أمن المعلومات

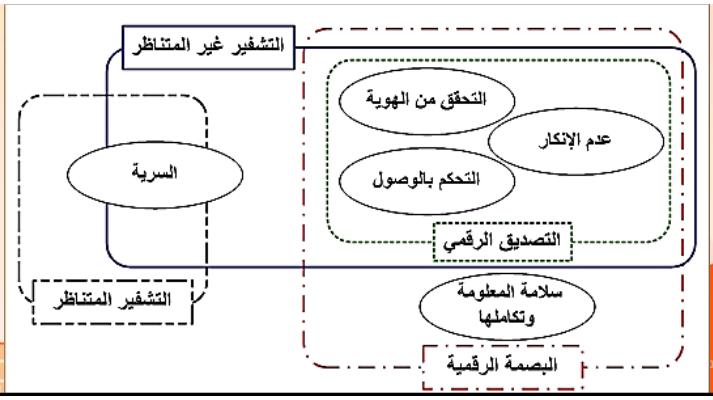
GS224-4

وسائل تحقيق اهداف أمن المعلومات

مقدمة

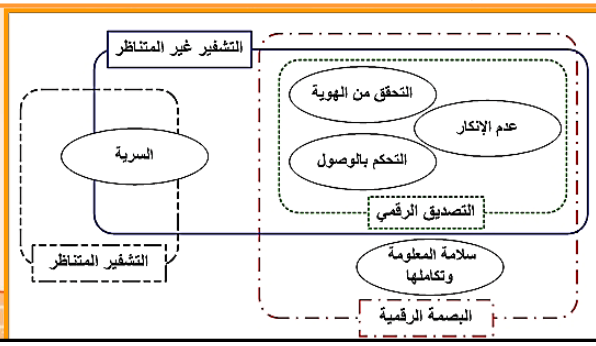
التقنيات الرئيسية المستخدمة كوحدات بناء اساسية لتحقيق بعض اهداف أمن المعلومات كالتحقق من الهوية ، والتحكم بالوصول، والسرية، وسلامة المعلومة و تكاملها ، هى :

1. التشفير (Encryption) : المتناظر و غير المتناظر
2. التوقيع الرقمى (Digital Signature)
3. البصمة الرقمية (Hash Value)



مقدمة

- **السرية** : يمكن تحقيقها باستخدام التشفير المتناظر أو غير المتناظر أو بهما معا.
- **التحقق من الهوية، والتحكم بالوصول، وعدم الانكار** : يمكن تحقيقها باستخدام التشفير غير المتناظر و التوقيع الرقمى معا.
- **سلامة المعلومة وتكاملها**: يمكن تحقيقها باستخدام البصمة الرقمية .
- **توفر الخدمة والمعلومة** : يمكن تحقيقها باستخدام الاجهزة و البرامج الرديفة و أنظمة الحماية من هجمات الحرمان من الخدمة (DoS).
- **التدقيق و المتابعة** : يمكن تحقيقها باستخدام تقنيات المتابعة و تسجيل الاحداث المرفقة بنظم التشغيل أو التى يتم بنائها من قبل شركات متخصصة فى ذلك.



التقنيات الرئيسية لتحقيق اهداف أمن المعلومات

1 – تحقيق السرية : التشفير (Encryption)

التشفير هو أحد تقنيات العمل الأساسية المستخدمة في مجال أمن المعلومات. فالتشفير يساعد بشكل أساسي على الحفاظ على سرية المعلومات. ومن خال تطبيقات ُمبتكرة يمكن للتشفير أيضاً ُ التأكد من تكامل المعلومات والتأكد من هوية المرسل. وكل العمليات التجارية التي يتم إجراؤها عبر الإنترنت تستخدم التشفير للحفاظ على أمن المعلومات. ويضمن التشفير أن المعلومات المالية، مثل أرقام بطاقات الائتمان، المرسلة عبر شبكة الإنترنت لا يتم سرقتها أثناء عملية النقل. وفي كثير من الحالات فإن التشفير ليس أمراً مناسباً فقط بل هو أمر مطلوب بموجب القانون الوطني، لذا فإن التشفير جزء أساسي من البنية التحتية التجارية و الإدارية الحديثة.

