GS224-3

أمن المعلومات

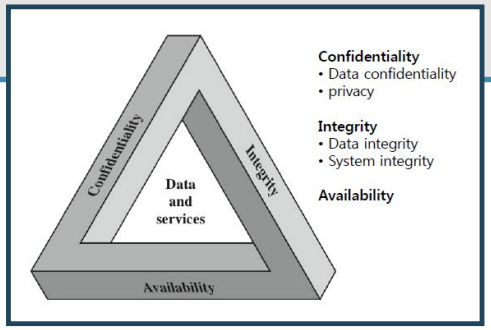
56ypzw5

IT-GS224 امن المعلومات Copy invite link

اهداف أمن المعلومات

الاهداف

- التعريف بعناصر أمن المعلومات و ماهيتها .
- تحديد عناصر أمن المعلومات و أمثلة لكل منها .
- توضيح دور عناصر أمن المعلومات و تأثير غيابها .
- إبراز دور التكامل بين عناصر أمن المعلومات لتوفير الحماية اللازمة للمعلومات .

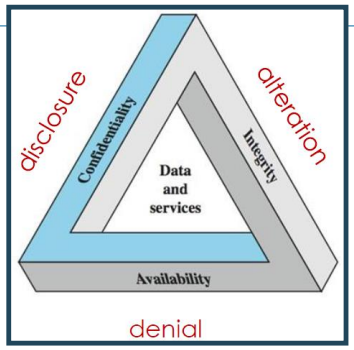


عناصر (اهداف) أمن المعلومات

وسواء أكانت المعلومة مستقرة في قواعد بيانات أو وسائط تخزين ثابتة، أم يتم تبادلها بين طرفين، فإنه لا بد من وجود القناعة التامة بتحقيق حد معين من أمن المعلومات في حال استقرارها أو نقلها. ويتحقق هذا الحد من خلال عناصر أمن المعلومات، التي هي عبارة عن عدة عناصر كل واحد منها يغطي جانبا مهما من جوانب آمن المعلومات، وإذا كان هناك خلل أو غياب لأحد هذه العناصر، فإنه سيكون هناك قصور في أمن المعلومة من ذلك الجانب، لقد حدد بعض المؤلفين ثلاث ركائز أساسية لأمن المعلومات هي: **السرية** (Confidently)، و**سلامة المعلومة وتكاملها** (Integrity)، و**التوفر** (Availability)، وأطلق على ذلك مثلث (CIA). إلا أن الاتحاد العالمي للاتصالات في توصياته، قد حدد العناصر الأساسية لأمن المعلومات في سبعة عناصر رئيسة، وهي: **التحقق من الهوية**، و**التحكم بالوصول**، و**السرية**، و**سلامة المعلومة وتكاملها**، و**عدم الإنكار**، **وتوافر أو ديمومة المعلومة**، و**المتابعة والتدقيق**.

عناصر أمن المعلومات

يمكن تعريف عناصر أمن المعلومات بأنها: " مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة، بحيث يغطي كل عنصر من هذه العناصر جانبا من جوانب الحماية المطلوبة ". ومعنى ذلك هو أن تتكامل هذه العناصر حتى توفر الحماية المطلوبة، وفي حال فقد اي منها فسيكون هنالك خلل أمني في ذلك الجانب الذي يغطيه هذا العنصر،



1- التحقق من الهوية (Authentication)

تعني الخدمة التي يمكن من خلالها التحقق من هُوية الشخص (أو الجهة) وأنه الشخص المعني لا غيره. فعند اتصال شخصين (أو جهتين) بعضهما ببعض، فلابد من أن يتعرف كل منهما إلى الآخر، لضمان أن يتخاطب كل منهما مع الشخص أو الجهة المعنية وليس مع غيرها. بعبارة أخرى: فإن التحقق من الهوية هو التحقق من أن المستخدم لنظام ما هو بالفعل من ادعى أنه ذلك المستخدم ، وفي حال نقل المعلومات، فإنه يجب التحقق من هوية المرسل لضمان أن المعلومة قادمة من مصدرها الحقيقي، وكذلك يجب التحقق من هوية المستلم لضمان أن المعلومة ذ اهبة إلى وجهتها الصحيحة.

تبدأ عملية التحقق من الهوية بالتعريف بالهوية أو تحديد الهوية، ويمكن تحقيق ذلك من خلال اسم المستخدم أو رقم الحساب مثلا. إن تحديد هوية الشخص أو التعريف به رقميا (إلكترونيا) أمر مهم، وقد يكون صعبا في بعض الأحيان؛ إذ إن الشخص الواحد نفسه قد يكون لديه أكثر من هوية رقمية.

1- التحقق من الهوية (Authentication)

- **معايير طرق تحديد الهوية :**
  1. ان تكون الهوية فريدة بمعنى ان تكون غير قابلة للتكرار.
  2. أن تكون غير مفصحة عن معلومات المستخدم و وظيفته و الغرض من الوصوله الى المعلومة.
  3. أن لا تكون مشتركة بين المستخدمين.
  4. أتباع معايير المعتمدة عند المؤسسة عند أنشاء حسابات ألمستخدمين.
- **عناصر التحقق من الهوية :**
  1. التحقق من هوية الشخص أو الجهة : التحقق من هوية طرفى الاتصال فى جميع مراحله و عدم قدرة المعتدى على انتحال شخصية أحد الطرفين.
  2. التحقق من أصل منشأ المعلومة : التحقق من أصل المعلومة بأنها صادرة من جهتها الأصلية – تأكيد مصدر المعلومات – بمعنى ارسلت من الجهة التى تدعى انها ارسلتها.

1- التحقق من الهوية (Authentication)

1. **التحقق باستخدام معيار واحد**: هذا المعيار هو **"ماذا تعرف؟"**، كاستخدام كلمات المرور أو أرقام التعريف الشخصية (Personal Identification Number-PIN) ويعتمد هذا المعيار في التحقق من الهوية على طلب (إدخال) معلومة لا يعرفها إلا الشخص المعني فقط ، ويعد من أدنى درجات التحقق من الهوية.
2. **التحقق باستخدام معيارين**: ويتم ذلك باستخدام معيار **"ماذا تعرف؟"**، بالإضافة إلى معيار آخر هو **"ماذا تملك؟"**، وتعتمد هذه الطريقة في التحقق من الهوية على طلب (إدخال) معلومة لا يعرفها إلا الشخص المعني فقط، ومعلومة أخرى لا يملكها الا الشخص نفسه.
3. **التحقق باستخدام ثلاثة معايير**: ويتم ذلك باستخدام معيار **"ماذا تعرف؟"**، ومعيار **"ماذا تملك؟"**، بالإضافة إلى معيار ثالث هو **"من أنت؟"**. وتعتمد هذه الطريقة التحقق من الهوية على طلب (إدخال) معلومة لا يعرفها إلا الشخص المعني فقط، ومعلومة أخرى لا يملكها إلا الشخص نفسه، ومعلومة ثالثة من واحدة أو أكثر من **خصائص الشخص الحيوية** التي تميزه من غيره، كبصمات الأصابع والعين، وأبعاد راحة اليد والوجه، والتعرف إلى الصوت، وغير ذلك. وتوفر هذا الطريقة أعلى درجات التحقق من الهوية، ولكنها تحتاج الى أجهزة و برمجيات إضافية، وتعد اكثر تعقيدا من سابقاتها.

2- التحكم في الوصول (Access Control)

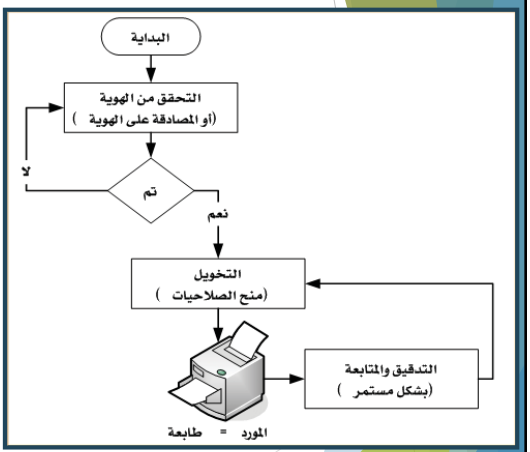
التحكم بالوصول هو طرق (أو وظائف) الحماية التي تتحكم بوصول المستخدمين أو الأنظمة إلى موارد المنشأة، كالأجهزة الرئيسة والبيانات المركزية، أو بعبارة أخرى: منع الاستخدام غير المرخص به للموارد . فتلك الطرق هي التي تحمي الأنظمة وموارد المنشأة المختلفة من الوصول غير الشرعي، كما أنها تساعد ي تحديد مستوى التخويل (Authorization) المصرح به بعد نجاح عملية التحقق من الهوية.

- **مراحل التحكم بالوصول**: لكى يتمكن مستفيد ما - مستخدم أو برنامج أو عملية ما أو غيره – من الوصول الى مورد ما و استخدامه أو الاستفادة منه فإنه يجب ان يمر برمحلتين أوليتين للتحكم بوصوله الى ذلك المورد هما : التحقق من الهوية و التخويل ثم مرحلة ثالثة بعد وصوله للمورد و استخدامه وهى التدقيق و المراقبة ، وكما هو موضح فى الشكل التالى .

