نشرة الكترونية توعوية رقم (١)

"الأمن السيبراني وأهميته"

صادرة عن اللجنة التنفيذية للجنة تكنولوجيا المعلومات
الاتحاد الاردني لشركات التأمين، كانون أول (ديسمبر)، 2020
دائرة الدراسات والتدريب

تقديم

بلا شك تكنولوجيا المعلومات هي ذات أهمية بالغة تبعاً لما لها من دور كبير في مختلف الأنشطة اليومية لشؤون حياتنا، ولأنه عالم الرقمية فقد تم تحويل جميع معلوماتنا الكترونياً، حيث أدى هذا الزخم الكبير إلى تسيير الأعمال بشكل إيجابي وعلى الرغم من ذلك أدى إلى وجود طامعين في معلومات الشركات من خلال الهجمات الالكترونية سواءً لتخريب أو للحصول على مقابل مادي مما جعل مفهوم الأمن السيبراني أكثر تداولاً في وقتنا الحالي.

الأمن السيبراني

الأمن السيبراني يدور حول حماية البيانات الموجودة في شكل إلكتروني (مثل أجهزة الكمبيوتر والخوادم والشبكات والأجهزة المحمولة وغيرها) من التعرض للخطر أو الهجوم، وجزء من ذلك هو تحديد ماهية البيانات المهمة، وأين توجد، ومدى تعرضها للخطر، وما هي التكنولوجيا التي يجب عليك تطبيقها من أجل حمايتها؟

أمن المعلومات

يهتم أمن المعلومات بالتأكد من الحفاظ على أمان البيانات بأي شكل من الأشكال وهي أوسع قليلاً من الأمن السيبراني لذلك، من المحتمل أن يكون شخص ما خبيراً في أمن المعلومات دون أن يكون خبيراً في الأمن السيبراني.

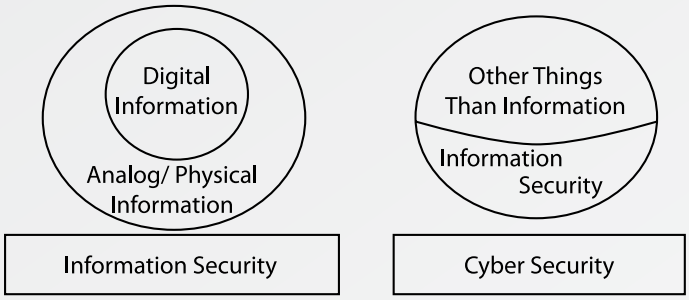
ووفقًا لمسرد ضمان المعلومات الوطني التابع لحكومة الولايات المتحدة الأمريكية ، يُعرّف أمن المعلومات : «هو حماية أنظمة المعلومات من الوصول غير المصرح به أو تعديل المعلومات ، سواء في التخزين أو المعالجة أو النقل، وضد رفض الخدمة للمستخدمين المصرح لهم أو تقديم الخدمة للمستخدمين غير المصرح لهم ، بما في ذلك التدابير اللازمة للكشف عن المستندات وتوثيقها ومواجهة مثل هذه التهديدات».

ثالوث «وكالة المخابرات المركزية الامريكية»

ثلاثة عناصر أو مجالات يجب التركيز عليها على نطاق واسع:
(اهتمامك هو للبيانات)

- ✓ السرية
- ✓ النزاهة
- ✓ التوفر (الاسترداد)

يشمل الأمن المادي وكذلك الأمن الالكتروني



الأمن في كلمة السر / المرور

- ✓ فرض سياسة أن تكون كلمة المرور معقدة ومركبة من أحرف وأرقام ورموز.
- ✓ فرض سياسة عدم استخدام كلمة مرور سابقة .
- ✓ فرض سياسة الحد الأدنى لعمر كلمة المرور .