مثال : ماذا نتوقع عندما نقوم بإرسال المعلومات عبر الانترنت؟ بالتأكيد نريد أن تصل المعلومات إلى الشخص المرسل إليه. لكن هل ذلك يكفي؟ ماذا إذا كانت الرسالة: "ليس لدي المال لدفع فاتورة الرسوم الدراسية لهذا الفصل الدراسي. يرجى تحويل 1000 دولار لحسابي الجاري رقم (#00000101010) في الاتحاد الائتماني، ورقم التوجيه المصرفي هو (123456789) وفي حال وجود أي صعوبة فإن كلمة السر هي (hello123).

التشفير (Encryption) :- «تحويل نص واضح أو مقروء إلى نص غير واضح، أو نص معمى، بطريقة تستطيع بواسطتها الأطراف المتعارف عليها فقط أن تحل التعمية وتحول النص الغير واضح أو المعمى إلى النص المقروء». ويمكن من ذلك استخلاص تعريف التّشفير التالي: «التّشفير هو العملية التي من خلالها يتم تغيير البيانات وجعلها في شكل غير مفهوم أو غير مقروء (أي تعميتها) ، بحيث لا يستطيع إرجاعها إلى وضعها الأصلي إلا الشخص أو الأشخاص المصرّح لهم فقط، الذين لديهم الأدوات اللازمة لذلك».

1 – تحقيق السرية : التشفير (Encryption)

- يعتبر التشفير هو اهم حجر في بناء امن المعلومات و لكنه ليس الحجر الوحيد على اية حال ، حيث يمكن القول ان اكثر وسائل امن المعلومات فعالية هي التشفير و يمكن تعريفه أيضا على النحو التالي **:"تشفير المعلومات هو تغيير مظهرها بحيث يختفي معناها الحقيقي".** فعن طريق تحوير صورة المعلومات بحيث تكون غير مفهومة لمن يتلصص عليها (تعميتها)، يستطيع إخصائيو امن المعلومات منع الأشخاص غير المرخص لهم من الاطلاع على هذه المعلومات، وبذلك يحقق التشفير **السرية**. كما ان التشفير يمكن استخدامه بهدف تحقيق **سلامة المعلومات** لان المعلومات التي لا يمكن قراءتها او الاطلاع عليها لا يمكن بالتالي تعديلها او تزييفها. و يستخدم التشفير كأساس لبعض البروتوكولات (مجموعة متتالية متفق عليها من الأفعال لتنفيذ مهمة معينة) التي تضمن إتاحة الموارد لمن يحتاجها (**توفر الخدمة**).
- يتضح من ذلك ان التشفير يقع في موقع الأساس من عناصر ضمان أمن المعلومات الأساسية : **السرية** و **سلامة المعلومات** و **توفر الخدمة**.
- وبرغم من ان التشفير يعتبر أداة هامة من أدوات امن المعلومات إلا انه يجب الا نبالغ في هذه الأهمية، فالتشفير لا يحل جميع مشاكل امن المعلومات. اضف الى ذلك الى انه اذا لم يستخدم التشفير بالشكل المناسب، فقد لا يكون فعالا في تأمين المعلومات، أو قد يؤدى الى سوء أداء النظام ككل. فالتشفير الضعيف يمكن ان يكون بالفعل اسوء من عدم التشفير لأنه يعطى إحساسا زائفا بالأمن، لذلك فمن الأهمية بمكان معرفة المواقف التي يكون فيها التشفير مفيدا و أن يتم استخدامه بكفاءة.

1 – تحقيق السرية : التشفير (Encryption)

الاخطار التي يمكن التغلب عليها بواسطة التشفير :

1. الاطلاع على المعلومات المحظورة.
2. محاولات تعديل المعلومات المنقولة او مرسلة.
3. إعادة توجيه المعلومات الى جهة أخرى.
4. تأخير إيصال بعض أجزاء المعلومة.
5. تغيير محتوى المعلومات المتبادلة.
6. إقحام معلومات مزيفة ضمن معلومات حقيقية متبادلة.
7. تغيير كلمات السر الخاصة بالمستخدمين.
8. انتحال شخصية مستخدم حقيقي.
9. تعديل معلومات مخزنة على نظام المعلومات.