2- التحكم في الوصول (Access Control)

مراحل التحكم بالوصول

1. **التحقق من الهوية** : هو الطريقة للتأكد من أن المستفيد هو من أدعى انه هو، وبشكل عام ، تلزم التحقق من المستفيد كخطوة أولى للوصول الى موارد المؤسسة.
2. **التخويل أو الترخيص** : وهى التاكد من أن المستفيد الذى جرى التعرف عليه و المصادقة علي هويته لديه الصلاحيات و الامتيازات التى تخوله استخدام المورد وتنفيذ العمليات التى يريدها عليه.



2- التحكم في الوصول (Access Control)

2. **التخويل او الترخيص :** معايير التحكم فى منح الصلاحيات و مراجعتها دوريا
   - المنح بناء على دور المستخدم و مهامه فى المؤسسة و العمل الذى يقوم به.
   - المنح بناء على الموقع الذى به المستخدم نسبة الى المورد.
   - المنح فى أوقات محددة للتعامل و التواصل فى اوقات و تواريخ مع المورد.
   - المنح بناء على الاجراء (العملية) المزمع اجراءها على البيانات و المورد المستخدم.
   - منح الصلاحيات للمجموعات اذا احتاجوا لنفس الصلاحيات على بيانات و موارد معينة .
   - عدم السماح الافتراضى او التلقائي (البدء من صفر صلاحيات ثم الاضافة حسب الحاجة)
3. **التدقيق و المتابعة :** متابعة عملية المستخدمين على الموارد و تسجيلها من أجل مراجعتها و معرفة اى خلل او تجاوز فى الصلاحيات الممنوحة لكل مستخدم و اتخاذ الاجراءات المناسبة بناء على النتائج :
   - حجب المستخدم نهائيا أو تعطيل حسابه وبذلك لا يمكنه استخدام اى مورد نهائيا
   - حجب المورد عن جميع المستخدمين بمن فيهم من صدر منه التجاوز
   - حجب صلاحيات معينة من المستخدم الذى صدر منه التجاوز

3- السرية (Confidentiality)

يمكن أن يطلق على هذا العنصر أيضا **الخصوصية**، وتعني الحفاظ على المعلومات من أن يطلع عليها (يقرأها ويفهمها) غير الأشخاص المصرح لهم فقط، أو بعبارة أخرى: منع الكشف غير المصرح به . فعندما أرسل رسالة "سرية"، فإن ذلك يتطلب أن لا يراها إلا المرسل والمرسل إليه فقط. فإن استطاع أحد الاطلاع عليها، فإنه لا يستطيع أن يفهم محتواها، أي يجب أن تكون غير مفهومة له.

هناك العديد من الطرق لتوفير السرية تتراوح بين حجب المعلومة يدويا، وعدم تسليمها إلا للأشخاص المصرح لهم فقط إلى طرق التشفير الحديثة التي تعتمد على خوارزميات رياضية معقدة يصعب فكها، إن لم يكن مستحيلا. من هنا يمكن القول إنه يمكن توفير عنصر السرية من خلال تشفير البيانات سواء، الثابتة منها أو المنقولة، وتطبيق سياسة صارمة للتحكم بالوصول، وتصنيف المعلومات، وتدريب العاملين على أنظمة وسياسات أمن المعلومات تدريبا جيدا.

قد يستطيع المهاجمون إحباط فاعلية عنصر السرية، باستخدام عدة طرق من أهمها: مراقبة الشبكة، وهجوم تصفح الكتف، والهندسة الاجتماعية. قد يكشف المستخدم عن بعض المعلومات الحساسة عمدا، أو عن طريق الخطأ عندما لا يقوم بتشفير هذه المعلومات، أو عندما يقع ضحية لهجمات الهندسة الاجتماعية، أو بسبب اللامبالاة والإهمال وغياب الحس الأمني عند معالجة مثل هذه المعلومات.

من الأمثلة المشهورة على هذه الخروقات أيضا، حفظ ملفات النسخ الاحتياطي مكان خارج المؤسسة، لكنها غير مشفرة (وهوفي حد ذاته إجراء سليم؛ لأنه لابد من حفظ بعض هذه النسخ في مكان بعيد عن المؤسسة، حتى يمكن الرجوع إليها حال تدمير المؤسسة بالكامل، لكن لا بد من تشفيرها، إذا لم يقم نظام النسخ الاحتياطي بذلك). في هذه الحالة أخرجت معلومات المؤسسة من داخل منظومة أمن معلوماتها نهائيا مهما كانت قوتها و وضعت خارجها. فإذا لم تكن مشفرة فهي عرضة للاطلاع عليها وفهمها من قبل الآخرين.

أمثلة: السرية

- **معلومات عن معدلات/درجات الطلبة** تعتبر بيانات سرية بمستوى عالي ، حيث ان بعض القوانين تحدد عرضها للطالب أو ولى أمره أو المستخدمين عندما تتطلب العلاقة المهنية ذلك.
- **معلومات عن تسجيل الطلبة** ربما تعتبر بمستوى سرية متوسط ، حيث الضرر محدود لو كشفت.
- **معلومات عن دليل الهاتف** بمستوى منخفض حيث هي مكشوفة للجميع

4- سلامة المعلومة و نزهتها (Data Integrity)

تعني الخدمة التي من خلالها يمكن الحفاظ على سلامة المعلومة من التعديل، أو الحذف، أو الإضافة، أو إعادة التركيب، أو إعادة التوجيه. وهذا أمر مهم جدا لضمان الثقة في المعلومة وأنها هي المعلومة الأصلية دون زيادة أو نقصان. فقد تكون المعلومة مشفرة وسريتها مضمونة، لكن قد تتعرض للتغيير طالما أنها معلومة إلكترونية. هذا التغيير لا بد من إيجاد طريقة لكشفه، وهوما يوفره هذا العنصر، وقد يترتب على ذلك إلغاء المعلومة وعدم الاعتماد عليها بالكلية.

تعني سلامة المعلومة وتكاملها بأنه تم تلقي الرسالة تماما كما أرسلت بالفعل. وهذا الأمر يولد الثقة لدى المتعامل مع المعلومة من أنها كاملة خ محتواها لم تنقص شيئا، وأنها صحيحة في مضمونها لم يطرأ عليها أي تغيير، وأنه جرت معالجتها أثناء تنقلها (كالحفظ وإعادة الإرسال) بالطرق الصحيحة التي لم تحدث فيها أي تغيير متعمد أو غير متعمد.

يهتم هذا العنصر بعملية "كشف" عدم سلامة المعلومة وتكاملها أكثر من اهتمامه بعملية "منع" التعديل على المعلومة، أو "تصحيح" ذلك التعديل. والسبب ذلك، أن أي تعديل غير مشروع على المعلومة، يجعلها معلومة غير آمنة حتى وإن جرى تصحيح التعديل. فما الفائدة من ذلك التصحيح إذا كانت المعلومة قد وصل إليها آخر وعرفها، وربما احتفظ بنسخة منها لديه؟ وهنا تبرز أهمية كشف إعادة توجيه الرسالة وكشف إعادة تركيبها، لأنه في مثل هذه الأحوال تصل الرسالة كاملة لكنها غير سليمة، ولا تقف قدرة الكشف عند كشف التعديل الذي ينتج عنه تشويه واضح المعلومة، بل يتعدى الأمر ذلك إلى كشف أي تعديل، حتى لو بقيت المعلومة بعده كأنها لم تتغير، ومثال ذلك أن يجري تغيير التاريخ أو الوقت أو اليوم إلى تاريخ أو وقت أو يوم آخرين يبدو لمتلقي المعلومة معه أن شيأ لم يتغير، بينما الواقع غير ذلك.

أمثلة : النزاهة

- **معلومات عن حساسية مريض بمستشفى ذات مستوى نزاهة عالي** : الطبيب يثق بأن المعلومات صحيحة و حديثة ، فمثلا لو ممرضة زورت البيانات تعمدا ، يجب ان تكون هناك إمكانية لقاعدة البيانات لاسترجاع البيانات لأصلها و تتبع البيانات لمعرفة من قام بالتزوير .
- **بيانات التسجيل في مجموعة او منتدى على الشبكة المعلوماتية يعتبر بمستوى نزاهة متوسط.**
- **الاستبانة المجهولة/العامة على الشبكة المعلوماتية تعتبر ذات مستوى نزاهة منخفض** (عدم الصحة امر طبيعي).

5- عدم الانكار / عدم التنصل (Non -Repudiation)

هي الخدمة التي من خلالها يمكن منع أي شخص أو جهة من إنكار أي عملية قاموا بها وكشفهم. فعلى سبيل المثال إذا منحت جهة معينة الصلاحية لجهة أخرى لشراء منتج معين، ثم أنكرت بعد ذلك آنها منحت هذه الصلاحية لتلك الجهة، فإن خدمة عدم الإنكار ستكشف ذلك.

في حالة إرسال رسالة بين طرفين، فإن عدم الإنكار يثبت إرسال المرسل لها ويثبت استقبال المستقبل لها، بحيث لا يمكن لأي منهما إنكار ذلك، وتزداد أهمية هذا الإثبات بازدياد أهمية الرسالة نفسها.

تشمل خدمة عدم الإنكار ايضا إثبات وقوع العمليات والإجراءات الإلكترونية في أوقات وتواريخ معينة عن طريق إلحاق بصمة التاريخ والوقت بالعملية نفسها .

