أمن الحاسبات و المعلومات

الفصل الثاني: **مكعب أمن المعلومات**

إعداد الدكتور / أسامة حسام الدين

محتوى الفصل الثاني

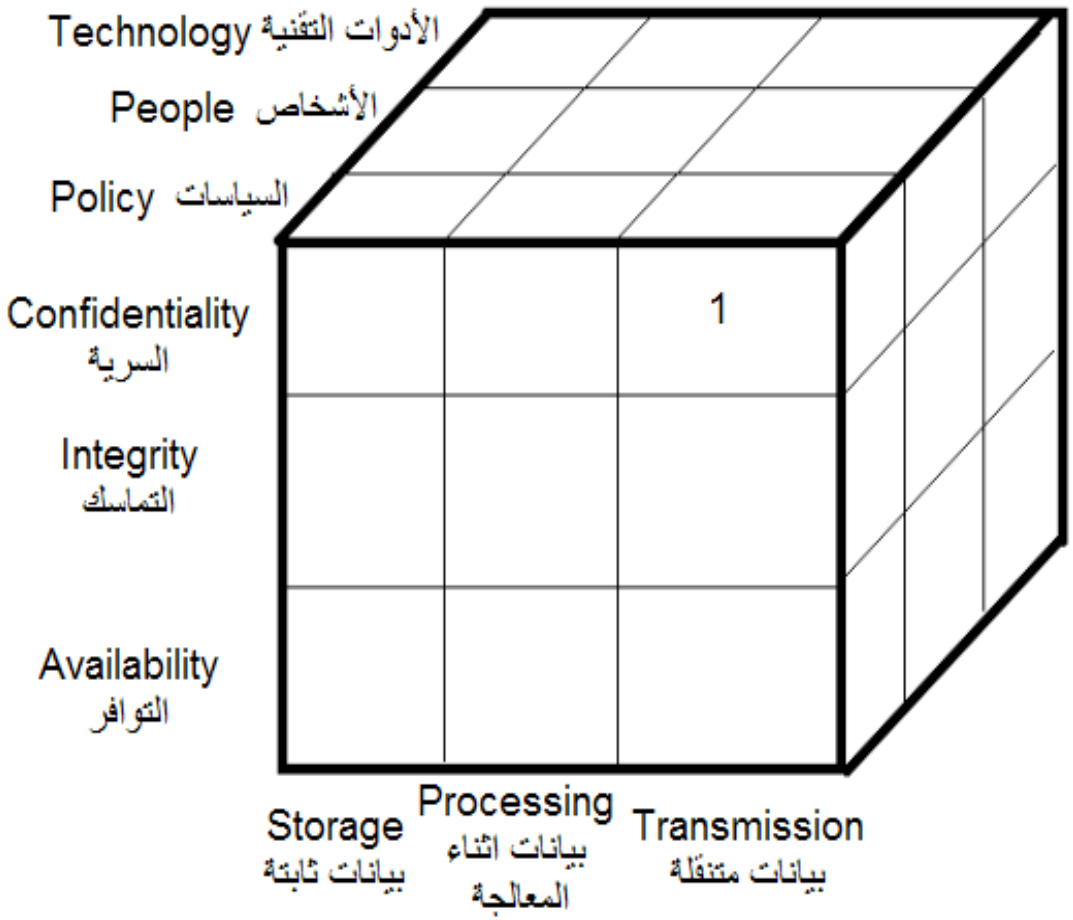
- نقدم في هذا الفصل مكعب أمن المعلومات المسمى مكعب ماكومبر.

يحتوي المكعب على ثلاثة محاور رئيسية هي

1. محور مبادئ أمن المعلومات
2. ومحور حالة البيانات
3. ومحور أدوات الحماية.

يركز المكعب على تقاطع الثلاث المحاور معا ليكون خلية.