1 – تحقيق السرية : عناصر التشفير

ويتألف التّشفير من عمليتين أساسيتين هما: التّشفير، وفك التّشفير. وحسب نوعية التّشفير، فإنّه يمكن استخدام مفتاح تشفير أو أكثر لإتمام هاتين العمليتين.

- «النّص الصريح»(Plain Text): وهو الرسالة أو(البيانات) الأصليّة قبل إجراء أيّ عمليّة عليها.
- "النص المشفّر"(Cipher Text) : يطلق على الرسالة المشفّرة بعد أن تشفّر.
- "التّشفير"(Encryption): تحويل الرسالة من نصّ صريح إلى نص مشفّر.
- "فك التّشفير"(Decryption): استرجاع النّصّ الصريح من النصّ المشفّر.
- "خوارزميّة التّشفير"(Encryption Algorithm): مجموعة الخطوات والعمليّات الرياضيّة التي يتم اتّباعها لتحويل النّص الصريح إلى نص مشفّر.
- "خوارزميّة فكّ التّشفير"(Decryption Algorithm): وهي الخوارزميّة العكسيّة لخوارزميّة التّشفير؛ لاسترجاع النّص الصريح من النّص المشفّر.
- "تحليل الشيفرة"(Cryptanalysis)، ويطلق عليها أيضًا(كسر الشيفرة)، وتعني التقنيات المستخدمة لفكّ تشفير رسالة بطريقة غير شرعيّة، أي كسر تشفيرها بوساطة طرف غير مصرّح له، ولا يعرف المفاتيح اللازمة لذلك[1].
- «المفتاح السِّرّي»(Key) : وهو عبارة عن قيمة غير معتمدة على الرسالة يختارها نظام التّشفير أو المستخدم.

التقنيات الرئيسية لتحقيق اهداف أمن المعلومات

2 - تحقيق عنصر التحقق من الهوية و عدم الانكار

يستخدم **التشفير** مع **التوقيع الرقمي** لتحقيق عناصر التحقق من الهوية و عدم الانكار بحيث يتم انتاج توقيع رقمي باستخدام المفتاح السري للمستخدم و الذى لا يعرفه و لا يملكه إلا الشخص او الجهة المعنية فقط، و بهذه الطريقة يتم التحقق من هوية المستخدم و من اصل منشأ المعلومات، من انه الشخص المعنى او الجهة المعنية لا غيرها. كذلك يتم تحقيق عنصر عدم الانكار حيث لا يستطيع المرسل (المستخدم) إنكار انه ارسل الرسالة (المعلومة) لأنه وقع عليها بمفتاحه الخاص الذى لا يعرفه و لا يملكه غيره.

التقنيات الرئيسية لتحقيق اهداف أمن المعلومات

3 - تحقيق هدف التحكم بالوصول

في المنشآت الصغيرة وفي البيئات التي لا تتطلّب أدوات تحكّم بالوصول خاصّة تضفي مزيدًا من الحماية لمواردها يمكن الاكتفاء باسم المستخدم وكلمة المرور للتحكّم بالوصول للموارد. وفي هذه الطريقة يُمنح المستخدم الصلاحيّات اللازمة التي بمجرد نجاح عمليّة الدخول تكون متاحة له كما هي الحال في البرامج التطبيقيّة التي تُدير مستخدميها بنفسها، وبذلك يكون للمستخدم حقّ الوصول إلى الموارد (ملفات، وطابعات، وقواعد وبيانات، وبرامج، ... إلخ) التي يحتاج إليها دون غيره من المستخدمين، وبذلك يتحقق عنصر التحكّم بالوصول. أمّا في حالة المنشآت الكبيرة التي يوجد فيها برامج تطبيقيّة كثيرة، يصعب معها استخدام اسم مستخدم وكلمة مرور لكل برنامج، والمنشآت ذات الطابع الحساس، فيلزم استخدام تقنيات التحكّم بالوصول التخصّصية، مثل: تقنية تسجيل الدخول الواحد، ومصفوفات التحكّم بالوصول، وأنظمة كشف التطفل، وأنظمة منع التطفل.