6- توفر المعلومة / الخدمة (Availability)

يقصد بتوافر المعلومة، أن تكون قابلة للوصول إليها واستخدامها حين الطلب من قبل أي شخص أو أي جهة معروفة ومحددة وفي أي وقت (مصرح به). ويمكن القول إن خدمة التوافر هي الخدمة التي تحمي النظام ليبقى متاحا دائما (ومن هنا يطلق عليها أحيانا "الديمومة") وهي موجهة خصيصا إلى أي خلل أو هجوم يمكن أن يؤدي إلى عدم توافر الخدمات، ومن أمثلة ذلك: هجوم الفيروسات، وهجمات حجب الخدمة و منعها (Denial of service-DoS). ويتطلب هذا الأمر في اغالب الأحيان حماية مادية تقنية كتقنيات توفير نظم احتياطية للمعلومات والطاقة الكهربائية.

إن الهدف العام من عنصر توافر المعلومة هو أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليها المستخدم، وأن توفر لها الحماية مما قد يتسبب عطل أو عدم توفر أي منها، وفي حال حدوث الأعطال أو الكوارث المعلوماتية يجب أن تكون هناك شبكة وأجهزة وأنظمة وبرامج بديلة يجري إحلالها آليا وبسرعة فائقة محل تلك التي تعرضت للعطل أو الكارثة، وفق خطة تشغيل للطوارئ يتم إقرارها والتدريب عليها جيدا قبل ذلك.

تجدر الإشارة إلى أنه لابد من الموازنة بين الحماية وتوافر المعلومات. فإذا سمح لأي شخص بالدخول إلى المعلومة في أي وقت ومن أي مكان وبأي طريقة اتصال؛ فإننا بذلك نحصل على درجة عالية من توافر المعلومة، لكن بالمقابل ينتج عن ذلك ثغرات أمنية كبيرة وكثيرة جدا، وبالمقابل، فإنه إذا جرى تقييد المعلومات بشكل كبير من أجل حمايتها سيكون من الصعب توفير المعلومات لجميع الشرائح التي تحتاج إليها في الاوقات المناسبة، والمطلوب هو الموازنة بين ذلك؛ للوصول إلى منزلة وسطية بين المنزلتين.

أمثلة : التوافر

- **نظام يقدم خدمة المصادقة:** مطلوب مستوى توفر عالي ، فمثلا اذا لم يتمكن مستخدم من التواصل مع مورد ما ، قد يؤدى هذا لخسائر مالية
- **موقع عام على الشبكة المعلوماتية لجامعة:** هذا يتطلب مستوى توفر متوسط حيث انه غير حساس و لكن عدم توفر الخدمة امر يسبب الاحراج.
- **دليل هاتف على الشبكة المعلوماتية:** ذو مستوى توفر منخفض حيث عدم توفر الخدمة يسبب مضايقة (يمكن إيجاد حلول أخرى).

7- المتابعة والتدقيق (Auditing)

تهدف المتابعة (ويطلق عليها أحيانا **المحاسبة**) إلى متابعة عمليات المستخدمين والتحقق من فرض سياسات أمن المعلومات، وأنها تطبق بشكل صحيح ودقيق.
كما يمكن استخدام نتائج المتابعة كأدوات تحقيق حالة خرق أنظمة أمن المعلومات لإثبات وقوع بعض الأحداث، وإثبات إدانة المستخدم (آو المتهم) أو براءته من القيام بذلك الحدث.

7- المتابعة والتدقيق (Auditing)

اسباب ضرورة اجراء المتابعة و التدقيق :

1. للتحقق من أن الاجهزة والانظمة والبرامج تعمل بشكل طبيعى وذلك من مراجعة سجلات الاحداث (Log File)، والتى تمكننا من الاجراء المناسب، مثل:
   - معرفة الاخطأ (Errors) التى تقع ، حيث سيوجد فى السجل رسالة خطأ توضح تفاصيله
   - معرفة رسائل التحذير(Alerts) التى تنبئ عن إمكانية حدوث مشكلة ما.
   - توفير المعلومات (Information) عن الاحداث التى تتم لمجرد الاخبار عنها و اخذ العلم بها فقط.
2. لمراقبة العمليات السيئة التى قد يقوم بها المستخدمين (عمدا او سهوا) .
3. للكشف عن عمليات التطفل و الاختراق
4. للمساعدة على استعادة الاحداث و معرفة متطلبات الاجهزة و اعداداتها ، لأستعادتها كما كانت عند حدوث مشكلة.
5. تشكل مصدر قانونيا رسميا للمؤسسة لأثبات الاحداث أو نفيها .
6. تشكل مصدر من المصادر التقارير الرسمية للمؤسسة عن انشطتها و المشاكل التى قد تقع فيها أو في أنظمتها.

7- المتابعة والتدقيق (Auditing)

عند إجراء عمليات التدقيق والمتابعة يجب مراعاة النقاط الآتية:

- حفظ وثائق المتابعة كسجلات الأحداث في مكان آمن.
- استخدام أدوات المتابعة المناسبة يؤدي إلى نتائج أفضل بحجم أقل من المعلومات، حيث إن من أكبر المشكلات التي تواجه أنظمة المتابعة هي كبر حجم معلومات المتابعة التي يلزم مراجعتها، وقد يكون بعضها غير ضروري.
- يجب المحافظة على معلومات المتابعة وسجلات الأحداث من التغيير غير الشرعي حتى لا تفقد مصداقيتها وقانونيتها.
- يجب تدريب العاملين في حقل المتابعة، ومراجعة وثائق المتابعة جيدا؛ للحصول على أفضل النتائج وبأسرع الأوقات.
- حصر صلاحية حذف وثائق المتابعة وسجلات الأعمال في مديري الأنظمة الموثوق بهم فقط.
- لابد أن تشمل المتابعة جميع الأحداث، بما في ذلك الأحداث الخاصة بذوي الصلاحيات العليا، مثل مديري الأنظمة.

7- المتابعة والتدقيق (Auditing)

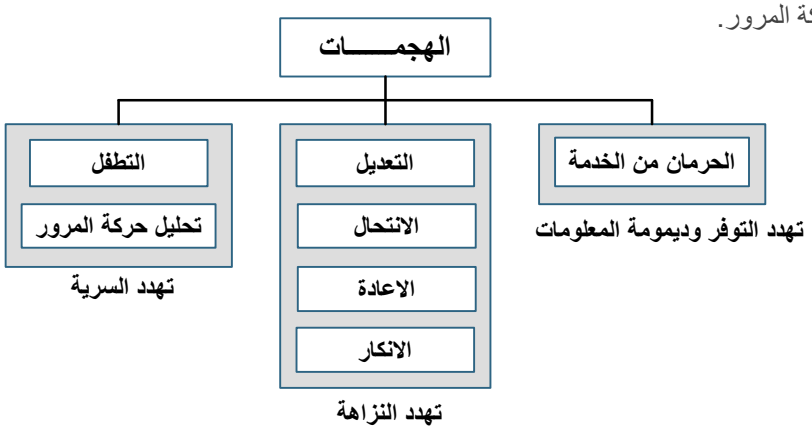
- **الاحداث التى تشملها المتابعة و التدقيق :**

1. **الاحداث على مستوى الانظمة** (كأنظمة التشغيل و الخوادم)، وتشمل: أداء النظام ، محاولات الدخول للنظام، عمليات تعطيل حسابات المستخدمين، عمليات تفعيل حسابات المستخدمين، استخدام ادوات ادارة النظام، استخدام موارد النظام، العمليات الاساسية، طلبات تغيير اعدادات النظام.
2. **الاحداث على مستوى البرامج التطبيقية**، وتشمل: رسائل الخطأ و المستخدمين الذين ظهرت لهم، الملفات التى تفتح و تغلق، التغييرات التى تحدث على الملفات، مخالفات أمن المعلومات و السياسات الامنية التى ترتكب داخل البرنامج.
3. **الاحداث على مستوى المستخدمين**، وتشمل: محاولات تحديد الهوية و التعريف بها و المصادقة عليها (سواء كانت ناجحة او فاشلة)، الملفات و الخدمات والموارد التى يستخدمها، الاوامر التى انشأها، مخالفات أمن المعلومات و السياسات الامنية التى ارتكبها أو تسبب بها.

التهديدات و الهجومات

يمكن أن تتعرض السرية والنزاهة والتوفر للتهديد من خلال عدة أنواع من الهجمات الأمنية. ويمكن تصنيف الهجمات إلى ثلاث مجموعات حسب علاقتها بأهداف (عناصر) الأمن.

هجمات تهدد السرية: بشكل عام، هناك نوعان من الهجمات يهددان سرية المعلومات: التطفل وتحليل حركة المرور.



التهديدات و الهجومات

1. **التطفل**: يشير التطفل إلى الوصول غير المصرح به إلى المعلومات أو اعتراضها .على سبيل المثال، قد يحتوي الملف المرسل عبر الإنترنت على معلومات سرية . يمكن لكيان غير مصرح له (متطفل) اعتراض الإرسال واستخدام المحتويات لمصلحته الخاصة .ولمنع التطفل، يمكن جعل المعلومات غير مفهومة للمعترض باستخدام تقنيات التشفير.
2. **تحليل حركة المرور**: على الرغم من أن تشفير المعلومات قد يجعلها غير مفهومة بالنسبة للمعترض، إلا أنه يمكن الحصول على بعض المعلومات الأخرى من خلال مراقبة حركة المرور عبر الإنترنت .على سبيل المثال، يمكن العثور على العنوان الإلكتروني (عنوان البريد الإلكتروني) للمرسل أو المستقبل ، ويمكن جمع أزواج من الطلبات والردود للمساعدة على تخمين طبيعة المعاملة.

