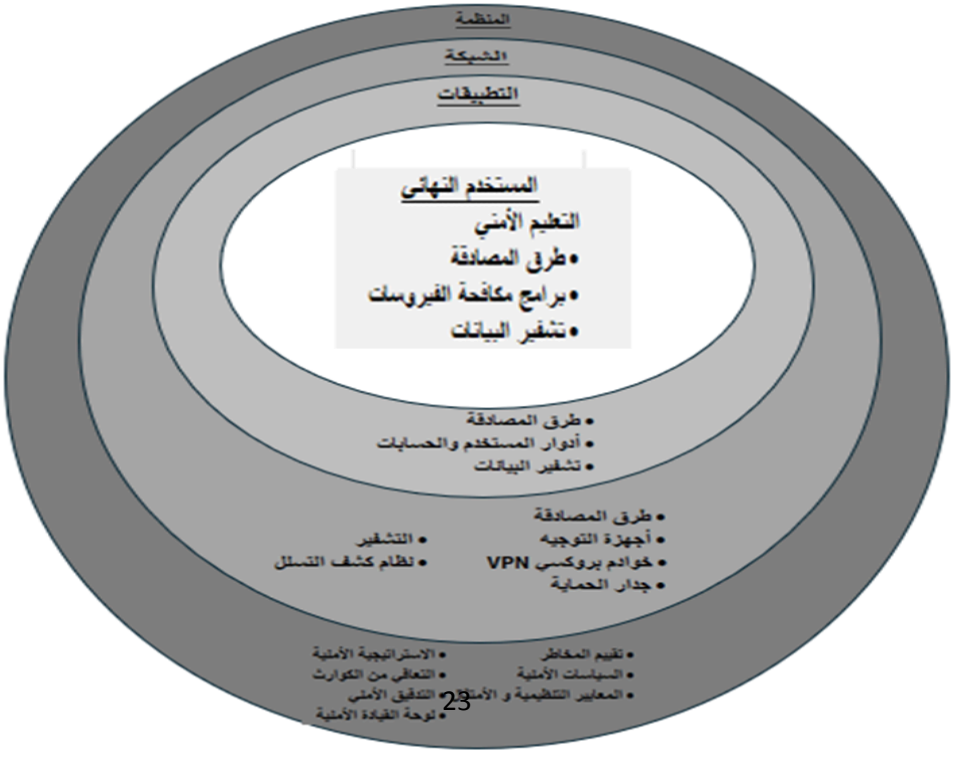
1-يوفر عرضًا شاملاً لجميع مؤشرات الأداء الرئيسية المتعلقة بالدفاعات الأمنية للمؤسسة، بما في ذلك:

- التهديدات
- التعرض
- الامتثال للسياسة
- تنبيهات الحادث

2-يقلل من الجهد المطلوب لرصد التهديدات وتحديدها والاستجابة لها.

تنفيذ CIA على مستوى الشبكة

يوفر الإنترنت مسارًا واسعًا ومفتوحًا لأي شخص في العالم للوصول إلى شبكة مؤسستك. ونتيجة لذلك، تواصل المؤسسات نقل المزيد من عملياتها التجارية إلى الإنترنت لتقديم خدمة أفضل للعملاء والموردين والموظفين والمستثمرين وشركاء الأعمال. ومع ذلك، فإن الوصول غير المصرح به إلى الشبكة من قبل متسلل أو موظف مستاء يمكن أن يؤدي إلى اختراق البيانات الحساسة وتدهور الخدمات بشدة، مع ما ينتج عنه من تأثير سلبي على الإنتاجية والقدرة التشغيلية. وهذا بدوره يمكن أن يخلق ضغطًا شديدًا على العلاقات مع العملاء والموردين والموظفين والمستثمرين وشركاء الأعمال، الذين قد يشككون في قدرة المنظمة على حماية معلوماتها السرية وتقديم خدمات موثوقة. يجب على المؤسسات إدارة أمان شبكاتها بعناية وتنفيذ إجراءات قوية لضمان عدم إمكانية الوصول إلى البيانات الحساسة لأي شخص غير مصرح له برؤيتها.



طرق المصادقة

- يجب على المؤسسة مصادقة المستخدمين الذين يحاولون الوصول إلى شبكتها
  - اسم المستخدم و كلمة السر
  - البطاقة الذكية ورقم التعريف الشخصي
  - بصمة
  - عينة من نمط الصوت
  - مسح شبكية العين
- تتضمن أنظمة المصادقة متعددة العوامل ما يلي:

1- القياسات الحيوية.

2- كلمات المرور لمرة واحدة.