مكعب ماكومبر



- ابتكر جون ماكومبر John McCumber مكعب أمن المعلومات ليكون إطارا عاما يشمل كل احتياجات نظم المعلومات الأمنية. ويشبه هذا المكعب مكعب روبيك المشهور،

مكعب ماكومبر

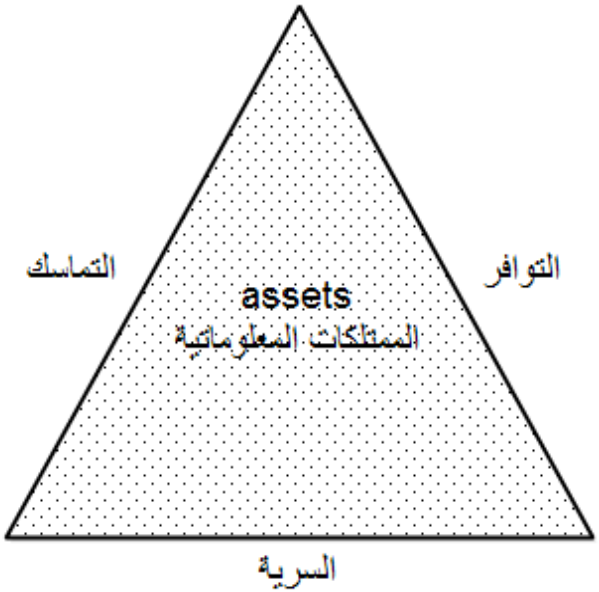
يحتوى المكعب على ثلاث محاور- رئيسية وهي

- محور مبادئ أمن المعلومات، ويعرف أيضا بمثلث الحماية الأمنية CIA Triad
- محور حالة البيانات
- محور أدوات الحماية

وتقاطع الثلاث محاور معا يعطي 3 × 3 × 3 = 27 خلية.
والتي تعبر- عن المجالات المختلفة التي يجب الاحتياط لها عند الإشار-ة إلى أي نظام امني معلوماتي

1 محور مبادئ أمن المعلومات

المبادئ الثلاث الرئيسية لأمن المعلومات هي السرية Confidentiality والتماسك Integrity والتوافر Availability وتختصر إلى CIA Triad بمعنى مثلث الحماية الأمنية.



- مثلث الحماية الأمنية، يحتوى على ثلاثة أضلاع، هي ضلع التوافر وضلع التماسك وضلع السرية.
- وفي منتصف المثلث توجد الممتلكات المعلوماتية وهي التي يراد حمايتها.

1. محور مبادئ أمن المعلومات: الممتلكات المعلوماتية

العتاد: يتم حفظ العتاد من السرقة، يجب أن يتم مراقبة العتاد بكاميرات المراقبة والتحكم في الوصول لها باستخدام الأقفال الفيزيائية أو بصمة الأصابع.

البرمجيات: هناك طرق لحماية البرمجيات من النسخ بإعطاء تراخيص ومعاقبة من يستخدم البرامج دون ترخيص مع استخدام الفوب أو الدونجل

البيانات: والبيانات هي الملفات المخزنة على الحاسب مثل ملفات الصوت والصورة والمستندات وملفات البرامج وقواعد البيانات (بيانات المستخدمين في الشركة وخارج الشركة). يمكن حفظ البيانات بتشفيرها.

خطوط الاتصال: يجب حفظ خطوط الاتصال من التصنت عليها باستخدام عمليات الحفظ الفيزيائي للأسلاك من التآكل والفئران.

1. محور مبادئ أمن المعلومات: حماية السرية

الطرق المستخدمة لحماية سرية البيانات يمكن تقسيمها إلى نطاقين عامين هما التشفير Cryptography والتحكم بالوصول Access Control

التشفير: التشفير يعني تحويل البيانات المعلوماتية من بيانات مفهومة إلى بيانات غير مفهومة والعكس.