الهجمات التي تهدد النزاهة: يمكن أن تعرض سلامة المعلومات ونزهتها للتهديد من خلال عدة أنواع من الهجمات: التعديل، والانتحال، والإعادة، والانكار.

1. **التعديل**: تعديل المعلومات بعد الوصول إليها أو بعد اعتراضها ، يقوم المهاجم بتعديل المعلومات لجعلها مفيدة له. على سبيل المثال، يرسل عميل رسالة إلى أحد البنوك لإجراء بعض المعاملات. يعترض المهاجم الرسالة ويغير نوع المعاملة لصالحه. لاحظ أنه في بعض الأحيان يقوم المهاجم ببساطة بحذف الرسالة أو تأخيرها للإضرار بالنظام أو الاستفادة منه.

التهديدات و الهجومات

2. **الانتحال**: يحدث الانتحال او التنكر عندما ينتحل المهاجم شخصية شخص آخر. على سبيل المثال، قد يسرق أحد المهاجمين البطاقة المصرفية ورقم التعريف الشخصي لعميل البنك ويتظاهر بأنه ذلك العميل. في بعض الأحيان يتظاهر المهاجم بدلاً من ذلك بأنه الكيان الشرعي. على سبيل المثال، يحاول أحد المستخدمين الاتصال بأحد البنوك، لكن موقعًا آخر يتظاهر بأنه البنك ويحصل على بعض المعلومات من المستخدم.
3. **الإعادة** : إعادة الاجراء هو هجوم آخر. يحصل المهاجم على نسخة من رسالة أرسلها المستخدم ويحاول لاحقًا إعادتها. على سبيل المثال، يرسل أحد الأشخاص طلبًا إلى البنك الخاص به ليطلب الدفع للمهاجم الذي قام بعمل له. يعترض المهاجم الرسالة ويرسلها مرة أخرى لتلقي دفعة أخرى من البنك.
4. **الانكار (أو التنصل)** : يختلف هذا النوع من الهجمات عن غيره لأنه يتم من قبل أحد طرفي الاتصال: المرسل أو المستقبل. قد ينكر مرسل الرسالة لاحقًا أنه أرسل الرسالة؛ وقد ينكر المستقبل الرسالة لاحقًا أنه قد استلم الرسالة. مثال على الرفض من قبل المرسل هو أن تطلب عميلة البنك من البنك الخاص بها إرسال بعض الأموال إلى طرف ثالث ولكنها تنكر لاحقًا أنها قدمت مثل هذا الطلب. يمكن أن يحدث مثال على الإنكار من جانب المستقبل عندما يشتري شخص ما منتجًا من الشركة المصنعة ويدفع ثمنه إلكترونيًا، لكن الشركة المصنعة تنفي لاحقًا استلام الدفعة وتطلب أن يتم الدفع لها مجددا.

التهديدات و الهجومات

الهجمات التي تهدد التوفر وديمومة المعلومات: و نذكر هنا هجومً "تعطيل/الحرمان من الخدمة".

الحرمان من الخدمة : يعد رفض الخدمة (DoS) هجومًا شائعًا جدًا. قد يؤدي ذلك إلى إبطاء خدمة النظام أو قاطعها تمامًا. يمكن للمهاجم استخدام عدة استراتيجيات لتحقيق ذلك. قد ترسل العديد من الطلبات الزائفة إلى الخادم مما يؤدي إلى تعطل الخادم بسبب حجم الحمل الزائد. قد يعترض المهاجم ويحذف استجابة الخادم للعميل، مما يجعل العميل يعتقد أن الخادم لا يستجيب. قد يعترض المهاجم أيضًا الطلبات المقدمة من العملاء، مما يتسبب في قيام العملاء بإرسال الطلبات عدة مرات وزيادة التحميل على النظام.

التهديدات و الهجومات

الهجمات السلبية و النشطة : يمكن تصنيف الهجمات إلى مجموعتين: سلبية ونشطة. ويبين الجدول التالي العلاقة بين هذا والتصنيف السابق.

- **الهجمات السلبية**: في الهجوم السلبي، هدف المهاجم هو الحصول على المعلومات فقط. وهذا يعني أن الهجوم لا يؤدي إلى تعديل البيانات أو الإضرار بالنظام. ويستمر النظام في عمله الطبيعي. ومع ذلك، قد يؤدي الهجوم إلى الإضرار بمرسل الرسالة أو متلقيها. الهجمات التي تهدد السرية - التطفل وتحليل حركة المرور - هي هجمات سلبية. قد يؤدي الكشف عن المعلومات إلى الإضرار بمرسل الرسالة أو مستقبلها، لكن النظام لا يتأثر. ولهذا السبب، يصعب اكتشاف هذا النوع من الهجمات حتى يعلم المرسل أو المستلم بتسريب معلومات سرية. ومع ذلك، يمكن منع الهجمات السلبية عن طريق تشفير المعلومات.
- **الهجمات النشطة :** قد يؤدي الهجوم النشط إلى تغيير المعلومات أو الإضرار بالنظام. الهجمات التي تهدد السلامة والتوافر هي هجمات نشطة. عادة ما يكون اكتشاف الهجمات النشطة أسهل من منعها، لأن المهاجم يمكنه إطلاقها بعدة طرق.

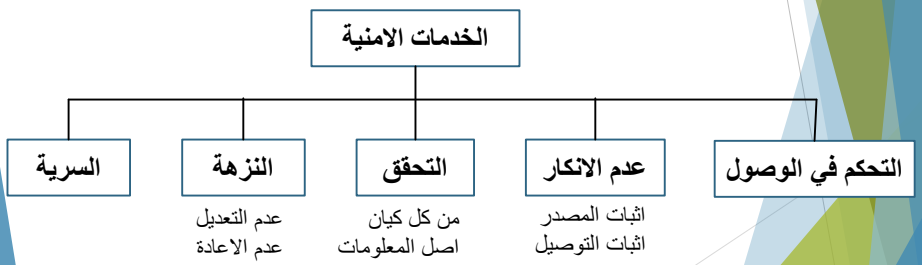
التهديدات و الهجومات

تصنيف الهجمات سلبية ونشطة

الهجوم	سلبى / نشط	يهدد
التطفل تحليل حركة المرور	سلبى	السرية
التعديل الانتحال الإعادة الانكار	نشط	النزاهة
الحرمان من الخدمة	نشط	التوفر

الخدمات الأمنية

حدد قطاع معايير الاتصالات خمس خدمات تتعلق بأهداف/عناصر الأمن والهجمات التي حددناها سابقا، ويبين الشكل تصنيف تلك الخدمات الخمس. ويمكن ربط واحدة أو أكثر من هذه الخدمات بواحد أو أكثر من أهداف الأمن.

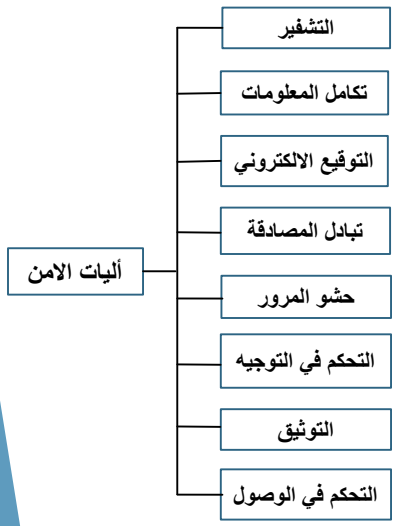


الخدمات الأمنية

1. **سرية المعلومات** : خدمة سرية المعلومات تعنى بحماية المعلومات من هجوم الكشف. الخدمة واسعة جدًا وتشمل سرية الرسالة بأكملها أو جزء منها وكذلك الحماية من تحليل حركة المرور، أي أنه مصمم لمنع التطفل وهجوم تحليل حركة المرور.
2. **نزاهة المعلومات و تكاملها** : يتم تصميم تكامل المعلومات و نزاهتها لحماية المعلومات من التعديل والإضافة والحذف وإعادة التشغيل من قبل الخصم. وقد يحمي الرسالة بأكملها أو جزء منها.
3. **المصادقة** (التحقق): توفر هذه الخدمة مصادقة الطرف على الطرف الآخر في الاتصال او الاجراء. في الاتصالات الموجهة، تتم المصادقة بين المرسل و المستقبل أثناء إنشاء الاتصال (مصادقة الكيان النظير). في الاتصالات الغير موجهة تتم المصادقة على مصدر المعلومات (مصادقة أصل المعلومات).
4. **عدم التنصل أو الانكار** : تحمي خدمة عدم التنصل من التنصل من جانب مرسل المعلومات أو مستقبلها. في حالة عدم الإنكار مع إثبات الأصل، يمكن لاحقًا لمستقبل المعلومات إثبات هوية المرسل في حالة رفضه. في حالة عدم التنصل مع إثبات التسليم، يمكن لمرسل المعلومات أن يثبت لاحقًا أنه تم تسليم المعلومات إلى المستلم المقصود.
5. **التحكم في الوصول**: يوفر التحكم في الوصول الحماية ضد الوصول غير المصرح به إلى المعلومات. مصطلح الوصول في هذا التعريف واسع جدًا ويمكن أن يشمل القراءة والكتابة والتعديل وتنفيذ البرامج وما إلى ذلك.

