الأكاديمية العربية الدولية
Arab International Academy

إسم المادة: أمن الشبكات والأدلة الجنائية

المحاضِر: م. خليل المحمد

الأكاديمية العربية الدولية – منصة أعد

مقدمة

هل تتذكرون لعبة الغميضة؟ من الصعب أن ننسى الاندفاع للعثور على مكان للاختباء المثالي.

أتذكر أنني كنت جالسًا خلف الملابس المعلقة في الخزانة، أو أقف متجمدًا مثل تمثال خلف ستارة نافذة في غرفة المعيشة .بينما كانت "مجرد لعبة" عندما كنا أطفالًا....

في عالم اليوم المتصل بالإنترنت، تحولت تلك اللعبة إلى نشاط أكثر قتامة وأكثر جدية حيث يختبئ المهاجمون في أماكن غير متوقعة وغالبًا ما تكون منسية .قد يعيش المهاجمون في بعض التقنيات والآلات والأنظمة لسنوات، ويظلون غير مرئيين بواسطة برامج مكافحة الفيروسات وعناصر التحكم الأخرى.

أنواع التهديدات

أنواع التهديدات التي قد تصلنا عبر الانترنت تقسم الى نوعين:

1- المهاجمون (Attackers): وهم اشخاص مدربين بطريقة عالية الكفاءة ويمتلكون مهارات عالية بهدف كشف أكبر كمية ممكنة من البيانات الحساسة.

2- الهجمات السيبرانية(Attacks): والتي من الممكن ان تكون:

- Cybercrime الجرائم السيبرانية
- extortion الابتزاز
- hacktivism القرصنة

من هم المستهدفون بالهجمات السيبرانية؟ كل الأفراد والمؤسسات والشركات والمنظمات والبنوك والحكومات والمنشآت.

أهمية الشبكات

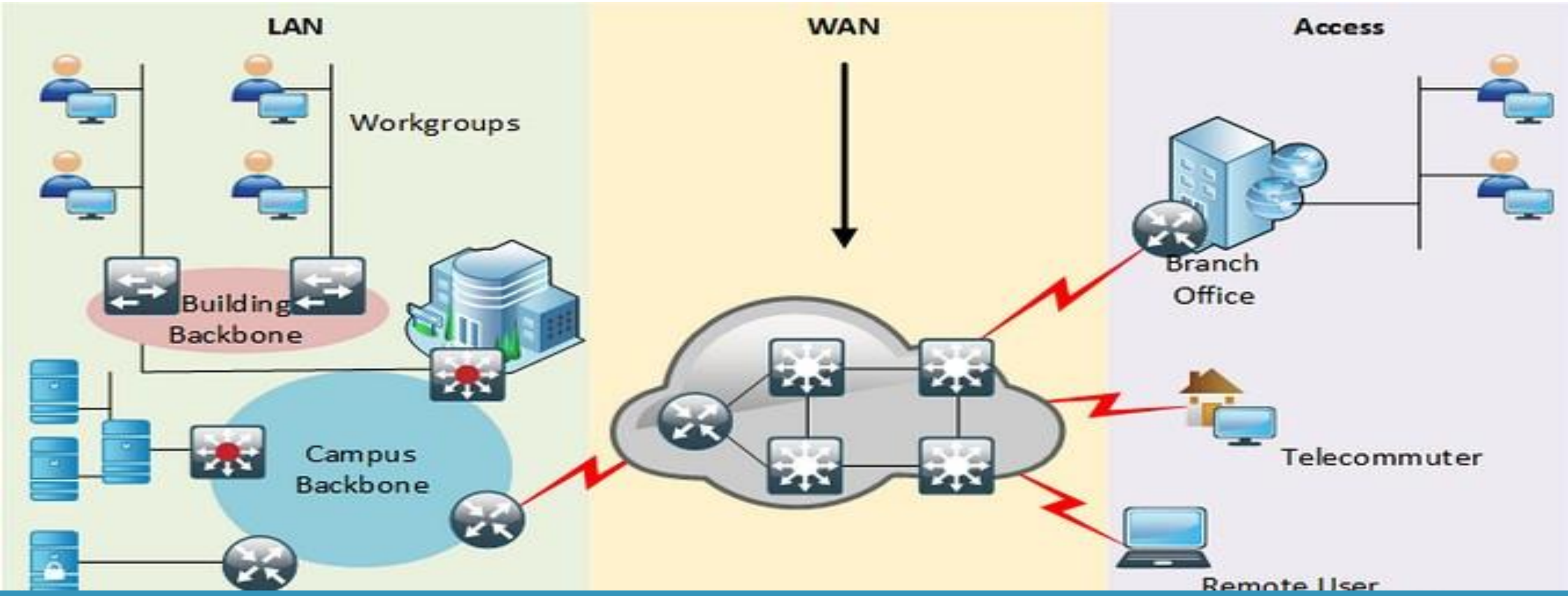
ان نجاح عمل أي منظمة أو شركة او مؤسسة سواء كانت كبيرة او صغيرة في العمل يعتمد بشكل أساسي على استخدام الشبكات التي أصبحت في عصرنا الحالي امر أساسي و لا مفر منه حيث يتم استخدام الشبكات للتواصل او ارسال واستقبال المعلومات وتخزينها.

كما توفر الشركات خدماتها عبر الشبكات هذه الشركات التي تعمل اونلاين

و تحاول الوصول عبر المحيطات باستخدام الشبكات للترويج لمنتجاتها.

لدينا اليوم أيضاً الشبكات الاجتماعية عبر تطبيقات مثل الفيسبوك, تويتر .....