التحكم بالوصول: التحكم بالوصول يعني تحجيم الوصول للملفات أو الحاسبات أو شبكات الحاسب أو قواعد البيانات ومنع الوصول إليها من أي شخص أو مورد إلا إذا أعطي الصلاحية لذلك. تتكون عملية التحكم بالوصول من ثلاث مراحل رئيسية هي **المصادقة** Authentication **والمنح** Authorization **والمتابعة** Accounting (مبدأ الثلاث ميمات "م م م" بالإنجليزية AAA)

1. محور مبادئ أمن المعلومات: حماية التماسك

- الشيء المتماسك هو الشيء الذي لا تغيره الحوادث. فالصخرة أكثر تماسكا من الطمي.
- فإذا أرسلت اليسا إلى بوب ملف إلكتروني، يجب أن يصل الملف آمنا لبوب بلا تعديل
- وإذا كتبت اليسا ملفا على معالج النصوص وتركته على الحاسوب في الشركة، ورجعت إلى الملف في اليوم التالي يجب أن تجده كما كان.
- **فحص التماسك** integrity check هو طريقة لقياس مدى تناسق مجموعة من البيانات مثل بيانات الصوت والصورة والملفات. إذا يتم التأكد كل فترة من أن البيانات لم تتغير بشكل غير مقصود أو بشكل تخريبي متعمد.

1. محور مبادئ أمن المعلومات: طرق حماية التماسك

1 الهاش Hash: وفيه يتم التأكد من صحة البيانات باستخدام كود الهاش الخاص بتلك البيانات. فإذا وجد تطابق بين كود الهاش القديم وكود الهاش المحسوب تكون البيانات صحيحة بلا تعديل.

- أبسط دوال الهاش هو **التدقيق بالمجموع** (checksum) ويتم عن طريق جمع القيمة العددية للبيانات، ثم إرسال المجموع (المجموع يمثل كود الهاش) مع البيانات. عند المستقبل يتم حساب مجموع البيانات مرة أخرى فإذا وجد تطابق كانت البيانات صحيحة ولم يتم تعديلها في الطريق بين المرسل والمستقبل.
- من **دوال الهاش** المشهورة MD5, SHA-1, SHA-256, SHA-512 وتم بناء هذه الخوارزميات على أسس رياضية معقدة.

1. محور مبادئ أمن المعلومات: طرق حماية التماسك

2. نظم التحقق من صحة البيانات: يمكن معرفة ما إذا تم التلاعب بالبيانات عن طريق إضافة جزء زائد على البيانات بغرض التحقق.

- على سبيل المثال كيف نعرف أن رقم بطاقة الائتمان الافتراضي 19358 رقم صحيح؟. يتم وضع آلية للتحقق،
- ولتكن، قم بجمع الأربعة أرقام الموجودة في يسار الرقم ثم أوجد باقي قسمة مجموعهم على 10 الرقم الناتج يجب أن يكون مساويا للعدد الموجود في خانة الآحاد. فمجموع 1، 9، 3، 5 هو 18 باقي قسمة 18 على العشرة هو 8.
- لذا فإن رقم بطاقة الائتمان صحيح. لاحظ أنه إذا تم التعديل في خانة الآحاد أو أي خانة أخرى فلن يتساوى باقي قسمة المجموع مع خانة الآحاد.

1. محور مبادئ أمن المعلومات: طرق حماية التماسك

3 •**نظم التحكم بالوصول:** يمكن الحفاظ على تماسك البيانات بالتحكم بالوصول لها عن طريق تحجيم صلاحيات التعديل وإعطاءها فقط للأشخاص المخولون بتعديل البيانات. ويفضل تطبيق مبدأين هامين :

- الأول يسمى مبدأ **"أقل الصلاحيات**least privilege " ويعني أن يتم منح الصلاحيات فقط التي يحتاجها المستخدم لأداء المهمة ولا نعطيه صلاحيات اكثر من ذلك.
- والمبدأ الثاني يسمى **"السياسة المغلقة** closed policy" وهي سياسة تعطي بشكل مبدأي للمستخدمين صلاحية القراءة فقط، ثم يتم منح الصلاحيات الأعلى عند الحاجة.