آليات الأمن

يوصي قطاع الاتصالات بعض آليات الأمن لتوفير خدمات الأمن المذكورة سابقا، والشكل التالي يصنف هذه الآليات.



1. **التشفير**: التشفير أو الإخفاء أو تعمية المعلومات يمكن أن يوفر السرية. ويمكن استخدام التشفير مع آليات أخرى لتقديم خدمات أخرى. ويتم استخدام تقنيتين للتشفير التعمية وتورية المعلومات.
2. **تكامل المعلومات و نزاهتها** : تُلحق آلية تكامل المعلومات بالبيانات قيمة تحقق قصيرة تم إنشاؤها بواسطة عملية محددة من المعلومات نفسها. يتلقى المستقبل البيانات والقيمة الاختبارية. يقوم بإنشاء قيمة تحقق جديدة من البيانات المستلمة ويقارن قيمة التحقق التي تم إنشاؤها حديثًا مع القيمة المستلمة. إذا كانت القيمتان المرجعيتان متماثلتين، فسيتم التاكد من سلامة المعلومات.

آليات الأمن

3. **التوقيع إلكتروني** : التوقيع الرقمي هو وسيلة يمكن من خلالها للمرسل التوقيع إلكترونيًا على المعلومات ويمكن للمستلم التحقق إلكترونيًا من التوقيع. يستخدم المرسل عملية تتضمن إظهار أنه يمتلك مفتاحًا خاصًا مرتبطًا بالمفتاح العام الذي أعلنه علنًا. يستخدم المستلم المفتاح العام للمرسل لإثبات أن الرسالة موقعة بالفعل من قبل المرسل الذي يدعي أنه أرسل الرسالة.
4. **تبادل المصادقة** : في تبادل المصادقة، يتبادل كيانان بعض الرسائل لإثبات هويتهما لبعضهما البعض. على سبيل المثال، يمكن لأحد الكيانات أن يثبت أنه يعرف سرًا من المفترض أن يعرفه هو فقط.
5. **حشوة المرور** : تعني حشوة حركة المرور إدخال بعض البيانات الزائفة في حركة المعلومات لإحباط محاولة الخصم استخدام هجوم تحليل حركة المرور.
6. **التحكم في التوجيه** : التحكم في التوجيه يعني اختيار مسارات متاحة مختلفة وتغييرها باستمرار بين المرسل والمستقبل لمنع الخصم من التنصت على مسار معين.
7. **التوثيق** : التوثيق يعني اختيار طرف ثالث موثوق به للتحكم في الاتصال بين كيانين. ويمكن القيام بذلك، على سبيل المثال، لمنع التنصل او الانكار. يمكن للمستقبل إشراك طرف موثوق به لتخزين طلب المرسل وذلك لمنع المرسل من إنكار تقديم مثل هذا الطلب لاحقًا.
8. **التحكم في الوصول** : يستخدم التحكم في الوصول طرقًا لإثبات أن المستخدم لديه حق الوصول إلى المعلومات أو الموارد المملوكة للنظام. ومن أمثلة ذلك كلمات المرور وأرقام التعريف الشخصية.

العلاقة بين خدمات وآليات الامن

يوضح الجدول التالي العلاقة بين خدمات الأمن وآليات الأمن. يوضح الجدول أنه يمكن استخدام ثلاث آليات (التشفير والتوقيع الرقمي وتبادل المصادقة) لتوفير خدمة المصادقة .ويوضح الجدول أيضًا أن آلية التشفير قد تدخل في ثلاث خدمات (سرية المعلومات، ونزاهة المعلومات، والمصادقة).

خدمــة الامن	آليــة الامن
سرية المعلومات	**التشفير، و التحكم في التوجيه**
نزاهة المعلومات و تكاملها	**التشفير، و التوقيع إلكتروني، و تكامل المعلومات و نزاهتها**
المصادقة	**التشفير، و التوقيع إلكتروني، و تبادل المصادقة**
عدم التنصل أو الانكار	**التوقيع إلكتروني، و تكامل المعلومات و نزاهتها، و التوثيق**
التحكم في الوصول	**التحكم في الوصول**

مستويات تأثير الاختراق الامني

- **منخفض:** الفاقد له تأثير محدود، بمعنى تراجع في الخدمة ، ضرر بسيط ، خسارة مالية غير مهمة أو أذى طفيف.
- **متوسط:** الفاقد له خطير ، بمعنى تراجع مهم خدمة ، أذى جدي للأشخاص ولكن بدون فقدان للحياة أو تهديد بإصابات.
- **عالي:** الفاقد له تأثير شديد أو كارثي غير مرغوب به على الخدمة ، أصول المؤسسة (موارد النظام) ، على الأشخاص (فقدان للحياة).

المتطلبات الوظيفية/العملية للأمن

- **الإجراءات التقنية**
  - التحكم في الوصول ؛ التعرف و المصادقة ؛ حماية النظام و الاتصالات ؛ نزاهة المعلومات و النظام
- **الإجراءات الإدارية**
  - التدريب و التوعية ؛ التفتيش و المحاسبة ؛ الترخيص و الجودة ؛ الاعتماد و التقييم الأمني ؛ التخطيط للطوارئ ؛ الصيانة ؛ حماية بيئة العمل ؛ التخطيط ؛ الامن الشخصي ؛ تقييم المخاطر.
- **تداخل و تشابك الإجراءات التقنية مع الإدارية**
  - تهيئة الإدارة ؛ الاستجابة للحوادث ؛ حماية الوسائط.

مبادئ التصميم الأساسية للأمن

لا توجد قائمة مرجعية كاملة يمكن لمصممي النظم اتباعها لضمان أن الأنظمة المعتمدة على الحاسب "آمنة". الأسباب كثيرة ، بما في ذلك الاختلافات الكبيرة عبر التقنيات والبيئات والتطبيقات والمتطلبات. وبشكل عام ، يتم تشجيع مصممي النظام على فهم واتباع مجموعة من مبادئ التصميم الأمن القابلة للتطبيق على نطاق واسع.

1) **البساطة والضرورة**: اجعل التصميم بسيط وصغير قدر الإمكان. مع تقليل عدد المكونات المستخدمة ، مع الاحتفاظ فقط بالمكونات الأساسية ؛ تقليل الوظائف، وتعطيل الوظائف غير المستخدمة. الاقتصاد والتوفير في التصميم يبسط التحليل ويقلل من الأخطاء والسهو. تهيئة عمليات النشر الأولي وذلك لتعطيل الخدمات والتطبيقات غير الضرورية بشكل اعتيادي.

2) **الإعدادات الافتراضية الآمنة**: استخدم الإعدادات الافتراضية الآمنة؛ تذكر أن الإعدادات الافتراضية غالبًا ما تظل دون تغيير. للتحكم في الوصول، قم بالرفض افتراضيًا. فضل التضمين الصريح على الاستثناء - استخدم القوائم البيضاء، وأدرج الأطراف المرخص لها (يتم رفض جميع الأطراف الأخرى)، بدلاً من القوائم السوداء للأطراف التي سيتم منعها من الوصول (يُسمح بجميع الأطراف الأخرى). تصميم الخدمات لتكون آمنة عند الفشل، مما يعني أنها عندما تفشل فهي "مغلقة" (رفض الوصول) بدلاً من "مفتوحة".

مبادئ التصميم الأساسية للأمن

3) **التصميم المفتوح**: لا تعتمد على التصميمات السرية أو جهل المهاجم أو الأمان بالغموض، بل ادعو وشجع على المراجعة والتحليل المفتوح. على سبيل المثال: على نطاق واسع لا يتم التشجيع على خوارزميات التشفير السرية، لذلك تم اختيار خوارزمية معيار التشفير المتقدم (AES) من بين مجموعة من المرشحين العامين من خلال مراجعة مفتوحة. مع عدم التعارض مع سلف، يمكنك الاستفادة من عدم القدرة على التنبؤ عندما يكون ذلك مفيدًا، حيث أن نشر تفاصيل الدفاع التكتيكي بشكل تحكمي نادرًا ما يكون مفيدًا (ليس هناك فائدة من الإعلان للصوص عن أنك في إجازة، أو نشر مخططات المنزل). امنع أي تسريب لرسائل الخطأ السرية أو بيانات زمنية، خشية أن تكون مفيدة للمهاجمين.

4) **التوسط الكامل**: للوصول إلى كل كيان، وبشكل مثالي تحقق من التفويض المناسب قبل منح الوصول مباشرة. علما بان التحقق من التفويض يتطلب المصادقة (التأكد من الهوية) كذلك التحقق من أن المكون المرتبط مصرح له، والتحقق من سلامة الطلب ايضا (يجب عدم تعديله بعد إصداره من قبل الطرف المفوض).