متطلبات الشبكة:



متطلبات الشبكة network demands

1. التوافر Availability : يجب ان تكون الشبكة متوفرة بشكل دائم لكي يستطيع المستفيدون من الخدمات الوصول اليها بكل وقت.
2. القابلية للتطوير Scalable : كلما زاد عدد المشتركين في الشبكة كلما زادت الحاجة لتوسيع هذه الشبكة.
3. قابلية الإدارة Manageable: كلما توسع نطاق عمل الشبكة كلما ازداد تعقيد هذه الشبكة وبالتالي تزداد الحاجة الى توسيع الإدارة.
4. الأمن Security : ليس من المعقول اثناء تصميم الشبكة اهمال جانب الامن والا ستتعرض الشبكة لهجمات خطيرة تتركها عرضة للتدمير.

تقييم الشبكات Assessment

عند التركيز على متطلبات الشبكة التي تزداد تعقيداً بزيادة تعقيد الشبكة وتوسعها من حيث زيادة الخدمات أو المشتركين عندئذٍ يجب اجراء تقييم دوري للشبكة ومكوناتها وتحديث المتطلبات باستمرار كل ستة أشهر على الأقل والأفضل كل ثلاثة أشهر, يركز التقييم على الأمن Security هذا التقييم يجب ان يكون مدعوم بشهادة الامان Certificate والتي يكون لها تاريخ صلاحية ولأخذ العلم فإن بعض الشركات قد تعطي تقييم دائم مدى الحياة وهذا غير واقعي وغير صحيح لأننا اليوم في عصر التطور المخيف للتكنولوجيا فالهجمات تتغير وتتطور والمهاجمون يغيرون اساليبهم باستمرار فلا تكن ضحية لهؤلاء.

الأمن السيبراني

المفهوم الرئيس للأمن السيبراني:

الأمن السيبراني هو العملية والتقنيات المستخدمة في حماية البيانات الحساسة وأنظمة الكمبيوتر والشبكات وتطبيقات البرامج من الهجمات الإلكترونية .الهجمات الإلكترونية عبارة عن مصطلحات عامة تغطي عددًا كبيرًا من الموضوعات ، ولكن بعضًا من أشهرها:

- العبث بالنظم والبيانات المخزنة بداخله
- استغلال الموارد
- الوصول غير المصرح به إلى النظام المستهدف والوصول إلى المعلومات الحساسة
- تعطيل السير العادي للأعمال وعملياتها
- استخدام هجمات برامج الفدية لتشفير البيانات وابتزاز الأموال من الضحايا

الأمن السيبراني

لفهم الحاجة إلى تدابير الأمن السيبراني وممارساتها، دعونا نلقي نظرة سريعة على أنواع التهديدات والهجمات:

1. Ransomware برامج الفدية: هو برنامج لتشفير الملفات يستخدم خوارزمية تشفير فريدة وقوية لتشفير الملفات على النظام الهدف.

2. Bot-nets Attack هجمات الروبوتات: تم تعريفه على أنه شبكة أو مجموعة من الأجهزة المتصلة بنفس الشبكة لتنفيذ مهمة .ولكن يتم استخدام هذا الآن من قبل الجهات الفاعلة السيئة والمتسللين الذين يحاولون الوصول إلى الشبكة وحقن أي رمز ضار أو برامج ضارة لتعطيل عملها.

الأمن السيبراني

3. Social Engineering هجمات الهندسة الاجتماعية: من خلال عرض إعلانات جذابة وجوائز وعروض ضخمة ويطلب منك إدخال تفاصيل حسابك الشخصي والبنكي .يتم نسخ جميع المعلومات التي تدخلها هناك واستخدامها في الاحتيال المالي والاحتيال في الهوية وما إلى ذلك.

4. Cryptocurrency Hijacking اختطاف العملات المشفرة: المستثمرون والمتداولون في العملات المشفرة هم الأهداف السهلة لهذا الهجوم.

الأمن السيبراني

5. Phishing التصيد: يعتبر التصيد الاحتيالي إجراءً احتياليًا يتمثل في إرسال رسائل بريد إلكتروني غير مرغوب فيها عن طريق التقليد على أنها من أي مصدر شرعي .

لتجنب ذلك ، يجب عليك معرفة المزيد حول حملات البريد الإلكتروني للتصيد الاحتيالي وإجراءاتها الوقائية. يمكن للمرء أيضًا استخدام تقنيات تصفية البريد الإلكتروني لتجنب هذا الهجوم.

6. البرمجيات الخبيثة Malware

يشير مصطلح "البرامج الضارة" إلى متغيرات البرامج الضارة - مثل الفيروسات المتنقلة والفيروسات وأحصنة طروادة وبرامج التجسس - التي توفر وصولاً غير مصرح به أو تتسبب في تلف الكمبيوتر .أصبحت هجمات البرامج الضارة "بلا ملفات" بشكل متزايد ومصممة للالتفاف حول طرق الكشف المألوفة، مثل أدوات مكافحة الفيروسات ، التي تقوم بالبحث عن مرفقات الملفات الضارة.

الأمن السيبراني

7.التهديدات الداخلية Insider threats

الموظفون الحاليون أو السابقون أو شركاء العمل أو المقاولون أو أي شخص لديه حق الوصول إلى الأنظمة أو الشبكات في الماضي يمكن اعتباره تهديداً داخلياً إذا أساءوا استخدام أذونات الوصول الخاصة بهم .يمكن أن تكون التهديدات الداخلية غير مرئية لحلول الأمان التقليدية مثل جدران الحماية وأنظمة الكشف عن التسلل، والتي تركز على التهديدات الخارجية.