1. محور مبادئ أمن المعلومات: طرق حماية التماسك

4 •**النسخ الاحتياطي:** النسخ الاحتياطية تساهم في الحفاظ على تماسك البيانات. فلو حدث عطب في البيانات الحالية يتم استرجاع البيانات السليمة من النسخ الاحتياطية.

- الأهم من عمل النسخ الاحتياطي، هو التأكد من أن النسخ الاحتياطية نفسها سليمة. وأن عملية الاسترجاع من النسخ الاحتياطية تتم بشكل سليم
- ولذلك يجب التأكد بشكل دوري من تماسك النسخ الاحتياطية وتجربة عمل الاسترجاع للتأكد من سلامة إجراءاتها.

تمرين عملي – النسخ الاحتياطي في ويندوز

– كيف يتم عمل النسخ الاحتياطي على قرص خارجي (فلاش) لاحد الملفات الموجودة على سطح المكتب.

1. محور مبادئ أمن المعلومات: الحاجة للتماسك

تختلف الحاجة لتماسك البيانات على حسب التطبيق. يمكن تقسيم الحاجة لتماسك البيانات لثلاث مستويات رئيسية

- **الحاجة الحرجة:** وتوجد في التطبيقات الخاصة بطوارئ المستشفيات وفي البيانات الطبية بشكل عام. وتوجد تلك الحالة أيضا في التطبيقات المالية،
- **الحاجة المتوسطة:** وتوجد في التطبيقات التي تقوم بتحليل البيانات. وأيضا تطبيقات قواعد البيانات. كما توجد في محركات البحث إذ يتم عمل تحقق بسيط.
- **الحاجة المنخفضة:** وذلك مثل المشاركات على مواقع التواصل الاجتماعي والمدونات والمشاركات الشخصية. حيث لا يتم الاهتمام بالتدقيق على صحة البيانات.

1. محور مبادئ أمن المعلومات: التوافر

التوافر يعني الاحتفاظ بالخدمة متوفرة بشكل دائم. على سبيل المثال، يجب أن تتوافر خدمة سحب الأموال من ماكينة الصراف 24/7 أو 24 ساعة 7 أيام في الأسبوع.

في **هجمة قطع الخدمة** (Denial of Service DoS) يتم إشغال الخوادم بكميات ضخمة من الطلبات (المسموح بها في العادة)، وإذا أراد المستخدم العادي الاستفادة من الخدمة، دائما ما يجد الخوادم مشغولة والخدمة غير متوفرة.

مبدأ **التسعات الخمس** إشارة إلى الخمس تسعات الموجودة في الرقم المراد كنسبة توافر يطمح إليها الجميع والرقم هو 99.999% بمعنى أن يسمح بتعطل النظام فقط 5.26 دقيقة في السنة

1. محور مبادئ أمن المعلومات: طرق حماية التوافر

1 النظم المكررة: النظم المكررة تعني شراء وحدات بديلة زائدة عن الحاجة ووضعها في أهبة الاستعداد. فإذا تعطلت وحدة أساسية يتم استبدالها على الفور بالوحدة المكررة الاحتياطية. وأشهر أنواع التكرار يسمى تكرار نون + 1

ن

ن + 1

1. محور مبادئ أمن المعلومات: طرق حماية التوافر

2 •صيانة المعدات: صيانة المعدات يهدف إلى الاحتفاظ بالمعدات تعمل بشكل دائم بإزالة الأعطال التي تعتريها.

- يمكن حصر النقاط الحرجة في النظام وهي المعدات التي لو توقفت ستسبب في تعطل كامل النظام. ثم وضع أجهزة احتياطية لها
- يجب أيضا توفير مولدات كهرباء احتياطية أو استخدام أجهزة عدم قطع الكهرباء UPS.
- يجب أيضا تنظيف وتبريد المعدات التي تحتاج إلى ذلك بشكل دوري.

1. محور مبادئ أمن المعلومات: طرق حماية التوافر

3 تحديث النظم: يتم ترقية النظم إلى أحدث الإصدارات بهدف سد الثغرات التي يتم اكتشافها. حيث أن النظم القديمة دائما ما تكون قابلة للاختراق.