3- الرموز المميزة للأجهزة التي يتم توصيلها بمنفذ USB وإنشاء كلمة مرور.

جدران الحماية وأجهزة التوجية

جدار الحماية :نظام من البرامج أو الأجهزة التي تعمل كحارس بين الشبكة الداخلية للمؤسسة والإنترنت.

جدار الحماية من الجيل التالي (NGFW) :نظام أمان شبكة يعتمد على الأجهزة أو البرامج، ويعمل على منع الهجمات عن طريق تصفية حركة مرور الشبكة بناءً على محتويات الحزمة.

جهاز التوجيه: جهاز شبكة يربط شبكات متعددة وينقل حزم البيانات بين الشبكات يسمح لك بـ:

- القيام بإنشاء شبكة آمنة عن طريق تعيين كلمة مرور لها.
- حدد عنوانًا فريدًا للتحكم في الوصول إلى الوسائط (MAC) لكل جهاز شرعي متصل بالشبكة ومنع الوصول بواسطة أي جهاز آخر.

التشفير

التشفير: عملية تشفير الرسائل أو البيانات بطريقة لا يمكن قراءتها إلا للأطراف المصرح لها بذلك.

مفتاح التشفير: قيمة يتم تطبيقها على النص غير المشفر لإنتاج نص مشفر لا يمكن قراءته بواسطة أولئك الذين ليس لديهم مفتاح التشفير

- هناك نوعان من خوارزميات التشفير:

1- متماثل.

2- غير متماثل.

أمان طبقة النقل (TLS): بروتوكول اتصالات يضمن الخصوصية بين تطبيقات الاتصال ومستخدميها على الإنترنت.

يمكّن TLS العميل على سبيل المثال، متصفح الويب من بدء محادثة خاصة مؤقتة مع الخادم.

خوادم البروكسي والشبكات الخاصة الافتراضية

خادم البروكسي :يعمل كوسيط بين متصفح الويب وخادم آخر على الإنترنت

تقوم بإدخال عنوان URL لموقع ويب في متصفحك.

تتم إعادة توجيه الطلب إلى الخادم الوكيل، الذي ينقل الطلب إلى الخادم الذي يستضيف موقع الويب.

يتم إرجاع صفحة الويب إلى الخادم الوكيل، الذي يقوم بعد ذلك بتمريرها إليك.

النتيجة: يرى موقع الويب أن الخادم الوكيل هو الخادم الفعلي زائر وليس أنت

الشبكة الخاصة الافتراضية (VPN):تمكن المستخدمين عن بعد من الوصول بشكل آمن إلى موارد الحوسبة الخاصة بالمؤسسة ومشاركة البيانات عن طريق إرسال واستقبال البيانات المشفرة عبر الشبكات العامة، مثل الإنترنت.

نظام كشف التسلل

نظام كشف التسلل (IDS): البرامج أو الأجهزة التي تراقب موارد النظام وأنشطته وتصدر تنبيهًا عندما تكتشف حركة مرور الشبكة التي تحاول التحايل على الإجراءات الأمنية

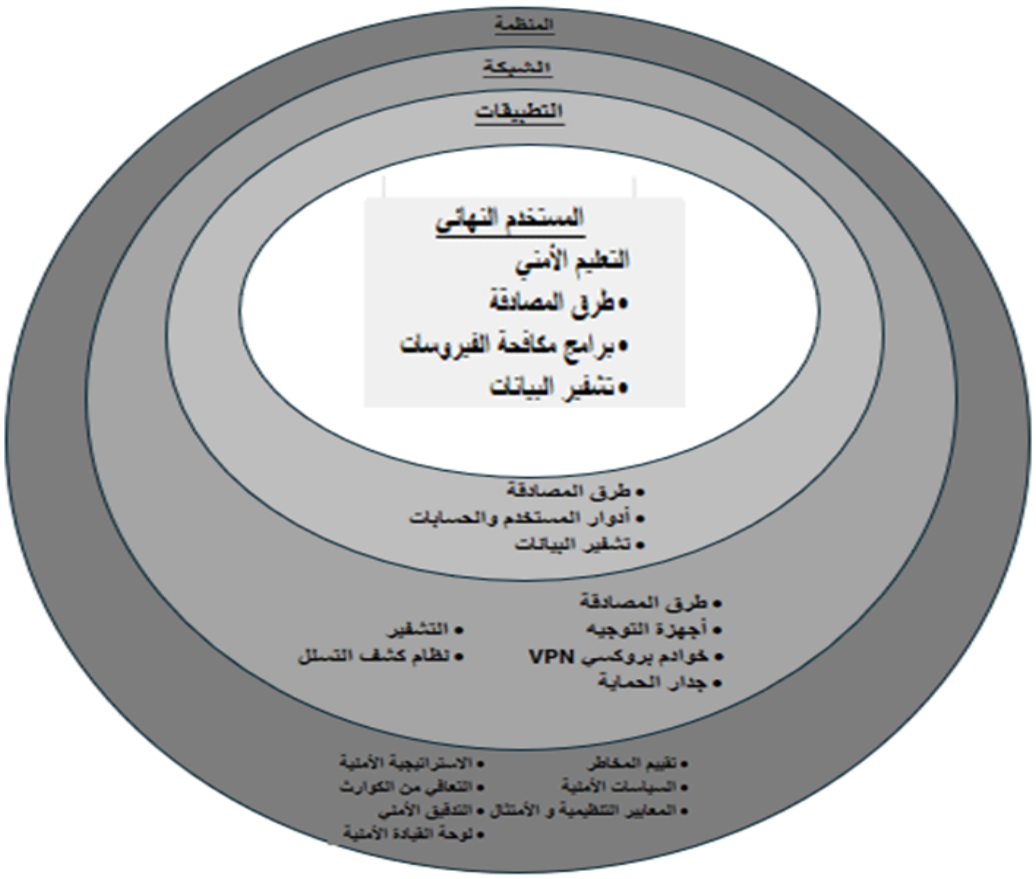
طريقتان لكشف التسلل:

1- مستند إلى المعرفة: يحتوي على معلومات حول هجمات محددة ونقاط ضعف النظام ويراقب محاولات استغلال هذه الثغرات الأمنية على سبيل المثال، محاولات تسجيل الدخول الفاشلة المتكررة.

2- يعتمد على السلوك: نماذج السلوك الطبيعي للنظام ومستخدميه بناءً على المعلومات المرجعية؛ يقارن النشاط الحالي بهذا النموذج، ويبحث عن الانحرافات على سبيل المثال، حركة المرور غير العادية في الساعات الفردية.

تنفيذ CIA على مستوى التطبيق

تعد طرق المصادقة وأدوار المستخدم وحساباته وتشفير البيانات من العناصر الأساسية لطبقة أمان التطبيق. ويجب أن تكون هذه العناصر موجودة للتأكد من أنها مسموحة فقط المستخدمين لديهم حق الوصول إلى المنظمة والتطبيقات والبيانات وأن الوصول إليها هو يقتصر على الإجراءات التي تتفق مع أدوارهم ومسؤولياتهم المحددة.



- **طرق المصادقة:**

1- عامل واحد: يتطلب بيانات اعتماد واحدة فقط على سبيل المثال، كلمة المرور.

2- عامل ثنائي: يتطلب نوعين من بيانات الاعتماد على سبيل المثال، البطاقة المصرفية والرقم السري.

- **أدوار المستخدم والحسابات:**

يستخدم لمنح المستخدمين السلطة لأداء مسؤولياتهم داخل التطبيق وليس أكثر.

- **تشفير البيانات:**

يحمي البيانات المستخدمة داخل التطبيق من الوصول غير المصرح به.

تنفيذ CIA على مستوى المستخدم النهائي

يجب أن يكون التثقيف الأمني وطرق المصادقة وبرامج مكافحة الفيروسات وتشفير البيانات موجودًا لحماية ما غالبًا ما يكون الحلقة الأضعف في المؤسسة والمحيط الأمني هو المستخدم النهائي.

تنفيذ CIA على مستوى المستخدم النهائي

- **التثقيف الأمني**

قم بتثقيف المستخدمين النهائيين حول أهمية الأمان حتى يتم تحفيزهم لفهم السياسات الأمنية ومتابعتها.

- **طرق المصادقة**

مطالبة المستخدمين النهائيين بتنفيذ رمز مرور الأمان الذي يجب إدخاله قبل أن تقبل أجهزتهم المزيد من الإدخال.

- **برامج مكافحة الفيروسات**

توقيع الفيروس: تسلسل محدد من البايتات يشير إلى وجود فيروس تم تحديده مسبقًا.