5) **الأجزاء المعزولة**: قم بتقسيم مكونات النظام باستخدام بنية عزل قوية تمنع الاتصال بين المكونات أو تسرب المعلومات والسيطرة. وهذا يحد من الضرر عند حدوث حالات فشل، ويحمي من تصعيد الامتيازات. قم بتقييد الاتصال المصرح به ما بين المكونات على مسارات يمكن ملاحظتها مع واجهات محددة للمساعدة على الوساطة والفحص واستخدام نقاط الاختناق. من الأمثلة التي تتضمن وسائل الاحتواء: عزل العمليات والذاكرة، وتقسيم القرص، والمحاكاة الافتراضية، وحماية البرمجيات، والمناطق، والبوابات، وجدران الحماية.

مبادئ التصميم الأساسية للأمن

6) **امتيازات اقل** : قم بتخصيص أقل عدد من الامتيازات اللازمة لمهمة ما، ولأقصر مدة ضرورية. على سبيل المثال، احتفظ بامتيازات المستخدم المميزة فقط للإجراءات التي تتطلب ذلك؛ قم بإسقاط الامتيازات واستعادتها إذا لزم الأمر لاحقًا. لا تستخدم حساب المدير في يونيكس للمهام التي يمكن تنفيذها بامتيازات المستخدم العادية. وهذا يقلل من الاعتراض، ويحد من الأضرار الناجمة عن ما هو غير متوقع.

7) **التصميم النمطي (تركيبي)**: تجنب تصميم وحدات متجانسة تركز مجموعات كبيرة من الامتيازات في كيانات فردية؛ يفضل التصميمات الموجهة للكيانات والأكثر دقة (على سبيل المثال، قدرات ليونيكس) التي تفصل الامتيازات عبر وحدات أصغر أو عمليات متعددة أو مبادئ رئيسية مستقلة.

8) **قواعد صغيرة موثوقة**: نسعى جاهدين من اجل تصميم برمجي صغير للمكونات التي يجب الوثوق بها، أي المكونات التي يعتمد عليها نظام أكبر بشدة من أجل الأمان. مثال 1: تعمل أنظمة الضمان العالي على مركزية خدمات الأمان المهمة في نواة صغيرة لنظام التشغيل الأساسي، والتي يسمح حجمها الأصغر بالتركيز الفعال للتحليل الأمني. المثال 2: تقوم خوارزميات التشفير بفصل الآليات عن الأسرار، مع تقليل متطلبات الثقة إلى مفتاح سري قابل للتغيير بتكلفة أقل بكثير من خوارزمية التشفير نفسها.

9) **ادوات تم اختبارها** : الاعتماد ما امكنً ذلك على أدوات الأمان التي تم اختبارها عبر الزمن والتي صممها الخبراء بما في ذلك البروتوكولات وأسس التشفير و الأدوات المساعدة، بدلاً من تصميم وتنفيذ أدوات خاصة بك. يُظهر التاريخ أن التصميم الأمني يصعب انجازه بشكل صحيح حتى بالنسبة للخبراء؛ وبالتالي فإن الهواة يشعرون بالإحباط الشديد (لا تعيد اختراع عجلة أضعف). وتزداد الثقة مع طول الفترة الزمنية التي تبقى فيها الآليات والأدوات على قيد الحياة (يسمى أحيانًا اختبار النقع).

مبادئ التصميم الأساسية للأمن

10) **أقل دهشة**: أن تتصرف آليات التصميم وواجهات استخدامها كما يتوقع المستخدمون. مواءمة التصاميم مع النماذج الذهنية للمستخدمين في حماية أهدافهم، وذلك لتقليل أخطاء المستخدم. خاصة عندما تكون الأخطاء غير قابلة للإصلاح (على سبيل المثال، إرسال بيانات خاصة أو أسرار إلى أطراف خارجية)، ومصممة خصيصًا لتجربة مستخدمين مستهدفين؛ احذر من التصميمات المناسبة للخبراء المدربين ولكنها غير بديهية أو تسبب أخطاء من قبل المستخدمين العاديين. إن الآليات الأبسط والأسهل في الاستخدام (أي القابلة للاستخدام) تسفر عن مفاجآت أقل.

11) **اشراك المستخدم**: يتم تصميم آليات أمنية تحفز المستخدمين على استخدامها، ولتعزيز الاستخدام التعاوني المنتظم؛ وبذلك يكون المسار الأقل مقاومة للمستخدمين هو المسار الآمن. ابحث عن خيارات التصميم التي تسلط الضوء على الفوائد، وتحسن تجربة المستخدم، وتقلل من الإزعاج. إن الآليات التي يُنظر إليها على أنها تستغرق وقتًا طويلاً أو غير ملائمة أو بدون فائدة ملحوظة تشجع على التجاوز وعدم الامتثال. على سبيل المثال: تستخدم مجموعة محدودة من مستخدمي (Gmail Google) طوعًية نظام مصادقة من خطوتين، والذي يزيد من كلمات المرور الأساسية عن طريق رموز مرور لمرة واحدة مرسل إلى هاتف المستخدم.

12) **مقدار التكلفة**: بالنسبة للآليات التي يتم فيها حساب مقدار الشغل المبذول، قم بتصميم آلية الأمان بحيث تتجاوز تكلفة العمل اللازم للتغلب عليها بشكل واضح موارد المهاجمين المتوقعين. استخدم دفاعات قوية بشكل مناسب للحماية من فئات الخصوم المتوقعة. مثال 1: يجب أن تكون مفاتيح التشفير العشوائية طويلة بما يكفي بحيث لا يمكن العثور عليها عن طريق البحث الاستقصائي العميق. مثال 2: يجب عدم السماح للمستخدم بختيار كلمات المرور ضعيفة للغاية بحيث يؤدي عدد قليل من التخمينات إلى الحصول على فرصة لا يستهان بها للنجاح.

مبادئ التصميم الأساسية للأمن

13) **الدفاع في العمق**: قم ببناء دفاعات في طبقات متعددة تدعم بعضها البعض، مما يجبر المهاجمين على هزيمة الطبقات المستقلة. تجنب نقاط الفشل الفردية. إذا كانت الطبقة الفردية تعتمد على عدة قطاعات دفاعية، فقم بتصميم كل منها لتكون قوية نسبيًا ("أسوار متساوية الارتفاع") وتقوية القسم الأضعف أولاً (يقفز المهاجمون الأذكياء على الحاجز الأدنى أو يكسرون الحلقة الأضعف). كافتراض تصميمي، افترض أن بعض الدفاعات ستفشل من تلقاء نفسها بسبب الأخطاء، وأن المهاجمين سوف يهزمون الدفاعات الأخرى بسهولة أكبر من المتوقع أو سيتجاوزونها تمامًا.

14) **استخراج الأدلة**: تسجيل أنشطة النظام من خلال سجلات الأحداث ووسائل أخرى لتعزيز المساءلة، وذلك للمساعدة في فهم حالات فشل النظام والتعافي منها، ودعم أدوات كشف التسلل. على سبيل المثال: تستكمل طرق التدقيق القوية أدوات التحليل الجنائي، للمساعدة في إعادة بناء الأحداث المتعلقة بالاقتحامات والأنشطة الإجرامية. في كثير من الحالات، قد تكون الآليات التي تسهل اكتشاف الهجمات واستخراج الأدلة أكثر فعالية من حيث التكلفة من الوقاية المباشرة.

15) **التحقق من نوع البيانات**: التحقق من أن جميع البيانات المستلمة تتوافق مع الخصائص المتوقعة أو المفترضة. إذا كان إدخال البيانات متوقعًا، فتأكد من أنه لا يمكن معالجتها كتعليمة برمجية بواسطة مكونات لاحقة. على سبيل المثال: قد يكون هذا جزءًا من تصفية وتحديد المدخلات (على سبيل المثال، الأحرف المشفرة في عناوين الانترنت) لمعالجة هجمات حقن التعليمات البرمجية وحقن الأوامر.

مبادئ التصميم الأساسية للأمن

16) **إزالة البقايا**: عند إنهاء جلسة أو برنامج، قم بإزالة جميع آثار البيانات الحساسة المرتبطة بالمهمة، بما في ذلك المفاتيح السرية وأي بقايا يمكن استردادها من وحدة التخزين الثانوية وذاكرة الوصول العشوائي وذاكرة التخزين المؤقت. لاحظ أن الحذف الشائع للملف يزيله من الدليل، في حين أن الحذف الآمن يهدف إلى جعل محتوى الملف غير قابل للاسترداد حتى بأدوات التحليل الرقمي. فيما يتعلق بإزالة البقايا، احذر من أنه أثناء نشاط العملية، قد تتسرب المعلومات إلى مكان آخر عبر القنوات الجانبية.

17) **التأكيد المستقل**: استخدم عمليات فحص متقاطعة بسيطة ومستقلة لزيادة الثقة في التعليمات البرمجية أو البيانات، خاصة عندما يتم توفيرها من قبل نطاقات خارجية أو عبر قنوات غير موثوقة. مثال: يمكن التأكد من سلامة تطبيقات البرامج أو المفاتيح العامة التي تم تنزيلها من خلال مقارنة تجزئة التشفير المحسوبة محليًا للعنصر بتجزئة "معروفة" تم الحصول عليها عبر قناة مستقلة (مكالمة صوتية، رسالة نصية، موقع موثوق به على نطاق واسع).