3 - تحقيق هدف التحكم بالوصول

تسجيل الدخول الأحادي فكرة استخدام تقنية تسجيل الدخول الواحد (Single Sign-on)، حيث يدخل المستخدم مرّة واحدة من خلال نظام موحّد مخصّص لهذا الغرض، وبعدئذ تكون جميع موارد الشبكة التي يحتاج إليها في متناوله، وفق الصلاحيّات الممنوحة له. قد يبدو للوهلة الأولى أنّ هذه الطريقة تضعف من أمن تلك الأنظمة، لكن الواقع يشير إلى أنّها تقوّي أمنها؛ لأنّ المستخدم الذي لديه عدد كبير من أسماء المستخدمين وكلمات المرور عادة ما يضطر إلى تسجيلها في مذكراته أو في حاسبة الشخصي؛ لتسهيل عمليّة الرجوع إليها وتذكرها، وهذا أمر ينافي السياسات الأمنيّة لكلمات المرور؛ لأنّها تكون بذلك عرضة لانكشافها للآخرين.

من تقنيات الدخول الأحادي :

1. **نظام "كيربورس"** (Kerberos) للتسجيل الأحادي على الشبكات الموزعة.
   - يخدم نظام الخادم/العميل
   - يستخدم نظم التشفير المتناظر لتشفير كلمات المرور عبر الشبكة
   - يحتوي على مركز توزيع المفاتيح والذى يحتفظ بجميع ارقام المستخدمين السرية.
2. **تقنية العميل اللطيف** (Thin Client) للتسجيل الأحادي على الشبكات المركزية.
   - تستخدم نهايات طرفية للدخول على الخادم المركزي عبر الشبكة
   - النهايات الطرفية عبارة عن واجهات عمل مادية فلا تعالج بها البيانات او تخزن و لا نظام تشغيل محلى، بها مجموعة أوامر بدائية للتواصل مع الخادم المركزي
   - التحكم و المعالجة مركزية .

3 - تحقيق هدف التحكم بالوصول

مصفوفة التحكّم بالوصول

مصفوفة التحكّم بالوصول (Access Control Matrix) هي جدول يحتوي المستفيدين كصفوف، والموارد كأعمدة، ويحدّد ما العمليّات الممكنة لكل مستفيد على كل مورد، كما هو موضّح في الجدول .

المستفيد	ملف١	ملف٢	ملف٣	ملف٤
أحمد	قراءة	قراءة، كتابة	قراءة	قراءة، كتابة
علي	تحكم كامل	لا يوجد	تحكم كامل	قراءة
محمد	قراءة، كتابة	لا يوجد	قراءة	تحكم كامل
صالح	تحكم كامل	تحكم كامل	لا يوجد	لا يوجد

مصفوفة التحكّم بالوصول.

يحتوي كل صف إمكانات (Capabilities) المستخدم المحدّد في ذلك الصف.

3 - تحقيق هدف التحكم بالوصول

أنظمة كشف التطفل (IDSs)

يقصد بكشف التطفل عمليّة كشف الاستخدام غير الشرعي أو الهجوم على الأجهزة والشبكات وأنظمة الاتصالات، والمهمة الأساسيّة لأنظمة كشف التطفل (Intrusion Detection Systems-IDSs) هي التقاط أيّ شيء مريب أو مشكوك فيه يحدث في الشبكة، والتنبيه على ذلك بشكل رسالة (فلاش) على شاشة مدير النظام أو رسالة قصيرة (SMS) أو بريد إلكتروني. وعادة ما تقوم أدوات كشف التطفل بتفحص سيل البيانات وسجلّات الأحداث، وكشف أي بيانات غير طبيعيّة والتنبيه عليها.