- **السلوك القائم**

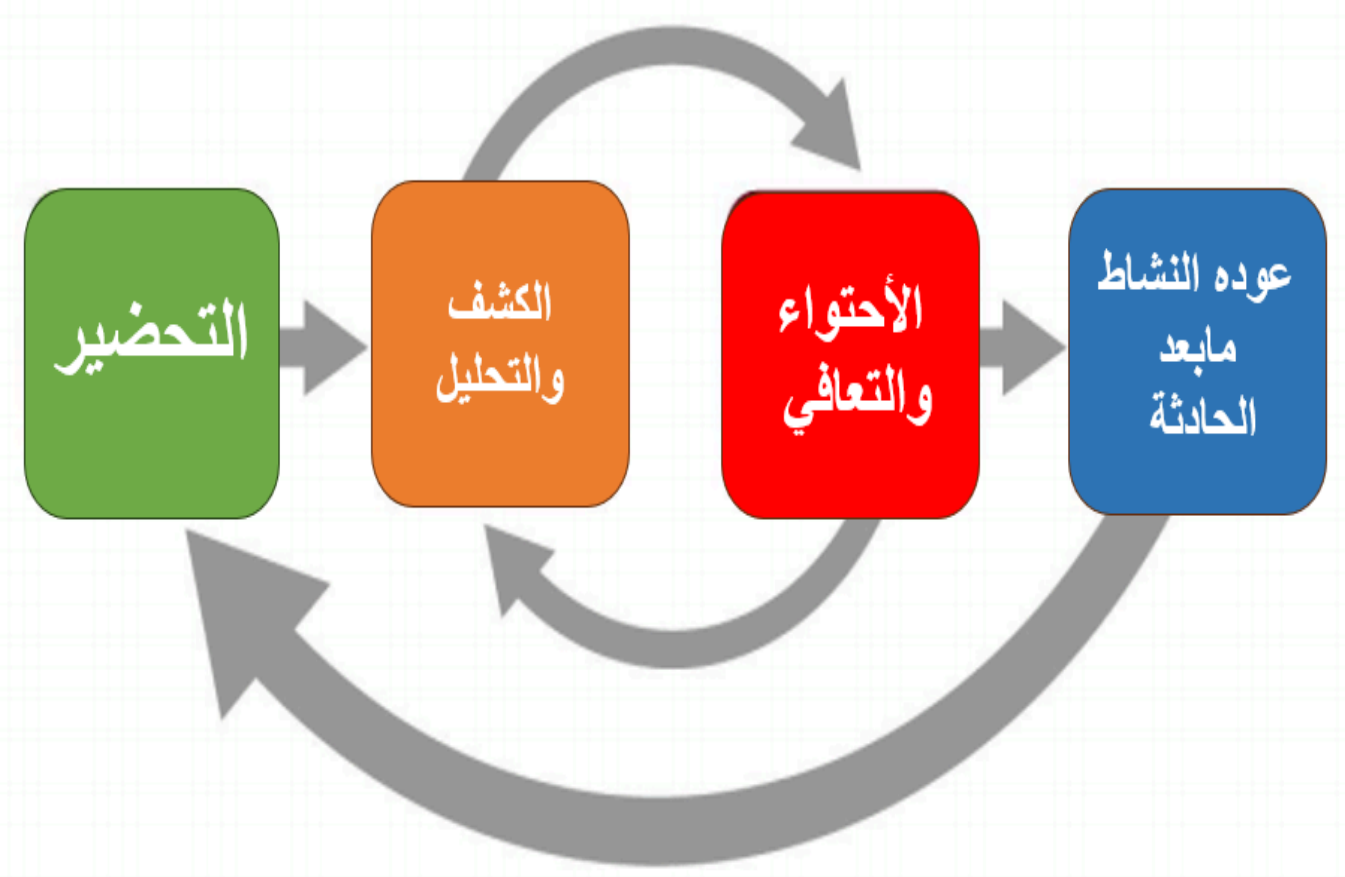
الكشف عن السلوك الضار في البرمجيات.

- **تشفير البيانات**

يعمل تشفير القرص بالكامل على حماية أجهزة التخزين أو محركات الأقراص الثابتة بحيث لا يمكن إزالتها من الكمبيوتر وتوصيلها بجهاز كمبيوتر آخر.

الرد على الهجوم السيبراني

- يجب أن تكون المنظمة مستعدة للأسوأ ، أي هجوم ناجح يهزم كل أو بعض دفاعات النظام ويلحق الضرر بأنظمة البيانات والمعلومات.
- في أي حادث أمني، يجب أن يكون الهدف الأساسي هو استعادة السيطرة والحد من الضرر، وليس محاولة مراقبة متسلل أو القبض عليه.
- تساعد خطة الاستجابة المعدة جيدًا في إبقاء الحادث تحت السيطرة الفنية والعاطفية.



الرد على الهجوم السيبراني

من أجل الرد على أي هجوم إلكتروني، هناك عناصر أساسية لأي خطة استجابة وهي:

1- إشعار الحادث.

2- حماية الأدلة وسجلات الأنشطة.

3- احتواء الحادث.

4- الاستئصال.

5- متابعة الحادث.