- القراصنة قد استخرجوا كل ثغرات النظم القديمة تقريبا وكتبوا برمجيات خبيثة كثيرة لاختراقها. فالقراصنة يستخدمون أحدث الأدوات والخدع
- يجب أيضا اختبار مقدرة النظم الحديثة على صد الهجمات وذلك باستخدام تقنيات مثل مسح المنافذ ومسح الثغرات واختبار الاختراق.

2. محور حالة البيانات

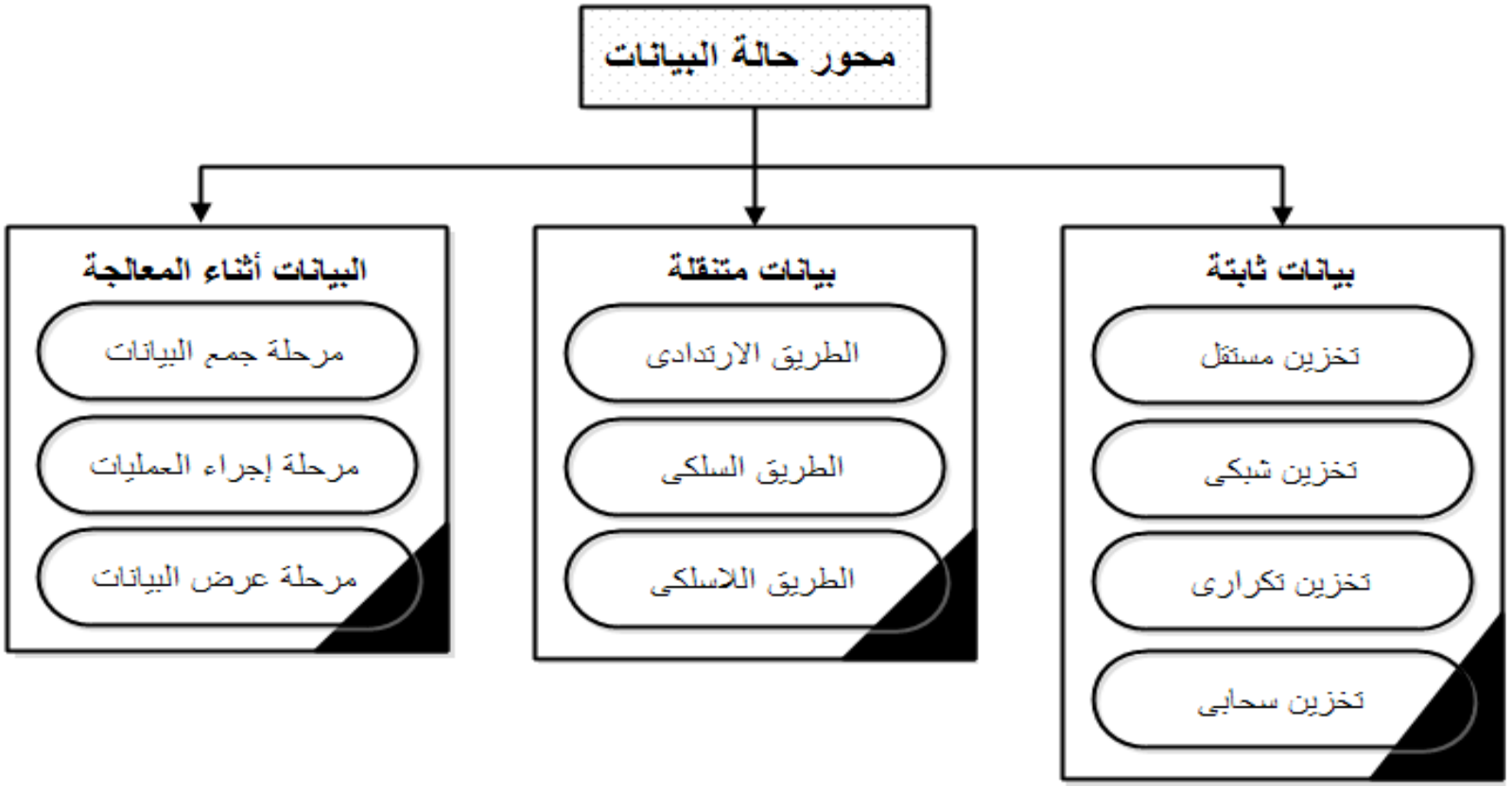
البيانات التي يتم تداولها على الإنترنت تتضاعف بشكل سريع. لذا يجب الاهتمام بتأمين البيانات في حالاتها الثلاث