8. هجمات رفض الخدمة الموزعة (DDoS) Distributed denial-of-service (DDoS) attacks

يحاول هجوم DDoS تعطل خادم أو موقع ويب أو شبكة عن طريق زيادة التحميل عليها بحركة المرور ، عادةً من أنظمة منسقة متعددة .هجمات DDoSتطغى على شبكات المؤسسات عبر بروتوكول إدارة الشبكة البسيط (SNMP) ، المستخدم في أجهزة المودم والطابعات والمحولات وأجهزة التوجيه والخوادم.

الأمن السيبراني

9. التهديدات المستمرة المتقدمة (APTs) Advanced persistent threats (APTs)

في APT ، يتسلل متطفل أو مجموعة من المتسللين إلى نظام ويظلون غير مكتشفين لفترة طويلة .يترك المتسلل الشبكات والأنظمة سليمة حتى يتمكن المتسلل من التجسس على النشاط التجاري وسرقة البيانات الحساسة مع تجنب تنشيط الإجراءات الدفاعية المضادة .يعد خرق الرياح الشمسية الأخير لأنظمة حكومة الولايات المتحدة مثالًا على.APT

10. هجمات Man-in-the-middle attacks

Man-in-the-middle هو هجوم تنصت ، حيث يقوم مجرم إلكتروني باعتراض ونقل الرسائل بين طرفين لسرقة البيانات .على سبيل المثال، في شبكة Wi-Fi غير آمنة ، يمكن للمهاجم اعتراض البيانات التي يتم تمريرها بين جهاز الضيف والشبكة.

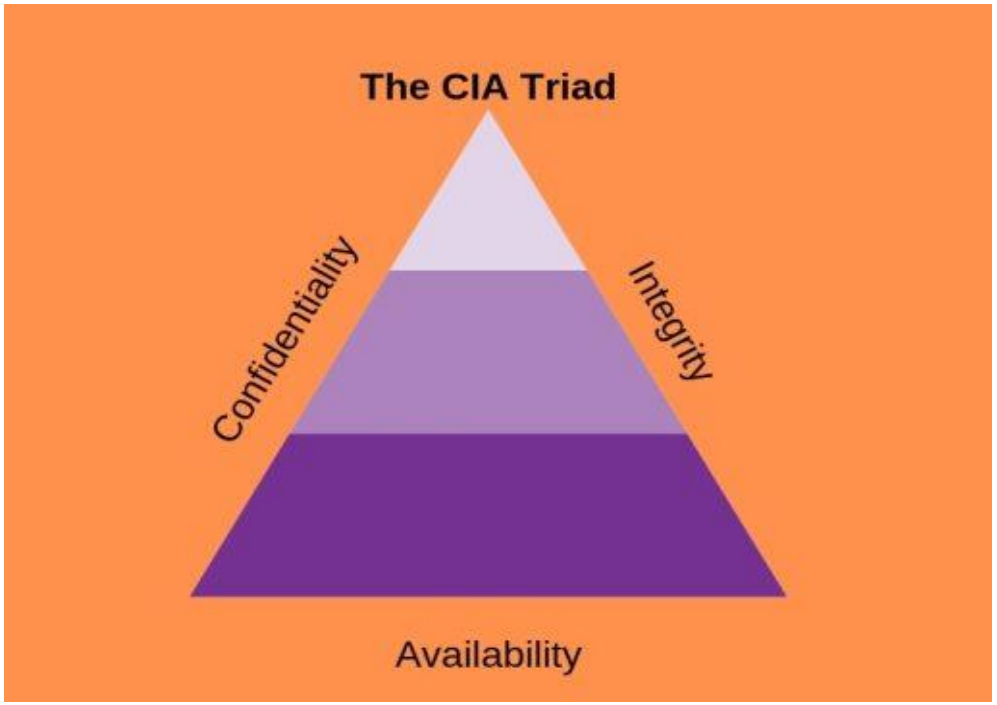
امن الشبكات كنقطة جوهرية

Physical control and technical controls:

Physical control: هو حماية المكونات الموجودة في مركز البيانات من الوصول الفيزيائي مثل استخدام كلمة مرور قوية لجهاز الحاسوب او استخدام كلمة مرور قوي للشبكة تكون مستحيلة التخمين حتى مع الخوارزميات التي تحاول اختراق كلمات المرور وان يكون مركز البيانات عالي الحماية مراقب بالكاميرات وتوظيف حراس الامن واستخدام الحواجز الحيوية.

technical controls: هي كل العناصر التي يتم استخدامها ضمن بناء الشبكة مثل الراوترات والسيرفرات كما تتضمن الموقع على الكلاود أي الويب وحتى التطبيقات وتشمل صلاحيات الدخول ومن هو مصرح له وما هي الصلاحيات ومن هو غير مصرح له وحجب الصلاحيات.

Key of security concept triad



الأمن السيبراني هو مصطلح واسع جدًا ولكنه يعتمد على ثلاثة مفاهيم أساسية تُعرف باسم CIA :

يتكون من مثلث السرية والنزاهة والتوافر .تم تصميم هذا النموذج لتوجيه المؤسسة مع سياسات الأمن السيبراني في مجال أمن المعلومات.

القصد من هذا المثلث الذي يحيط بالداتا هو لحماية البيانات

Key of security concept triad

1- السرية confidentiality:

يحدد القواعد التي تحد من الوصول إلى المعلومات, تتخذ السرية تدابير لتقييد وصول المهاجمين والمتسللين عبر الإنترنت إلى المعلومات الحساسة

.في المنظمة ، يُسمح للأشخاص أو يُحرمون من الوصول إلى المعلومات وفقًا لفئتهم الوظيفية وذلك بحسب التسلسل الوظيفي أو بحسب دور الموظف الذي يشغل هذا المنصب يعني لديه وصول لمعلومات معينة بينما يحرم من الوصول إلى معلومات اخرى هي ليست صلاحياته إذن حسب employee level اي مستوى هذا الموظف يجب أن يكون related الى هذه المعلومات يجب أن يكون له علاقة بهذه المعلومات.