6- استخدام MSSP.

7- الطب الشرعي الكمبيوتر.

إشعار حادث

يتمثل أحد العناصر الأساسية في أي خطة استجابة في تحديد من يجب إبلاغه ومن لا يجب إبلاغه في حالة وقوع حادث يتعلق بأمن الكمبيوتر.

- تشمل الأسئلة التي يجب تغطيتها ما يلي:
  - داخل الشركة، من الذي يجب إعلامه، وما هي المعلومات التي يجب أن يمتلكها كل شخص؟
  - تحت أي ظروف يجب على الشركة الاتصال بالعملاء والموردين الرئيسيين؟
  - كيف تقوم الشركة بإبلاغهم بوجود خلل في العمل دون إثارة قلقهم دون داع؟
  - متى يجب الاتصال بالسلطات المحلية أو مكتب التحقيقات؟
- يوصي معظم خبراء الأمن بعدم تقديم معلومات محددة حول الاختراق في المنتديات العامة، مثل التقارير الإخبارية والمؤتمرات والاجتماعات المهنية ومجموعات المناقشة عبر الإنترنت.
- يجب أن تظل جميع الأطراف العاملة على المشكلة على اطلاع ودراية دون استخدام الأنظمة المتصلة بالنظام المخترق. وربما يقوم الدخيل بمراقبة هذه الأنظمة ورسائل البريد الإلكتروني لمعرفة ما هو معروف عن الاختراق الأمني.
- إن القرار الأخلاقي الحاسم الذي يجب اتخاذه هو ما يجب إخباره للعملاء والآخرين الذين قد تكون بياناتهم الشخصية قد تعرضت

للاختراق بسبب حادث كمبيوتر. تميل العديد من المنظمات إلى إخفاء مثل هذه المعلومات خوفًا من الدعاية السيئة وفقدان العملاء.

- ونظرًا لأن الكثيرين ينظرون إلى هذا التقاعس على أنه غير أخلاقي وضار، فقد تم إصدار عدد من قوانين هيئة الأمن السيبراني لإجبار المؤسسات على الكشف عن وقت انتهاك بيانات العملاء.

حماية الأدلة وسجلات الأنشطة

- يجب على المنظمة توثيق جميع تفاصيل الحادث الأمني أثناء عملها على حل الحادث الأمني.
- يلتقط التوثيق أدلة قيمة للمحاكمة المستقبلية ويوفر البيانات للمساعدة أثناء مراحل القضاء على الحادث ومتابعته.
- من المهم بشكل خاص التقاط جميع أحداث النظام، والإجراءات المحددة التي تم اتخاذها وجميع المحادثات الخارجية ماذا ومتى ومن في سجل ولأن هذا قد يصبح دليلاً للمحكمة، يجب على المنظمة إنشاء مجموعة من إجراءات التعامل مع المستندات باستخدام القسم القانوني كمورد.

احتواء الحادث

في كثير من الأحيان، من الضروري التصرف بسرعة لاحتواء الهجوم ومنع الوضع السيئ من أن يصبح أسوأ. يجب أن تحدد خطة الاستجابة للحوادث بوضوح عملية تحديد ما إذا كان الهجوم خطيرًا بدرجة كافية لتبرير إيقاف تشغيل الأنظمة الحيوية أو فصلها عن الشبكة إن كيفية اتخاذ مثل هذه القرارات، ومدى سرعة اتخاذها، ومن يتخذها، كلها عناصر لخطة استجابة فعالة.

الاستئصال ومتابعة الحوادث

- **الاستئصال**

قبل أن تبدأ مجموعة أمن تكنولوجيا المعلومات في جهود الاستئصال، يجب عليها جمع وتسجيل جميع الأدلة الجنائية المحتملة من النظام ومن ثم التحقق من كافة النسخ الاحتياطية وان تكون حديثة وكاملة وخالية من البرامج الضارة.

- **متابعة الحادث**

جزء أساسي من المتابعة هو تحديد كيفية اختراق أمن المنظمة حتى لا يتكرر ذلك مرة أخرى.

يتضمن تقرير الحادث الرسمي تسلسلاً زمنيًا مفصلاً للأحداث وتأثير الحادث.

يمكن أن يكون إنشاء صورة قرص الطب الشرعي لكل نظام مخترق على وسائط الكتابة فقط للدراسة اللاحقة وكدليل مفيدًا للغاية. بعد القضاء على الفيروس، يجب إنشاء نسخة احتياطية جديدة. طوال هذه العملية، يجب الاحتفاظ بسجل لجميع الإجراءات المتخذة.