18) **سلامة الاستجابة للطلب**: التحقق من أن الاستجابات تطابق الطلبات في بروتوكولات تحليل الأسماء والبروتوكولات الموزعة الأخرى. يجب أن يكشف تصميمها عن تغيير الرسالة أو استبدالها، وأن يتضمن عمليات التحقق من سلامة التشفير التي تربط الخطوات ببعضها البعض ضمن معاملة معينة أو تشغيل بروتوكول؛ احذر البروتوكولات التي تفتقر إلى المصادقة. على سبيل المثال: طلب شهادة يحدد اسم موضوع فريد أو مجال يتوقع ردًا على ذلك شهادة لذلك الموضوع؛ يجب التحقق من هذا الحقل في شهادة الاستجابة مع الطلب.

مبادئ التصميم الأساسية للأمن

19) **تردد في التخصيص**: كن مترددًا في تخصيص الموارد أو بذل مجهود في التفاعلات مع وكلاء خارجيين غير مصادق عليهم. بالنسبة للعمليات أو الخدمات ذات الامتيازات الخاصة، كن مترددًا في العمل كقناة لتمرير هذه الامتيازات إلى وكلاء غير مصادق عليهم (غير موثوق بهم). ضع عبئًا أكبر لإثبات الهوية أو السلطة على الوكلاء الذين يبدأون الاتصال أو التفاعل. (لا ينبغي للطرف الذي يبدأ مكالمة هاتفية أن يسأل: من أنت؟) يؤدي الفشل في اتباع هذا المبدأ إلى تسهيل هجمات رفض الخدمة المختلفة.

20) **الأمن اثناء التصميم**: قم ببناء الأمان، بدءًا من مرحلة التصميم الأولية لدورة التطوير، نظرًا لأن التصميم الآمن غالبًا ما يتطلب دعمًا معماريًا أساسيًا غائبًا إذا كان الأمان بمثابة وظيفة إضافية في مرحلة متأخرة. اذكر بوضوح أهداف تصميم الآليات الأمنية وما لم يتم تصميمها للقيام به، حيث أنه من المستحيل تقييم الفعالية دون معرفة الأهداف. في وثائق التصميم والتحليل، اذكر بوضوح جميع الافتراضات المتعلقة بالأمن، وخاصة المتعلقة بالثقة والأطراف الموثوق بها؛ لاحظ أن السياسة الأمنية نفسها قد لا تحدد الافتراضات.

21) **تصميم قابل للتطوير**: ضع في اعتبارك التطور عند تصميم البنى الأساسية والآليات والبروتوكولات. على سبيل المثال: تصميم أنظمة ذات مرونة خوارزمية، بحيث تكون ترقية خوارزمية التشفير (على سبيل المثال، التشفير والتجزئة) عملية سهلة ولا تؤثر على مكونات النظام الأخرى. وتتمثل عملية الإدارة ذات الصلة في إعادة تقييم فعالية آليات الأمان بشكل منتظم، في ضوء التهديدات والتكنولوجيا والبنيات المتطورة - والاستعداد لتحديث التصميمات حسب الحاجة.

مواضع الهجوم/الاختراق

- **مواضع الهجوم:** هو محل الضعف او الثغرة الذى يمكن الوصول اليه او يمكن استغلاله في النظام.
  - نقاط الربط المفتوحة
  - الخدمات التي خارج حماية جدار الامن
  - موظف له إمكانية الوصول لمعلومات حساسة
- **ثلاثة أصناف**
  - موضع الهجوم في الشبكات (مواضع الثغرات بالشبكة)
  - موضع الهجوم في البرمجيات (مواضع الثغرات بالبرنامج)
  - موضع الهجوم على المستخدمين (الهندسة الاجتماعية)
- **تحليل الهجوم:** تقييم حجم و خطورة التهديدات على النظام.

شجرة الهجوم/الاختراق

تعتبر شجرة الهجوم أداة مفيدة لنمذجة التهديدات، وخاصة لتحديد اسلوب الهجوم. تبدأ الشجرة بعقدة جذر في الأعلى، توضح هدف الهجوم الشامل (على سبيل المثال، دخول منزل). تبين العقد السفلية الطرقَ البديلة للوصول إلى الهدف الأعلى (على سبيل المثال، الدخول عبر النافذة، أو عبر الباب، أو نفق في الطابق السفلي)، ويمكن تجزئة كل منها بشكل مماثل (على سبيل المثال، فتح نافذة غير مقفلة، وكسر نافذة مقفلة).

كل عقدة داخلية هي جذر لشجرة فرعية و تحدد تفرعاتها طرق الوصول إليها. تنتهي الأشجار الفرعية بالعقد الطرفية (النهائية). يسرد المسار الذي يربط العقدة الطرفية بالجذر الخطوات (اسلوب الهجوم) التي تؤلف هجومًا كاملاً؛ وقد تقوم العقد الوسيطة بتفصيل خطوات المتطلبات الأساسية، أو تصنيف اساليب مختلفة.

التفرعات المتعددة للعقدة (الشكل) هى افتراضيًا بدائل مميزة (عقدة **"أو / OR"** منطقية (احداها))؛ و يمكن وضع مجموعة فرعية من العقد عند مستوى معين على أنها مجموعة **"و / AND"** منطقية (جميعها)، حيث تشير إلى أن جميعها ضرورية معًا لتحقيق الهدف الأصلي. يمكن إضافة تعليقات توضيحية للعقد بتفاصيل مختلفة، على سبيل المثال، الإشارة إلى أن الخطوة غير ممكنة، أو من خلال القيم التي تشير إلى التكاليف أو التدابير الأخرى. يمكن تنظيم معلومات الهجوم التي تم التقاطها بشكل أكبر، مما يشير في كثير من الأحيان إلى تصنيفات طبيعية لأساليب الهجوم ضمن فئات معروفة من الهجمات.

شجرة الهجوم/الاختراق

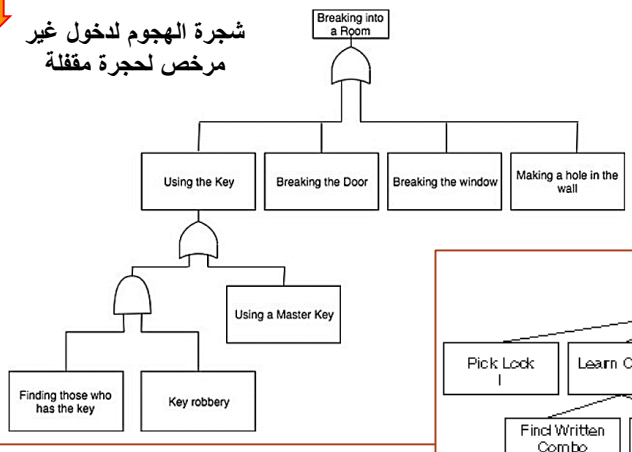
الناتج الرئيسي لشجرة الجوم هو قائمة واسعة (ولكنها عادة غير مكتملة) بالهجمات المحتملة، على سبيل المثال، (الشكل التالي) . يمكن فحص اتجاهات الهجوم لتحديد أي منها يشكل خطراً حقيقيا على النظام المستهدف؛ فإذا كانت الظروف المبينة في العقدة غير ممكنة لسبب ما، فسيتم وضع علامة على المسار بأنه غير صالح، وهذا يساعد في الحفاظ على التركيز على التهديدات الأكثر قابلية للتطبيق . لاحظ عدم التماثل: يحتاج المهاجم إلى إيجاد طريقة واحدة فقط لاقتحام النظام، في حين يجب على المدافع (مشرف الأمن) الدفاع ضد جميع الهجمات القابلة للتطبيق.

يمكن أن تساعد شجرة الهجوم في تشكيل سياسة الأمن، وفي التحليل الأمني للتحقق من وجود آليات لمواجهة جميع مسارات الهجوم المحددة، أو تفسير سبب عدم جدوى مسارات معينة بالنسبة للخصوم معنيين بالنظام المستهدف. قد تساعد مسارات الهجوم التي تم تحديدها في تحديد أنواع الإجراءات الدفاعية اللازمة لحماية أصول معينة من أنواع معينة من الهجومات الضارة. يمكن استخدام أشجار الهجوم لتحديد أولويات المسارات على أنها عالية أو منخفضة، على سبيل المثال، بناءً على سهولة استخدامها وفئات الخصوم ذات الصلة.

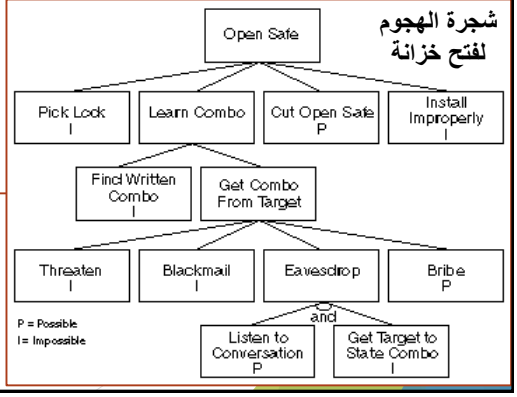
تشجع منهجية شجرة الهجوم على شكل من أشكال التفكير الذهني الموجه، مما يضيف هيكلية إلى ما يعتبر بخلاف ذلك عملية عشوائية. وتستفيد العملية من العقل الإبداعي حيث المهارة تتحسن مع الخبرة. ومن الأفضل أيضًا استخدام هذه العملية بشكل متكرر، فمع توسيع الشجرة يتم تحديد هجمات جديدة عند المراجعة من قبل الزملاء، أو دمجها مع الأشجار التي أنشأها الآخرون بشكل مستقل. تحفز أشجار الهجوم مشرفي الأمن على "التفكير مثل المهاجمين" للدفاع ضدهم بشكل أفضل.