Key of security concept triad

2- التكامل integrity:

هذا يضمن أن البيانات متسقة ودقيقة وجديرة بالثقة خلال الفترة الزمنية الخاصة بها

التكامل هو التأكد من أن لا يتم التلاعب بالبيانات أو تغييرها أو حذفها أو تدميرها أو فقدانها بالكامل ولا يسمح للناس غير المرخصين unauthorized بالوصول او التلاعب او تحرير البيانات.

يجب اتخاذ التدابير المناسبة في المنظمة لضمان سلامتها .أذونات الملفات والتحكم في وصول المستخدم هي التدابير التي تتحكم في خرق البيانات .كما يجب تطبيق الأدوات والتقنيات لاكتشاف أي تغيير أو خرق في البيانات .تستخدم المنظمات المختلفة المجموع الاختباري وحتى المجموع الاختباري للتشفير للتحقق من سلامة البيانات.

Key of security concept triad

3- التوفرavailability :

يجب الحفاظ على التوفر من حيث جميع المكونات الضرورية مثل الأجهزة والبرامج والشبكات والأجهزة ومعدات الأمان. .

يضمن هذا الأداء السلس والوصول إلى البيانات دون أي انقطاع .أيضًا توفير اتصال مستمر بين المكونات من خلال توفير نطاق ترددي كافٍ. كما يتضمن أيضًا اختيار معدات أمنية إضافية في حالة حدوث أي كارثة أو اختناقات .يجب أن تضمن الأدوات المساعدة مثل جدران الحماية وخطط التعافي من الكوارث والخوادم الوكيلة وحل النسخ الاحتياطي المناسب التعامل مع هجمات نهج ناجح ، يجب أن يمر عبر طبقات متعددة من الأمن لضمان الحماية لكل مكون من مكونات الأمن .

تشمل بشكل خاص أجهزة الكمبيوتر وأنظمة الأجهزة والشبكات والبرامج والبيانات المشتركة.