- **الثابتة**
- **المتنقلة**
- **وأثناء المعالجة.**

فالبيانات المتنقلة تحتاج تأمين أكثر من البيانات الثابتة. على سبيل المثال، الأموال في الشركة المصرفية (البنك) تحتاج لتأمين أقل من الأموال التي تنتقل بين أفرع البنك المختلفة.

2. محور حالة البيانات

الشكل يوضح الإطار العام لمحور حالة البيانات (الثابتة والمتنقلة وأثناء المعالجة).



2. محور حالة البيانات: البيانات الثابتة (طرق التخزين)

- البيانات الثابتة هي البيانات التي تحفظ بلا انتقال و لا تعديل في الأوقات التي لا يصل إليها المستخدمون. يمكن أن يكون التخزين محليا أو مركزيا. وتوجد عدة **طرق للتخزين** منها ما يلي:

1. **التخزين المستقل:** ويسمى أيضا التخزين المباشر، تكون وحدة التخزين مستقلة عن النظم الأخرى وموصلة بالنظام بشكل مباشر- مثل الأقراص الصلبة وذاكرة الفلاش.
2. **التخزين التكراري:** مثل استخدام مجموعة متكررة من الأقراص الصلبة (ريد RAID) وهي وحدة تخزين مستقلة ولكنها تمتلك خاصية التكرار-.

2. **محور حالة البيانات:** البيانات الثابتة (طرق التخزين)

3. **<u>التخزين الشبكي</u>:** يوجد نوعين من التوصيل الشبكي، النوع الأول هو وحدة التخزين الموصلة بالشبكة (NAS) وهو مكان مركزي في الشبكة يتم تخزين البيانات عليه، يمكن توسعته في المستقبل على حسب الرغبة. النوع الثاني هو شبكة التخزين المحلية (SAN) هو عبارة عن شبكة محلية مخصصة فقط لتخزين البيانات
4. **<u>التخزين السحابي</u>:** هو عبارة عن وحدات تخزينية موجودة في مركز بيانات بعيد يمكن الوصول إليها من خلال الإنترنت. جوجل درايفGoogle Drive ودروب بوكس-Dropbox و iCloud كلها أمثلة على التخزين السحابي

محور حالة البيانات: البيانات المتنقلة .2

تنتقل البيانات من طرف إلى طرف عبر الشبكات. وفي الطريق قد تجد المتربصين (القراصنة). والطرق الإلكترونية هي أحد الأشكال الآتية:

- **الطريق الارتدادي bouncing:** وهي تعني استخدام وحدات التخزين المستقلة في نقل البيانات من جهاز إلى آخر. وتشبه ارتداد كرة القدم بين أرجل اللاعبين.
- **الطريق السلكي:** وهنا تستخدم كابلات لنقل البيانات التي تتحول إلى شكل نبضات كهربائية كما في الأسلاك النحاسية أو نبضات ضوئية كما في كابلات الألياف الضوئية.
- **الطريق اللاسلكي:** وتستخدم الموجات اللاسلكية مثل موجات الراديو في نقل البيانات.

2. محور حالة البيانات: البيانات أثناء المعالجة

تمر البيانات بثلاث مراحل أثناء معالجتها:

مرحلة جمع البيانات: توجد عدة طرق لجمع البيانات منها الإدخال اليدوي للبيانات أو استخدام الماسحات الضوئية أو استخدام حساسات التقاط البيانات كالكاميرات وحساسات الحرارة والرطوبة.