سيكون هذا مفيدًا أثناء مرحلة متابعة الحادث ويضمن عدم تكرار المشكلة. من الضروري إجراء نسخ احتياطي للتطبيقات والبيانات الهامة بانتظام. ومع ذلك، نفذت العديد من المؤسسات عمليات نسخ احتياطي غير كافية ووجدت أنها لا تستطيع استعادة البيانات الأصلية بشكل كامل بعد وقوع حادث أمني. يجب إنشاء جميع النسخ الاحتياطية بتكرار كافٍ لتمكين الاستعادة الكاملة والسريعة للبيانات إذا أدى الهجوم إلى تدمير النسخة الأصلية، ويجب اختبار هذه العملية للتأكد من أنها تعمل.

استخدام MSSP

مزود خدمة الأمان المدارة (MSSP):شركة تقوم بمراقبة وإدارة وصيانة أمن الكمبيوتر والشبكات للمؤسسات الأخرى.

تستخدم العديد من المؤسسات الصغيرة ومتوسطة الحجم MSSP نظرًا لأن مستوى الخبرة الداخلية في مجال أمان الشبكات اللازمة لحماية عملياتها التجارية يكون مكلفًا للغاية بحيث لا يمكن الحصول عليه وصيانته.

مواكبة مجرمي الكمبيوتر: ومع القوانين واللوائح الجديدة يمكن أن تكون شاقة بالنسبة للمنظمات.

يقوم المتسللون الإجراميون بالدس والحث باستمرار، محاولين اختراق الأمان والدفاعات من المنظمات.أيضًا، تتطلب قوانين مثل قانون HIPAA، وSarbanes-Oxley، وقانون باتريوت الأمريكي من الشركات إثبات أنها تقوم بتأمين بياناتها.

بالنسبة لمعظم المؤسسات الصغيرة ومتوسطة الحجم، يعد مستوى الخبرة الداخلية في مجال أمن الشبكات اللازمة لحماية عملياتها التجارية مكلفًا للغاية بحيث لا يمكن الحصول عليه وصيانته. ونتيجة لذلك، تقوم العديد من المؤسسات بالاستعانة بمصادر خارجية لعمليات أمن الشبكات الخاصة بها مزود خدمة الأمن المدارة

(MSSP)، وهي شركة تقوم بمراقبة وإدارة وصيانة أجهزة الكمبيوتر وأمن الشبكات للمؤسسات الأخرى.

تتضمنMSSPs شركات مثل AT&T وComputer Sciences Corporation، وDell SecureWorks، وIBM، وSymantec، وVerizon. توفر خدمات MSSP خدمة قيمة لأقسام تكنولوجيا المعلومات الغارقة في مجموعات من التنبيهات والإنذارات الكاذبة القادمة من شبكات VPN؛ ومكافحة الفيروسات، وجدار الحماية، ومعرفات الهوية (IDS)؛ وغيرها من أنظمة المراقبة الأمنية. بالإضافة إلى ذلك، توفر بعض خدمات MSSP امكانية فحص الثغرات الأمنية وحظر الويب وإمكانيات التصفية.