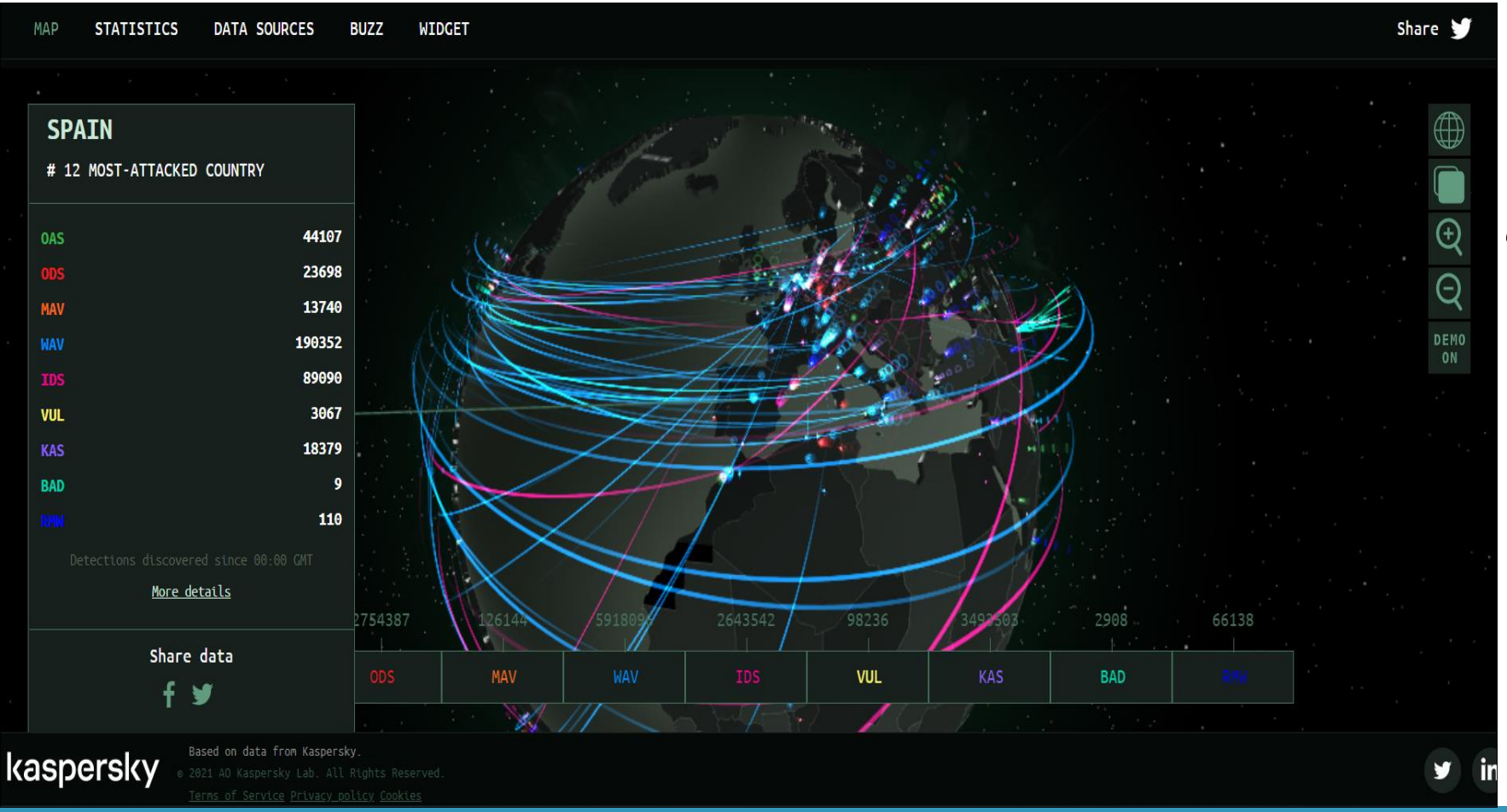
الهجمات السيبرانية

Cyber threats بدأت الهجمات السيبرانية منذ العام سنة 1988 عندما كان عندنا دودة إلكترونية ثم تطورت الفيروسات وتحولت إلى هجمات إلكترونية وكذلك الهجمات ال المنسقة coordinated attacks خطرة جدا لأن هجمات منتظمة ومنسقة والدفاع ضد هذه الهجمات ستكون صعبة جدا لأنهم المهاجمين مدربين على هذه الهجمات إذن حتى نستطيع حماية مؤسستنا يجب أن نثقف الأعضاء والموظفين ونجري لهم الدورات التدريبية ونوعيه نعطيهم دورات توعية يستطيعون استخدام كلمة سر قوية يستخدمون الحروف الكبيرة والرموز إذا نستخدم كلمة سر قوية لحماية الحسابات وحاول أن تغير كلمة السر كل فترة زمنية محددة وحافظ على مكان عملك و تتأكد من share drivers المشاركة بين الحاسبات بالإضافة إلى ذلك لا تحاول أن تقوم بالنقر على أي رابط يأتيك بالإيميل على الشبكة بشكل عام إلا بعد التأكد وتفكر أكثر من مرة قبل أن تعمل click النقر على أي رابط لأن هذا فيه خطورة كبيرة جدا

الهجمات السيبرانية

/https://cybermap.kaspersky.com

اذا اتبعنا الرابط المدرج أعلاه سوف ندخل الى موقع لشركة كاسبر سكاي يبين بالوقت الحقيقي والمباشر الهجمات السيبرانية حول العالم



Network Risk management

مفهوم إدارة المخاطر:

Information Security Risk Management?

إدارة مخاطر أمن المعلومات ، أو ISRM، هي عملية إدارة المخاطر المرتبطة باستخدام تكنولوجيا المعلومات. وهو ينطوي على تحديد وتقييم ومعالجة المخاطر المتعلقة بسرية أصول المنظمة وسلامتها وتوافرها. الهدف النهائي من هذه العملية هو معالجة المخاطر وفقًا لتحمل المخاطر الشامل للمؤسسة. يجب ألا تتوقع الشركات القضاء على جميع المخاطر ؛ بدلاً من ذلك ، يجب عليهم السعي لتحديد وتحقيق مستوى مخاطر مقبول لمنظمتهم.

Network Risk management

مراحل ISRM

1- تحديد الأصول :ما هي البيانات أو الأنظمة أو الأصول الأخرى التي تعتبر "جواهر التاج" لمؤسستك؟ على سبيل المثال ، ما هي الأصول التي سيكون لها أكبر تأثير على مؤسستك إذا تم اختراق سريتها أو نزاهتها أو توفرها؟ ليس من الصعب معرفة سبب أهمية سرية البيانات مثل أرقام الضمان الاجتماعي والملكية الفكرية .لكن ماذا عن النزاهة؟ ، فقد تؤدي مشكلة تكامل بسيطة في بيانات التقارير المالية إلى تكلفة باهظة .أو ، إذا كانت إحدى المؤسسات عبارة عن خدمة بث موسيقى عبر الإنترنت وتم اختراق توفر ملفات الموسيقى ، فقد تفقد المشتركين.

2- تحديد نقاط الضعف :ما هي نقاط الضعف على مستوى النظام أو البرامج التي تعرض سرية الأصول وسلامتها وتوافرها للخطر؟ ما هي نقاط الضعف أو القصور في العمليات التنظيمية التي يمكن أن تؤدي إلى تعرض المعلومات للخطر؟

Network Risk management

- **3- تحديد التهديدات :** ما هي بعض الأسباب المحتملة لتعرض الأصول أو المعلومات للخطر؟ على سبيل المثال ، هل مركز بيانات مؤسستك موجود في منطقة تسود فيها التهديدات البيئية ، مثل الأعاصير والفيضانات؟ هل يتم استهداف الشركات التي تقدم خدمات مماثلة بشكل نشط واختراقهم من قبل نقابة إجرامية معروفة ، أو مجموعة ناشطة في مجال القرصنة ، أو كيان ترعاه الحكومة؟ تعد نمذجة التهديدات نشاطًا مهمًا يساعد في إضافة سياق من خلال ربط المخاطر بالتهديدات المعروفة والطرق المختلفة التي يمكن أن تتسبب بها هذه التهديدات في تحقيق المخاطر من خلال استغلال الثغرات الأمنية.

- **4- تحديد الضوابط:** ما الذي لديك بالفعل لحماية الأصول المحددة؟ يعالج عنصر التحكم بشكل مباشر ثغرة أمنية محددة أو تهديدًا إما عن طريق إصلاحه بالكامل (العلاج) أو تقليل احتمالية و / أو تأثير الخطر الذي يتم تحقيقه (التخفيف) .على سبيل المثال ، إذا كنت قد حددت خطر استمرار المستخدمين الذين تم إنهاء خدمتهم في الوصول إلى تطبيق معين ، فقد يكون عنصر التحكم عملية تقوم تلقائيًا بإزالة المستخدمين من هذا التطبيق عند الإنهاء .عنصر التحكم التعويضي هو عنصر تحكم "شبكة أمان" يعالج المخاطر بشكل غير مباشر .بالاستمرار مع نفس المثال أعلاه ، قد يكون عنصر التحكم التعويضي عبارة عن عملية مراجعة وصول ربع سنوية .خلال هذا الاستعراض .