تتكوّن أغلب أنظمة كشف التطفل من ثلاثة مكوّنات رئيسة هي: الحسّاسات (Sensors)، وأدوات التحليل (Analyzing tools)، و واجهات التواصل مع مديري الأنظمة (Interfaces). تُجمّع الحسّاسات البيانات وأنشطة المستخدمين وترسلها لأدوات التحليل، وتُحلّل أدوات التحليل البيانات والأحداث الواردة إليها من الحسّاسات، والتعرّف إلى أيّ بيانات أو أنشطة تبدو مريبة أو غير طبيعيّة، وعند وجود أيّ نتائج إيجابيّة لدى أدوات التحليل، تُرسل إلى واجهات التواصل مع مديري الأنظمة لإخطارهم بوجود شيء مُريب وغير طبيعي.

أنواع أنظمة كشف التطفل:

1. أنظمة كشف التطفل الشبكية:
   - أجهزة لكشف التطفل على الشبكة (حاسوب خاص)، تربط بالشبكة.
   - تنسخ كل حزم البيانات المارة بناقل الشبكة
   - تحلل و تفحص حزم البيانات للبحث عن أي حزم مريبة.
2. أنظمة كشف التطفل على الأجهزة:
   - برمجيات تنصب على الحواسيب لمراقبة أي نشاط مريب عليها
   - لمتابعة المستخدمين
   - تركب على الخوادم المهمة و الحساسة.

3 - تحقيق هدف التحكم بالوصول

أنظمة منع التطفل(IPSs)

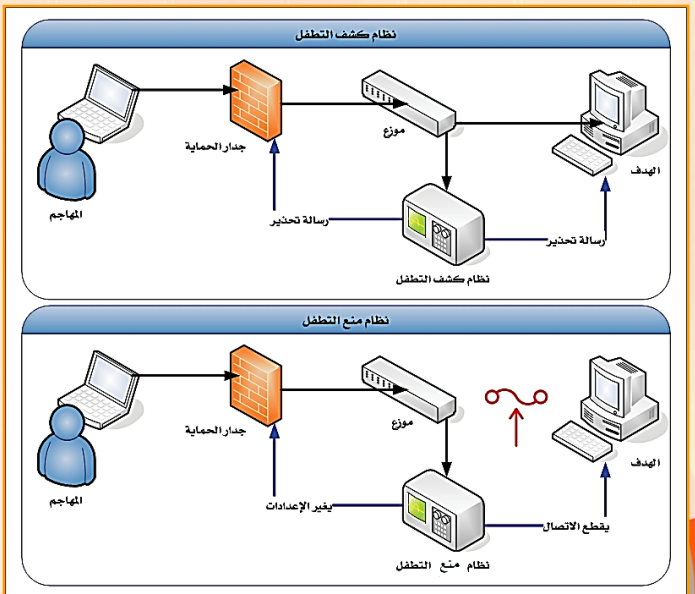
في أنظمة كشف التطفل يُكشف عن البيانات والأنشطة غير الطبيعيّة، ومن ثم التنبيه عليها فقط. أمّا أنظمة منع التطفل(Intrusion Prevention Systems-IPSs) فتكشف البيانات والأنشطة غير الطبيعيّة، ثم تمنعها من الوصول إلى أهدافها، كما يوضح ذلك الشكل .

وبذلك فإنّ أنظمة منع التطفل تقوم بخطوات استباقيّة لمنع المتطفّل من الوصول إلى أهدافه. فكما يتّضح من الشكل ، يقطع جهاز منع التطفل المضمّن(Inline IPS) الاتصال بين المهاجم والهدف عند وجود بيانات مريبة، كما يتدخل مباشرة، ويعدّل قوائم التحكّم بالوصول(ACLs) لجدار الحماية.