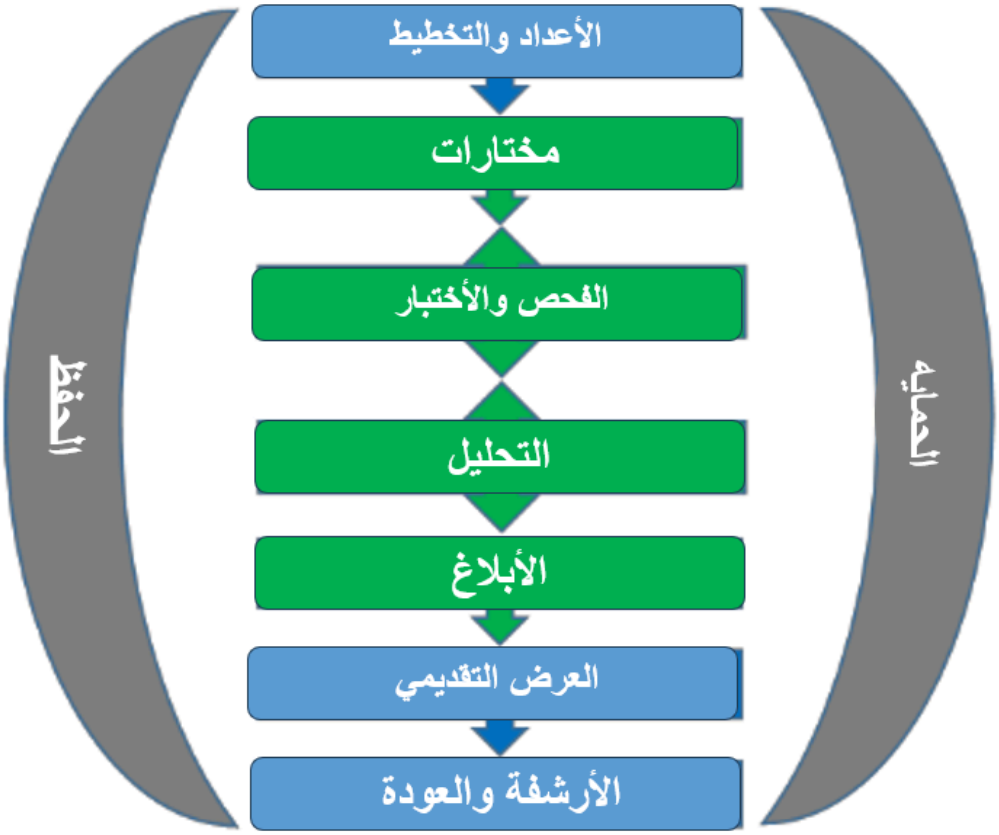
الطب الشرعي الكمبيوتر

الطب الشرعي الحاسوبي: هو الانضباط وذلك يجمع بين عناصر القانون وعلوم الكمبيوتر وجمع وفحص وحفظ البيانات من أنظمة الكمبيوتر والشبكات وأجهزة التخزين بما يحافظ على سلامة البيانات المجمعة بحيث تكون مقبولة كدليل أمام المحكمة.

إن التعامل السليم مع تحقيقات الطب الشرعي للكمبيوتر هو المفتاح لمكافحة جرائم الكمبيوتر بنجاح في المحكمة.

يمكن فتح تحقيق في الطب الشرعي الحاسوبي ردًا على تحقيق جنائي أو دعوى مدنية. وقد يتم إطلاقه أيضًا لمجموعة متنوعة من الأسباب الأخرى، على سبيل المثال، لتتبع الخطوات التي تم اتخاذها عند فقدان البيانات، أو لتقييم الضرر بعد حادث كمبيوتر، أو للتحقيق في الكشف غير المصرح به عن البيانات الشخصية أو السرية الخاصة بالشركة، أو لتأكيد أو تقييم تأثير التجسس الصناعي.

الطب الشرعي الكمبيوتر



ملخص

الجزء الأول

لماذا تنتشر حوادث الكمبيوتر إلى هذا الحد، وما آثارها؟

- تشمل الأسباب ما يلي:

1-زيادة تعقيد الحوسبة.

2-التوسع في الأنظمة وتغييرها.

3-زيادة في انتشار سياسات BYOD.

4-الاعتماد المتزايد على البرامج ذات نقاط الضعف المعروفة.

5-زيادة تطور أولئك الذين قد يلحقون الأذى.

- الاستغلال: هجوم على نظام معلومات يستغل ثغرة أمنية معينة في النظام غالبًا ما يكون ذلك نتيجة لسوء تصميم النظام أو تنفيذه.

ملخص

الجزء الثاني

لماذا تنتشر حوادث الكمبيوتر إلى هذا الحد، وما آثارها؟

- مرتكبو الجرائم الحاسوبية:

1- هاكر القبعة السوداء.

2- كراكر.

3- جاسوس خبيث من الداخل.

4- جاسوس صناعي.

5- مجرم إلكتروني.

6- ناشط هاكر.

7- إرهابي الإنترنت.

- هاكر القبعة البيضاء: يتم تعيينه من قبل منظمة لاختبار أمان أنظمة المعلومات الخاصة بها مما يسمح للمنظمة بتحسين دفاعاتها.

ملخص

الجزء الثالث

لماذا تنتشر حوادث الكمبيوتر إلى هذا الحد، وما آثارها؟

- مآثر الكمبيوتر الشائعة:

1- برامج الفدية والفيروسات والديدان.

2- أحصنة طروادة.

3- القنابل المنطقية.

4- التهديدات المختلطة.

5- رسائل إلكترونية مزعجة.

6- هجمات DDoS والجذور الخفية.

7- التهديدات المستمرة المتقدمة.

8- التصيد الاحتيالي، والتصيد الاحتيالي، والتصيد الاحتيالي عبر الرسائل النصية القصيرة، والتصيد الاحتيالي.

9- التجسس الإلكتروني والإرهاب الإلكتروني.