Network Risk management

التقييم:

هي عملية دمج المعلومات التي جمعتها حول الأصول ونقاط الضعف والضوابط لتحديد المخاطر .هناك العديد من الأطر والأساليب لذلك ، ولكن من المحتمل أن تستخدم بعض الاختلافات في هذه المعادلة:

المخاطرة = (التهديد × الضعف (احتمال الاستغلال × تأثير الاستغلال) × قيمة الأصول) - ضوابط الأمان

Risk = (threat x vulnerability (exploit likelihood x exploit impact) x asset value) - security controls

ملاحظة: هذا تشبيه بصيغة مبسطة للغاية .إن حساب المخاطر الاحتمالية ليس بهذه البساطة تقريبًا ، الأمر الذي يثير استياء الجميع.

Network Risk management

العلاج

بمجرد تقييم المخاطر وتحليلها ، ستحتاج المنظمة إلى تحديد خيارات العلاج:

- **المعالجة** :تنفيذ عنصر تحكم يعمل على إصلاح المخاطر الأساسية بشكل كامل أو شبه كامل.
مثال :لقد حددت ثغرة الأمنية على خادم حيث يتم تخزين الأصول الهامة ، وقمت بتطبيق تصحيح لتلك الثغرة الأمنية.

- **التخفيف** :تقليل احتمالية و / أو تأثير الخطر ، ولكن ليس إصلاحه بالكامل.
مثال :لقد حددت ثغرة أمنية على الخادم حيث يتم تخزين الأصول الهامة ، ولكن بدلاً من تصحيح الثغرة الأمنية ، فإنك تقوم بتنفيذ قاعدة جدار الحماية التي تسمح فقط لأنظمة معينة بالاتصال بالخدمة المعرضة للخطر على الخادم.

- **التحويل :**تحويل المخاطر إلى كيان آخر حتى تتمكن مؤسستك من التعافي من التكاليف المتكبدة للمخاطر المحققة.
مثال :تشتري تأمينًا يغطي أي خسائر قد يتم تكبدها إذا تم استغلال الأنظمة الضعيفة
.ملاحظة: يجب استخدام هذا لتكملة معالجة المخاطر والتخفيف من حدتها ولكن لا يحل محلها تمامًا.

Network Risk management

- **قبول المخاطر :**

عدم إصلاح الخطر .يعد هذا مناسبًا في الحالات التي يكون فيها الخطر منخفضًا بشكل واضح والوقت والجهد اللازمين لإصلاح تكاليف المخاطر أكثر من التكاليف التي سيتم تكبدها في حالة إدراك المخاطر.

مثال :لقد حددت ثغرة أمنية على الخادم ولكنك خلصت إلى أنه لا يوجد شيء حساس على ذلك الخادم ؛ لا يمكن استخدامه كنقطة دخول للوصول إلى الأصول الهامة الأخرى ، والاستغلال الناجح للثغرة أمر معقد للغاية .نتيجة لذلك ، قررت أنك لست بحاجة إلى إهدار الوقت والموارد لإصلاح الثغرة الأمنية.

تجنب المخاطر :إزالة جميع حالات التعرض لمخاطر محددة

مثال :لقد حددت خوادم مزودة بأنظمة تشغيل (OS) على وشك الوصول إلى نهاية عمرها الافتراضي ولن تتلقى بعد الآن تصحيحات أمان من مُنشئ نظام التشغيل .تقوم هذه الخوادم بمعالجة وتخزين البيانات الحساسة وغير الحساسة .لتجنب خطر اختراق البيانات الحساسة ، يمكنك ترحيل هذه البيانات الحساسة بسرعة إلى خوادم أحدث يمكن الوصول إليها .تستمر الخوادم في تشغيل ومعالجة البيانات غير الحساسة أثناء تطوير خطة لإيقاف تشغيلها وترحيل البيانات غير الحساسة إلى خوادم أخرى.

Topology Network

نريد أن نصمم مخطط الشبكة لمنظمة معينة أو لشركة معينة يجب أن نأخذ بعين الاعتبار مجموعة أشياء تدخل ضمن network التي هي:

1- Assets

2- Risks

3- Threats

4- Vulnerability

Topology Network

1 - Assets: و لها نوعين نوع ملموس فيزيائي physical ملموس والآخر غير ملموس الغير ملموس مثل قواعد البيانات database معلومات الموظفين السجلات الطبية لكنها تعتبر ضمن الأسس أما الملموسة فيقصد بها الكمبيوترات الأجهزة أجهزة الكمبيوتر الراوتر الطابعات printers سيرفرات كل هذه تعتبر من أجزاء الأساس كتحليل المخاطر risk analysis من المهم أن نعرف أن يكون لدينا إي موازنة من أجل budget for security نقوم بعمل تقييم evaluating وترتيب المخاطر عن طريق عنونة addressing هذه المخاطر يعني يجب أن نعرف أن المخاطر التي إيه يمكن أن تقع الشركة فيها ويجب أن نرتب هذه المخاطر بعد أن نقوم بعمل تقييم كامل يجب أن نرتب هذه المخاطر على أساس التقييم كم سيطول هذا التقييم ومدى خطورتها نعمل لها ترتيب .

2 - Risks إذا أردنا أن نعرف riskفهو عبارة عن معادلة تقول يساوي Threatsمضروبة Vulnerability

Risks= Threats* Vulnerability المخاطر تساوي التهديدات مضروبة بنقاط الضعف ماذا يعني ماذا نعني بالمخاطر أو risk هناك حالات يكون فيها تهديدات موجودة لكن بغياب نقاط الضعف لن يكون هناك أي خطر أي أخطار وهناك في حالات بالعكس يكون هناك نقاط ضعف لكن لا تشكل أي تهديدات أيضا لا يعتبر مخاطر إذا عندما تكون في خطر حقيقي يجب أن يتوفر عاملين هما التهديدات ونقاط الضعف.