مرحلة إجراء العمليات على البيانات: في هذه المرحلة يتم تغيير البيانات الأصلية. تقوم البرامج والأجهزة بتعديل البيانات مثل البرامج الخاصة بالتشفير والضغط. وفي بعض الأحيان تقوم البرمجيات الخبيثة بتعديل البيانات وإلحاق الضرر بها.

مرحلة إخراج وعرض البيانات: وهي مرحلة رؤية البيانات المعروضة في شكل جداول أو رسومات بيانية. يتم عرض البيانات على نظم العرض المختلفة كالطابعات والشاشات

محور أدوات الحماية .3

أدوات الحماية هي ما نستخدمه في رد الهجمات الإلكترونية أو إيقافها قبل حدوثها أو اكتشافها أثناء حدوثها

نظم المعلومات نستخدم

- **أدوات** فيزيائية كالكاميرات والجدران النارية وأدوات برمجية مثل مكافح الفيروسات.
- ونقوم بتدريب **الأشخاص** على نظم الحماية وتوعيتهم بآخر المستجدات الخاصة بأمن الحاسبات والمعلومات.
- وأيضا نفرض **سياسات** على الموظفين كاستخدامهم لكلمات سر.

محور أدوات الحماية – التقنيات3.

مضاد الفيروسات anti-virus : ويوجد منها عدة أنواع، منها ما يحمي الشبكة ومنها ما يحمي الحاسوب الشخصي:

نظم اكتشاف ومنع الدخلاء: (IDS, IPS) يقوم بفحص الأنشطة على الأجهزة المضيفة أو الشبكات. ويقوم بعمل سجل الأحداث (log) ويعطي رسائل تحذيرية في حال اكتشاف نشاط غير عادي.

الشبكة الافتراضية الخاصة VPN) هي شبكة افتراضية آمنة وظيفتها هي توصيل أفرع الشبكة المختلفة باستخدام شبكة الأنترنت وبشكل آمن.

محور أدوات الحماية – 3. الأشخاص

إن استثمار أموال طائلة في شراء التقنيات الحديثة لن يكون ذا أهمية في حال عدم وعي الأشخاص داخل الشركة حيث يكون الشخص هو أضعف الوصلات الموجودة في سلسلة الحماية

يجب فرض وبناء ثقافة الوعي الأمني لدى الأشخاص في الشركة كالآتي

- تخصيص يوم في السنة يسمى يوم التوعية الأمنية، يقوم المتخصصون فيه بالاجتماع ومناقشة الحالة الأمنية للشركة.
- توزيع ملصقات ونشرات على فريق العمل بالشركة.
- تنظيم ورش عمل وندوات قصيرة للتوعية الأمنية.
- تنظيم دورات تدريبية متخصصة في أمن الحاسبات والمعلومات، داخليا أو خارجيا.

محور أدوات الحماية – السياسات.3

السياسة الأمنية هي مجموعة من الأهداف الأمنية للشركة والتي تشمل قواعد السلوك الوظيفي للمستخدمين ومدراء النظم وتحدد متطلبات النظام. ومنها:

- **سياسات تعريف الهوية والمصادقة** – وتحدد الأشخاص أصحاب الصلاحيات وهم من يستطيعون الوصول لموارد الشبكة،
- **سياسات كلمة المرور** – تؤكد على أن كلمات المرور تحقق الحد الأدنى من المتطلبات ويتم تغيرها بشكل دوري.
- **سياسة الاستخدام المقبول** Acceptance Use Policy (AUP) – تحدد موارد الشبكة وكيفية استخدامها بالطريقة المقبولة لدى الشركة. ويمكن أن تحدد أيضا عواقب مخالفة السياسات.
- **التعامل مع الحوادث** – وتصف كيف يمكن التصرف في حالة وجود حادث كهجوم شبكي أو اختراق امني.

الأسئلة