أنواع أنظمة كشف التطفل:

1. أنظمة منع التطفل الشبكية:
2. أنظمة منع التطفل على الأجهزة:

3 - تحقيق هدف التحكم بالوصول



التقنيات الرئيسية لتحقيق اهداف أمن المعلومات

4 - تحقيق هدف سلامة المعلومة و تكاملها (النزاهة)

4 - تحقيق عنصر سلامة المعلومة وتكاملها

يمكن التحقّق من سلامة الرسالة وخلوّها من أيّ حذف أو تعديل أو إضافة باستخدام البصمة الرقميّة. فبمجرد تطبيق تقنية البصمة الرقميّة سيتم كشف أيّ تعديل أو حذف أو إضافة، وبذلك يتحقق عنصر سلامة المعلومة وتكاملها.

كما يمكن تحقيق سلامة البيانات وضبط عمل المستخدمين من خلال تحديد خيارات محدّدة (مثل القوائم المنسدلة)، التي يجري التعامل معها لاختيار البيانات وإدخالها في الأنظمة والبرامج المختلفة، ثم تنفيذ العمليّات على تلك البيانات (كالتعديل والحذف)، وفق صلاحيّات محدّدة ودقيقة، ومن ذلك أيضًا التحكّم بالملفّات المهمة وحجب إمكانيّة الوصول إليها عن المستخدمين العاديين، وتزويد البرامج التطبيقيّة بوسائل التحقّق من صحة البيانات المدخلة، ورفض البيانات غير المعقولة أو غير المتوقّعة حسب طبيعة حقول تلك البيانات، كإدخال بيانات مالية كبيرة في حقول صغيرة (أو العكس)، أو إدخال حروف في حقل تاريخ مثلًا. أمّا قواعد البيانات فيجب أن يُحصر التعامل معها في أشخاص محدّدين ذوي قدرة وكفاءة عالية.

التقنيات الرئيسية لتحقيق اهداف أمن المعلومات

5 - تحقيق هدف توفر المعلومة (الديمومة)

5 - تحقيق عنصر توفر المعلومة

بعد ظهور هجمات تعطيل الخدمة (DoS)، أصبح عنصر توفر المعلومات عنصرًا أساسيًا في أمن المعلومات، ومع تقدم استخدام الإنترنت وانتشارها، أصبح توفر مواقع الخدمات على الشبكة أمرًا ضروريًّا يحتم على مديري هذه المواقع العناية التامة بتوفر (ديمومة) المواقع، وحصر خروجها من الخدمة في أضيق نطاق. وهناك وسائل أساسية لتحقيق عنصر توفر المعلومات، وهي:

- أن يكون هناك سعة كافية في الشبكة والأنظمة والخوادم وأجهزة التخزين ومركز البيانات (Data Center) بشكل عام، من أجل أن تعمل بمستوى جيّد وباستمرارية وبكفاءة عالية.
- القدرة على العودة بعد حدوث الأعطال أو التوقّفات بطريقة سريعة وآمنة.
- تجنّب وجود نقطة العطل الوحيدة (Single Point of Failure)، الذي تتسبب في التوقّف الكامل في حال تعرضها للعطل.

5 - تحقيق هدف توفر المعلومة

- أخذ نسخ احتياطيّة من البيانات والأنظمــة والبرامج، وكذلك من إعدادات أجهزة الشبكة، ســواءً المحلية(LAN)، أم الواسعــة(WAN)، وأي أجهزة أخرى حسب طبيعة عمل المنشأة؛ للرجوع إليها عند الحاجة.
- توفير أجهزة وأنظمة وتقنيات رديفة(في نفس مركز البيانات) تعمل جنبًا إلى جنب مع الأجهزة والأنظمة والتقنيات الأساسيّة، حسب الحاجة والأهمية.

- الحماية من التأثيرات السلبية للمكوّنات الطبيعية كالحرارة والرطوبة والغبار والملوثات والكهرباء الساكنة، مع ضرورة تأريض الدوائر الكهربائيّة وتوفير موانع الصواعق.
- توفير مركز بيانات رديــف(Disaster Recovery Data Center)؛ لاستخدامه عند وقوع الكوارث، ويتم التحــول إليه آليًّا عند وقوع الأعطــال الكبيرة أو الكوارث المعلوماتيّة، التي تسبّب توقّــف مركز البيانات الرئيس. ويجب في هذه الحالة توفير جميع الأجهزة والبرامج وأجهزة الربط وخطوطها اللازمة في مركز البيانات الرديف والرئيس. **تقنيات التناوب**: التناوب اليدوي (نشط/غير نشط)، او التناوب الآلي (نشط/نشط).