Topology Network

3- Threats ما هي التهديدات؟ ممكن التهديدات أن تكون أي شيء على سبيل المثال ممكن أن تكون التهديدات مجموعة إرهابيين يخربون شيء معين أو ممكن يكون موظف داخل network انزعج من الشركة وأحب أن يعمل انتقام معين أو تكون مشكلة طبيعية صار إعصار مثلا وانقطع الاتصال بين الأبراج حقيقة هذه ال هذه التهديدات تؤدي إلى نقاط ضعف وبالتالي هذا يؤدي إلى مخاطر هذا يؤدي إلى ضرر كبير assets على سبيل المثال قد نكون نمرر links في مكان معين وحدث إعصار و وقع برج معين أو تحرك المايكرويف أو تحرك الصحن ممكن أن يقطع اللينك بين نقطتين فهذا يعمل damage أو ضرر

4- Vulnerability نستطيع اعتبارها هو الضعف الموجود في نفس في النظام ذاته نفسه أي أنك عندما تستخدم نظام لا تعمل له تحديث أنتجت أو تطبيقات كراك أو مشاكل human error أو مشكلة سوفتوير أصبح فيها bugs أو نسيت الباسورد نسيت كلمة السر كل هذه تدخل في الفيلا روبوتي الضعف نقاط الضعف وهي ستدخل ضمن الun authorized access.

ما مدى معرفتك بالأدلة الجنائية الرقمية؟

علم الادلة الجنائية الرقمية هو فرع من فروع علم الادلة الجنائية يركز على استعادة المواد الموجودة في الأجهزة الرقمية المتعلقة بجرائم الإنترنت والتحقيق فيها .تم استخدام مصطلح الادلة الجنائية الرقمية لأول مرة كمرادف للطب الشرعي الحاسوبي .منذ ذلك الحين ، توسعت لتشمل التحقيق في أي أجهزة يمكنها تخزين البيانات الرقمية .على الرغم من الإبلاغ عن أول جريمة كمبيوتر في عام 1978 ، تلاها قانون أجهزة الكمبيوتر في فلوريدا ، إلا أنه لم يصبح مصطلحًا معترفًا به حتى التسعينيات .لم تظهر السياسات الوطنية المتعلقة بالأدلة الجنائية الرقمية إلا في أوائل القرن الحادي والعشرين.

الادلة الجنائية الرقمية هو عملية تحديد الأدلة الرقمية، وحفظها وتحليلها وتوثيقها .يتم ذلك من أجل تقديم الأدلة في محكمة قانونية عند الاقتضاء.

الأدلة الجنائية الرقمية

خطوات الأدلة الجنائية الرقمية:

من أجل قبول الأدلة الرقمية في محكمة قانونية ، يجب التعامل معها بطريقة محددة للغاية بحيث لا تكون هناك فرصة لمجرمي الإنترنت للتلاعب بالأدلة:

1. تحديد الهوية

أولاً ، ابحث عن الدليل ، مع الإشارة إلى مكان تخزينه.

2. الحفظ

بعد ذلك ، قم بعزل وتأمين وحفظ البيانات. وهذا يشمل منع الناس من احتمال العبث بالأدلة.

الأدلة الجنائية الرقمية

3. التحليل

بعد ذلك ، أعد بناء أجزاء من البيانات واستخلص النتائج بناءً على الأدلة الموجودة.

4. التوثيق

بعد ذلك ، قم بإنشاء سجل لجميع البيانات لإعادة إنشاء مسرح الجريمة.

5. العرض

أخيرًا ، لخص واستنتج الخاتمة.

الأدلة الجنائية الرقمية

متى يتم استخدام الأدلة الجنائية الرقمية في إعداد الأعمال؟

بالنسبة للشركات ، يعد التحليل الجنائي الرقمي جزءًا مهمًا من عملية الاستجابة للحوادث .يقوم محققو الادلة الجنائية بتحديد وتسجيل تفاصيل الحادث الإجرامي كدليل لاستخدامه في إنفاذ القانون .غالبًا ما تكون القواعد واللوائح المحيطة بهذه العملية مفيدة في إثبات البراءة أو الجرم في محكمة قانونية

من هو محقق الادلة الجنائية الرقمية؟

محقق الادلة الجنائية الرقمية هو شخص لديه الرغبة في متابعة الأدلة وحل جريمة ما تقريبًا .تخيل حدوث خرق أمني في شركة ما ، مما يؤدي إلى سرقة البيانات .في هذه الحالة ، سيأتي محلل جنائي للكمبيوتر ويحدد كيف تمكن المهاجمون من الوصول إلى الشبكة ، وأين اجتازوا الشبكة ، وماذا فعلوه على الشبكة ، سواء أخذوا معلومات أو زرعوا برامج ضارة .في ظل هذه الظروف ، يتمثل دور محقق الأدلة الجنائية في استعادة البيانات مثل المستندات والصور ورسائل البريد الإلكتروني من محركات الأقراص الثابتة للكمبيوتر وأجهزة تخزين البيانات الأخرى ، مثل محركات الأقراص المضغوطة ومحركات أقراص فلاش ، مع حذفها أو تلفها أو التلاعب بها بأي طريقة أخرى.