ملخص

الجزء الرابع

لماذا تنتشر حوادث الكمبيوتر إلى هذا الحد، وما آثارها؟

- وزارة الأمن الداخلي (DHS): وكالة فيدرالية مسؤولة عن توفير مكتب الأمن السيبراني والاتصالات مسؤول عن تعزيز أمن ومرونة وموثوقية البنية التحتية السيبرانية والاتصالات في الولايات المتحدة.
- US-CERT شراكة بين وزارة الأمن الوطني والقطاعين العام والخاص تم إنشاؤها لحماية البنية التحتية للإنترنت في البلاد ضد الهجمات الإلكترونية.

ملخص

الجزء الخامس

لماذا تنتشر حوادث الكمبيوتر إلى هذا الحد، وما آثارها؟

- القوانين الصادرة لمكافحة الجرائم الحاسوبية:

1-قانون الاحتيال وإساءة استخدام الكمبيوتر.

2-الاحتيال والأنشطة ذات الصلة فيما يتعلق بالوصول النظام الأساسي للأجهزة.

3-الأسلاك المخزنة والاتصالات الإلكترونية و قوانين الوصول إلى سجلات المعاملات.

4-الولايات المتحدة الأمريكية قانون باتريوت.

ملخص

الجزء السادس

ما الذي يمكن فعله لتنفيذ برنامج أمني قوي لمنع الهجمات الإلكترونية؟

- ثالوث أمان وكالة المخابرات المركزية: السرية والنزاهة وتوافر موارد وبيانات تكنولوجيا المعلومات.
- يجب أن تتضمن استراتيجية الأمان الخاصة بالمؤسسة إجراءات أمنية على مستوى المؤسسة والشبكة والتطبيقات والمستخدم النهائي.

ملخص

الجزء السابع

ما الذي يمكن فعله لتنفيذ برنامج أمني قوي لمنع الهجمات الإلكترونية؟

- العناصر الأساسية لاستراتيجية الأمن القائمة على المخاطر:

1- تقييم المخاطر لتحديد التهديدات وترتيب أولوياتها.

2- خطة واضحة المعالم للتعافي من الكوارث تضمن توافر البيانات الرئيسية وأصول تكنولوجيا المعلومات.

3- تعريف السياسات الأمنية لتوجيه الموظفين لمتابعة العمليات والممارسات الموصى بها.

4- عمليات تدقيق أمنية دورية للتأكد من أن المستخدمين النهائيين يتبعون السياسات المعمول بها ولتقييم مدى كفاية السياسات الأمنية.

5- معايير الامتثال التي تحددها الأطراف الخارجية.

6- استخدام لوحة معلومات الأمان لتتبع مؤشرات الأداء الرئيسية.

ملخص

الجزء الثامن

ما الذي يمكن فعله لتنفيذ برنامج أمني قوي لمنع الهجمات الإلكترونية؟

1-التأكيد المعقول: يجب على المدير استخدام حكمه للتأكد من أن تكلفة الرقابة لا تتجاوز فوائد النظام أو المخاطر التي ينطوي عليها.

2-طبقة أمان الشبكة - العناصر الأساسية: طرق المصادقة، وجدار الحماية، وأجهزة التوجيه، والتشفير، والخوادم الوكيلة، VPN، وIDS

3-طبقة أمان التطبيق - العناصر الأساسية: طرق المصادقة، وأدوار المستخدم وحساباته، وتشفير البيانات.

4-طبقة أمان المستخدم النهائي – العناصر الأساسية: الأمان، التعليم، طرق المصادقة، برامج مكافحة الفيروسات، وتشفير البيانات.

ملخص

الجزء التاسع

ما هي الإجراءات التي يجب اتخاذها في حالة نجاح الاختراق الأمني؟

- يجب وضع خطة الاستجابة قبل وقت طويل من وقوع أي حادث، وينبغي أن تتناول ما يلي:

1- إشعار.

2- حماية الأدلة وسجلات النشاط.

3- الاحتواء.

4- الاستئصال.

5- متابعة.

- يجب على المؤسسات تنفيذ إصلاحات ضد نقاط الضعف المعروفة وإجراء عمليات تدقيق دورية لأمن تكنولوجيا المعلومات.

ملخص

الجزء العاشر

ما هي الإجراءات التي يجب اتخاذها في حالة نجاح الاختراق الأمني؟

- تستخدم العديد من المؤسسات موفر خدمة الأمان المُدارة(MSSP) لمراقبة أمان أجهزة الكمبيوتر والشبكات وإدارتها وصيانتها.
- يقوم الخبراء المدربون في مجال الطب الشرعي الحاسوبي بجمع البيانات من أجهزة وشبكات الكمبيوتر وفحصها وحفظها، بطريقة تحافظ على سلامة البيانات بحيث تكون مقبولة كدليل في المحكمة.