5 - تحقيق هدف توفر المعلومة

- الحماية من التأثيرات السلبية للمكونات الطبيعية كالحرارة و الرطوبة والملوثات و الكهرباء الساكنة.
- توفير مركز بيانات رديف لاستخدامه عند وقوع الكوارث القاهرة و تحول العمل اليه آليا، مع مراعاة:
  - تحديث البيانات في المركز الرديف بشكل مستمر.
  - سهولة و ضمان التحول السلس و السريع من المركز الرئيس الى الرديف عند الحاجة.
- التدريب الجيد للعاملين على التعامل مع الأعطال، والتحويل الى التجهيزات الرديفة، و متابعة ذلك و ادارته.
- استخدام أنظمة مكافحة البرامج الضارة .
- استخدام أنظمة الطاقة الكهربائية الاحتياطية.
- استخدام أنظمة كشف هجمات تعطيل الخدمة (DoS) ومكافحتها.

وتشير الدراسات الحديثة إلى أنّ عدم توفــر المعلومة لا يُعزا للأعطال والأسباب المتعلّقة بالأجهزة والبرمجيات، وإنّما قد تحدث كذلك بسبب أخطاء الفنيين ومديري الأنظمة، أو بسبب عدم القدرة على التعامل مع الإنذارات المبكرة أو إهمالها، وتؤكد تلك الدراسات على ضرورة التدريب والتأهيل الجيّد لجميع من يتعامل مع المعلومة من: مستخدمين وفنيّين ومديرين.

6 - تحقيق هدف المتابعة و التدقيق

6 - تحقيق عنصر المتابعة

يمكن تحقيق عنصر المتابعة والتدقيق على مستويات مختلفة، تتراوح من مجرّد متابعة ما يجري على الحاسب الشخصي، إلى متابعة مراكز البيانات والشبكات الكبيرة، وهناك وسائل وأنظمة تدقيق ومتابعة لكل مستوى، منها:

- سجلّات أحداث نظام التشغيل(Operating System Events Log) التي ترد رفق أنظمة التشغيل، لمتابعة الأحداث التي تتم على مستوى الأجهزة الشخصية أو محطات العمل وتدقيقها.
- سجلّات أحداث الشبكة(Network Events Log) الخاصة بأنظمة تشغيل الشبكات وإدارة المستخدمين، لمتابعة ما يدور في الشبكة وما يقوم به المستخدمون، وأوقات تلك الأحداث وتواريخها.

6 - تحقيق هدف المتابعة و التدقيق

- سجلّات أحداث قاعدة البيانات(Database Events Log) الخاصة بقواعد البيانات، لمتابعة ما يدور في قواعد البيانات، وأوقات تلك الأحداث وتواريخها.

ويمكن استخدام هذه الأنظمة والاستفادة منها في إجراء عمليّات المتابعة والتدقيق بإحدى الطرق التالية:

- إجراء عمليّات تدقيق ومتابعة تاريخيّة(Historical) بعد انتهاء الأحداث، ثم اتخاذ الإجراءات المناسبة وفقًا لنتائج هذه العمليّات.
- إجراء عمليّات تدقيق ومتابعة حيّة مباشرة(Online) وقت وقوع الأحداث لإخطار المسؤولين عن معالجة تلك الأحداث في حينه بما يجري، ومن ذلك: إرسال رسالة بريد إلكتروني، أو رسالة قصيرة(SMS) على الهاتف المحمول ليعملوا على حلّها.
- أجراء عمليّات تدقيق ومتابعة وقائية(Preventive)، بحيث تعالج أنظمة التدقيق نفسها الأخطاء عند وقوعها مباشرة، أو على الأقل إيقاف مصدر الخطر أو الخلل دون انتظار تدخل المسؤولين.