الأدلة الجنائية الرقمية

متى بدأت الادلة الجنائية الرقمية؟

إذا نظرنا إلى الوراء في تاريخ الادلة الجنائية الرقمية، فإن تطبيق القانون خلال تلك الفترة كان لديه الحد الأدنى من الفهم لتطبيق تقنيات الادلة الجنائية الرقمية .ومع ذلك ، خلال السبعينيات والثمانينيات ، كان فريق الادلة الجنائية يمثل في الغالب ممثلين عن وكالات إنفاذ القانون الفيدرالية مع خلفية كمبيوتر .كان مجال الاهتمام الأول لإنفاذ القانون هو تخزين البيانات ، حيث تم إجراء معظم التوثيق رقميًا .لا يمكن إنكار أن مصادرة الوثائق والاحتفاظ بها وتحليلها كانت مهمة طويلة للسلطات .في هذه الحالة ، أطلق مكتب التحقيقات الفيدرالي برنامج Magnet media في عام 1984 ، والذي كان أول برنامج رسمي للأدلة الجنائية الرقمية.

الأدلة الجنائية الرقمية

كيف يتم استخدام الادلة الجنائية الرقمية في التحقيق؟

البصمة الرقمية : هي معلومات حول شخص ما على النظام ، مثل صفحات الويب التي زاروها ، والوقت الذي كانوا فيه نشطين ، والجهاز الذي كانوا يستخدمونه .باتباع البصمات الرقمية ، سيقوم المحقق باسترداد البيانات المهمة لحل قضية الجريمة .على سبيل المثال لا الحصر - مات بيكر ، في عام 2010 ، وكرينار لوشا ، في عام 2009 ، وتم حل المزيد من القضايا بمساعدة الادلة الجنائية الرقمية.

المحققون الجنائيون السيبرانيون خبراء في التحقيق في البيانات المشفرة باستخدام أنواع مختلفة من البرامج والأدوات .هناك العديد من التقنيات القادمة التي يستخدمها المحققون اعتمادًا على نوع الجريمة الإلكترونية التي يتعاملون معها .تشمل مهام المحققين السيبرانيين استعادة الملفات المحذوفة ، وكسر كلمات المرور ، والعثور على مصدر الخرق الأمني .بمجرد جمع الأدلة ، يتم تخزينها وترجمتها لجعلها قابلة للعرض أمام المحكمة أو للشرطة لمزيد من الفحص .يمكن فهم دور الادلة الجنائية الإلكتروني في الجرائم الجنائية من خلال دراسة حالة: القضايا الباردة والادلة الجنائية السيبراني

الأدلة الجنائية الرقمية

مراحل الأدلة الجنائية الرقمية:

المرحلة الأولى - الاستجابة الأولى

يُعرف الإجراء الذي يتم تنفيذه مباشرةً بعد وقوع حادث أمني باسم الاستجابة الأولى. يعتمد بشكل كبير على طبيعة الحادث.

المرحلة الثانية - التفتيش والضبط

في هذه المرحلة ، يبحث المختصون عن الأجهزة المتورطة في تنفيذ الجريمة. ثم تم ضبط هذه الأجهزة بعناية لاستخراج المعلومات منها.

المرحلة الثالثة - جمع الأدلة

بعد مرحلة البحث والضبط ، يستخدم المحترفون الأجهزة التي تم الحصول عليها لجمع البيانات. لديهم طرق جنائية محددة جيدًا للتعامل مع الأدلة.

الأدلة الجنائية الرقمية

المرحلة الرابعة- تأمين الأدلة

يجب أن يتمتع طاقم الطب الشرعي بإمكانية الوصول إلى بيئة آمنة حيث يمكنهم تأمين الأدلة. يحددون ما إذا كانت البيانات التي تم جمعها دقيقة وحقيقية ويمكن الوصول إليها.

المرحلة السادسة - تحليل البيانات

في إطار تحليل البيانات ، يقوم الموظفون المسؤولون بمسح البيانات التي تم الحصول عليها لتحديد معلومات الأدلة التي يمكن تقديمها إلى المحكمة. تدور هذه المرحلة حول فحص البيانات وتحديدها وفصلها وتحويلها ونمذجة لتحويلها إلى معلومات مفيدة.

المرحلة الخامسة - الحصول على البيانات

من الأصول (ESI) الحصول على البيانات هو عملية استرداد المعلومات المخزنة إلكترونيًا الرقمية المشتبه بها. يساعد ذلك في الحصول على نظرة ثاقبة للحادث بينما يمكن أن تؤدي العملية غير الصحيحة إلى تغيير البيانات ، وبالتالي التضحية بسلامة الأدلة.

المرحلة السابعة - تقييم الأدلة

ترتبط عملية تقييم الأدلة ببيانات الإثبات بالحادث الأمني. يجب أن يكون هناك تقييم شامل يعتمد على نطاق القضية.

الأدلة الجنائية الرقمية

المرحلة التاسعة - الشهادة كشاهد خبير

يجب على المحققين الشرعيين الاتصال بالشاهد الخبير للتأكد من دقة الأدلة. الشاهد الخبير هو المحترف الذي يحقق في الجريمة لاسترداد الأدلة.

ما هي أدوات الأدلة الجنائية الرقمية؟

في التسعينيات، تم إجراء التحقيقات الرقمية من خلال التحليل المباشر وكان استخدام الجهاز المعني لفحص الوسائط الرقمية أمرًا شائعًا .بمرور الوقت، أدى الاستخدام المتزايد للأجهزة المليئة بكميات هائلة من المعلومات إلى جعل التحليل المباشر غير فعال .في النهاية، تم إنشاء أدوات الادلة الجنائية الرقمية لمراقبة البيانات الموجودة على الجهاز دون إتلافه .في الوقت الحاضر، يمكن تصنيف أدوات الادلة الجنائية الرقمية على أنها أدوات رقمية مفتوحة المصدر للأدلة الجنائية وأدوات أجهزة الادلة الجنائية الرقمية وغيرها الكثير.

الأكاديمية العربية الدولية
Arab International Academy

شكراً لحضوركم

آمل ان تكونوا قد حققتم الفائدة