شجرة الهجوم/الاختراق

شجرة الهجوم لدخول غير مرخص لحجرة مقفلة



شجرة الهجوم لفتح خزانة



Goal: Read a specific message that has been sent from one Windows 95 computer to another.
1. Convince sender to reveal message. (OR)
 1.1. Bribe user.
 1.2. Blackmail user.
 1.3. Threaten user.
 1.4. Fool user.
2. Read message when it is being entered into the computer. (OR)
 2.1. Monitor electromagnetic emanations from computer screen. (Countermeasure: use a TEMPEST computer.)
 2.2. Visually monitor computer screen.
3. Read message when it is being stored on sender's disk. (Countermeasure: use SFS to encrypt hard drive.) (AND)
 3.1. Get access to hard drive. (Countermeasure: put physical locks on all doors and windows.)
 3.2. Read a file protected with SFS.
4. Read message when it is being sent from sender to recipient. (Countermeasure: use PGP.) (AND)
 4.1. Intercept message in transit. (Countermeasure: use transport-layer encryption program.)
 4.2. Read message encrypted with PGP.
5. Convince recipient to reveal message. (OR)
 5.1. Bribe user.
 5.2. Blackmail user.
 5.3. Threaten user.
 5.4. Fool user.
6. Read message when it is being read. (OR)
 6.1. Monitor electromagnetic emanations from computer screen. (Countermeasure: use a TEMPEST computer.)
 6.2. Visually monitor computer screen.
7. Read message when it is being stored on receiver's disk. (OR)
 7.1. Get stored message from user's hard drive after decryption. (Countermeasure: use SFS to encrypt hard drive.) (AND)
  7.1.1. Get access to hard drive. (Countermeasure: put physical locks on all doors and windows.)
  7.1.2. Read a file protected with SFS.
 7.2. Get stored message from backup tapes after decryption.
8. Get paper printout of message. (Countermeasure: store paper copies in safe.) (AND)
 8.1. Get physical access to safe.
 8.2. Open the safe.

شجرة هجوم

الهدف : قراءة معلومة تم ارسالها من حاسوب ويندوز 95 الى آخر.

وضح شجرة الهجوم؟

شجرة الهجوم/الاختراق

الشكل التالي يوضح مثال لتحليل شجرة هجوم لتطبيق مصادقة حساب مصرفي على الانترنت. عقدة أصل الشجرة هي هدف المهاجم ، المربعات المظللة على الشجرة هي الطرفيات والتي تمثل احداث تتضمن الهجوم، في حين ان المربعات الغير مظللة عبارة عن أنواع أخرى يمكن ان تحتوى على حدث هجوم معين او اكثر. لاحظ في الشجرة ان جميع العقد عدى الطرفيات هي على شكل عقدة-أو (احداها).

التحليل المستخدم لبناء هذه الشجرة مبنى على المكونات المستخدمة في عملية المصادقة:

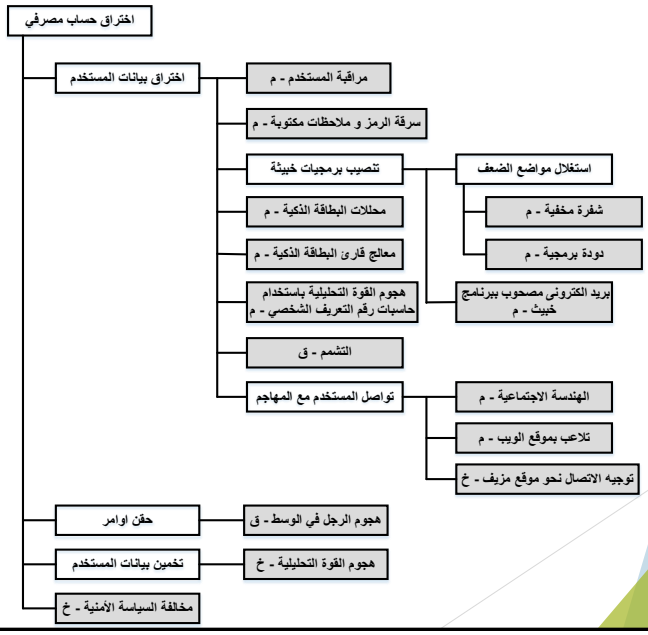
- **المستخدم و المحطة الطرفية للمستخدم (م)** : هذا الهجوم يستهدف معدات المستخدم ، البطاقات الذكية و كلمات المرور كذلك أفعال المستخدم.
- **قناة الاتصال (ق)** : هذا النوع من الهجوم يركز على روابط الاتصال.
- **خادم المصرف على الشبكة (خ)** : هذه الأنواع من الهجوم هي هجومات غير مباشرة ضد الخادم الذي يستضيف تطبيق المصادقة المصرفية.

أربعة أنواع من هجومات يمكن تحديدها، كل منها يستغل احدى او اكثر من المكونات السابقة ، هذه الأنواع من الهجمات هي:

شجرة الهجوم/الاختراق

- **اختراق بيانات المستخدم:** هذه الاستراتيجية يمكن استخدامها ضد مواضع هجوم عدة . توجد لها عدة إجراءات هجومية مثل مراقبة أفعال المستخدم بملاحظة ارقامه السرية او غيرها من بيانات المصادقة ، او سرقة البطاقة الذكية او ملاحظاته مكتوبة. الخصم يمكن ان يخترق او يكشف معلومات البطاقات باستخدام أدوات هجوم مختلفة، مثل اختراق البطاقات الذكية ، او استخدام أسلوب القوة التحليلية لتخمين الرقم السري. استراتيجية أخرى محتملة هي تضمين برمجية خبيثة لاختراق اسم و كلمة مرور المستخدم. يمكن للخصم ان يحاول الحصول على معلومات المصادقة عن طريق التنصت على قناة الاتصال (التشمم/الالتقاط). في النهاية، الخصم يمكن ان يستخدم عدة طرق لمشاركة الاتصال مع المستخدم المستهدف.
- **حقن أوامر:** في هذا النوع من الهجوم، المستخدم له القدرة على اعتراض الاتصال بين المحطة الطرفية للمستخدم و خادم المصرف على الشبكة. هناك عدة طرق مستخدمة تمكن من انتحال على شكل مستخدم شرعي و كسب إمكانية الوصول الى النظام المصرفي.
- **تخمين بيانات مصادقة المستخدم:** لوحظ ان هجومات القوة التحليلية ضد نظم المصادقة المصرفية ممكنة بأرسال اسم و كلمة مرور مستخدم عشوائية. و تعتمد علي آلية وجود حواسيب مجندة موازعة و هي تستضيف برمجيات لحساب اسم او كلمة مرور المستخدم.
- **مخالفة السياسات الأمنية:** مثال على ذلك ، مخالفة السياسات الأمنية للمصرف بربط آلية الدخول بتحكم ضعيف في الوصول، الموظف بذلك يسبب في حادث امنى داخلي قد يعرض حسابات الزبون للاختراق.

مثال : شجرة هجوم مختصرة لاختراق حساب مصرفي



استراتيجية أمن المعلومات

الاستراتيجية العامة لتوفير الامن

- **الخطة:** ماذا يجب ان تدعم لنظم الامن
  - الأصول و قيمتها
  - سهولة الاستخدام ضد الامن
  - تكلفة الامن ضد تكلفة الفشل/الاصلاح
- **الإنجاز/الآلية:** كيفية فرض،
  - المنع
  - الاكتشاف
  - الاستجابة
  - الاصلاح
- **الصحة/الضمان:** هل مضمونة حقا (الفعالية/النقد/المراجعة).

وقعة الامن

في الواقعة الامنية، من المستوى الأعلى، يحقق المهاجم أو المهاجمين غاياتهم من خلال تنفيذ الهجوم ، وقد تتكون الواقعة من هجوم واحد أو عدة هجمات (كما هو موضح في دورة الإعادة). العناصر الرئيسية لوقعة الهجوم هي:

- **الفعل** (Action): خطوة يتخذها المستخدم أو العملية من أجل تحقيق نتيجة .
- **الهدف** (Target): كيان معنوي او مادى بالحاسب الألى أو الشبكة.
- **حدث** (Event): فعل موجه إلى هدف ما بقصد أن يؤدي إلى تغيير حالة أو حالات الهدف.
- **الأداة** (Tool): وسيلة لاستغلال ضعف/ثغرة بنظام الحاسب أو الشبكة.
- **الثغرة** (Vulnerability): ضعف في النظام يسمح بفعل غير مصرح به.
- **العواقب** (Unauthorized result): نتائج غير مرغوبة لحدث ما.
- **الهجوم** (Attack): سلسلة من الخطوات يتخذها المهاجم لتحقيق نتائج غير مرغوبة.
- **المهاجم** (Attacker): الشخص الذي يحاول تنفيذ هجومًا واحدًا أو أكثر من أجل تحقيق غاية ما.
- **الغاية** (Objectives): الغرض أو الهدف النهائي للحادثة.
- **الواقعة** (Incident): مجموعة من الهجمات يمكن تمييزها عن بعضها البعض وذلك لتميز المهاجمين والاعتداءات والأهداف والمواقع والتوقيتات.

وقعة الامن