- ✓ فرض سياسة الحد الأعلى لعمر كلمة المرور.
- ✓ فرض سياسة الحد الأدنى لطول كلمة المرور.
- ✓ فرض التذكير من خلال البريد الإلكتروني لتغيير كلمة المرور.
- ✓ فرض سياسة قفل جهاز الكمبيوتر حين يكون المستخدم بعيدا عن الجهاز.
- ✓ البيانات بشكل عام.
- ✓ الوعي عند فتح الملفات (USB، مرفقات الإيميل أو غيرها، مواقع الويب، CD، DVD. BR ، أي مصدر آخر، تنزيل / تثبيت الملفات).
- ✓ الوعي عند تصفح الإنترنت.
- ✓ احتفظ ببياناتك في مكان آمن. (نسخة إلكترونية / نسخة ورقية).
- ✓ تأكد من أن البيانات لديها نسخة احتياطية.
- ✓ وضع سياسة للاحتفاظ العمري بالبيانات.
- ✓ الوعي بكيفية مشاركة / تقديم البيانات
- ✓ أخذ صور شخصية (تأكد من عدم تضمين بيانات سرية).
- ✓ سياسة المكتب النظيف (تأكد من عدم تقديم مستندات سرية).
- ✓ إرسال البريد الإلكتروني (تأكد من السرية والمرفقات والموضوع والمستلمين).
- ✓ المؤتمرات عبر الصوت والصورة (تأكد من احتوائه على رمز مرور، وحفظه آمنًا، وإذا تم تسجيله، وليس الوقوع في اليد الخاطئة، وأيضاً مدى حساسية المؤتمر لأخذه علنًا أو بشكل خاص).
- ✓ الاجتماعات (تأكد من عدم نسيان الأشياء الخاصة بك، دفتر الملاحظات، الكمبيوتر المحمول، الهاتف المحمول، تأكد من مسح اللوح الأبيض إذا كان يحتوي على بيانات حساسة).

السلوك مع الأجهزة الالكترونية

- ✓ استخدام أقفال (الموصلات) الكابلات في حالة استخدام أجهزة الكمبيوتر المحمولة.
- ✓ عند السفر - لا تترك الكمبيوتر المحمول / الهاتف أبدًا في الأماكن العامة المفتوحة أو دون رؤية واضحة، فمن الضروري أن تبقي عينيك مفتوحتين، وإذا كنت بعيدًا أو مشغولًا، فتأكد من وجود الكمبيوتر المحمول / الهاتف في مكان آمن.
- ✓ أي أجهزة تخزين حساسة (سحابة، USB، أقراص مدمجة، إلخ.) يجب التعامل معها بعناية، خاصة أثناء السفر.
- ✓ يجب التعامل مع أي وسيلة دخول / وصول حساسة (المفاتيح، البطاقات، تطبيقات الأجهزة المحمولة، الرموز، إلخ.) بعناية.
- ✓ الوعي بكيفية الوقاية من أخطار الحريق والتعامل معها.
- ✓ لا تترك أجهزة الكمبيوتر المحمول والهواتف المحمولة في الشاحن مطلقًا أثناء عدم استخدامها.
- ✓ يجب أن تكون كهرباء الحائط صحيحة وسليمة.
- ✓ يجب أن تكون وصلات الكهرباء سليمة ومطابقة للأحمال الكهربائية المطلوبة.

إدارة المستند Document Management. (Business / IT)

هي قطعة من مادة مكتوبة أو مطبوعة أو إلكترونية تقدم معلومات أو أدلة أو تعمل كسجل رسمي.

أنواع المستندات

مستند خاضع للرقابة

هو مستند يجب أن يخضع للمراجعة الرسمية، والموافقة الرسمية، والتوزيع الخاضع للرقابة، والتعديل الخاضع للتحكم والتخزين والوصول الخاضعين للرقابة، أو بعبارة أخرى، المستند الخاضع للرقابة هو مستند يمر عبر عمليات التحكم في المستندات، أي يتم دائمًا التحكم في الأدلة والإجراءات والعقود وتسليمات الموردين وقواعد السلوك وما إلى ذلك.

مستند غير خاضع للرقابة

أي مستند لا تتخذ منه قرارات عمل، لا يمكن السيطرة عليه، مثال على ذلك، آخر أخبار الشركة أو خطاب تهنئة، ما هو تصنيف البيانات؟ يبدأ تصنيف البيانات بوضع العلامات ومعالجة المستندات بمستويات مختلفة من السرية. تتوافق هذه المستويات مع الأسماء، وترتبط في النهاية بكيفية استخدامها ونقلها وحمايتها في نهاية المطاف داخل وخارج العمل.

مستويات تصنيف البيانات

عامة:

هذه المعلومات هي معلومات عامة، ويمكن مشاركتها علناً على موقع الويب الخاص بك ومناقشتها علناً ومع أي شخص. المعلومات العامة كما يوحي الاسم، هي معلومات عامة، ولا تتطلب أي ضوابط إضافية عند استخدامها.

داخلي:

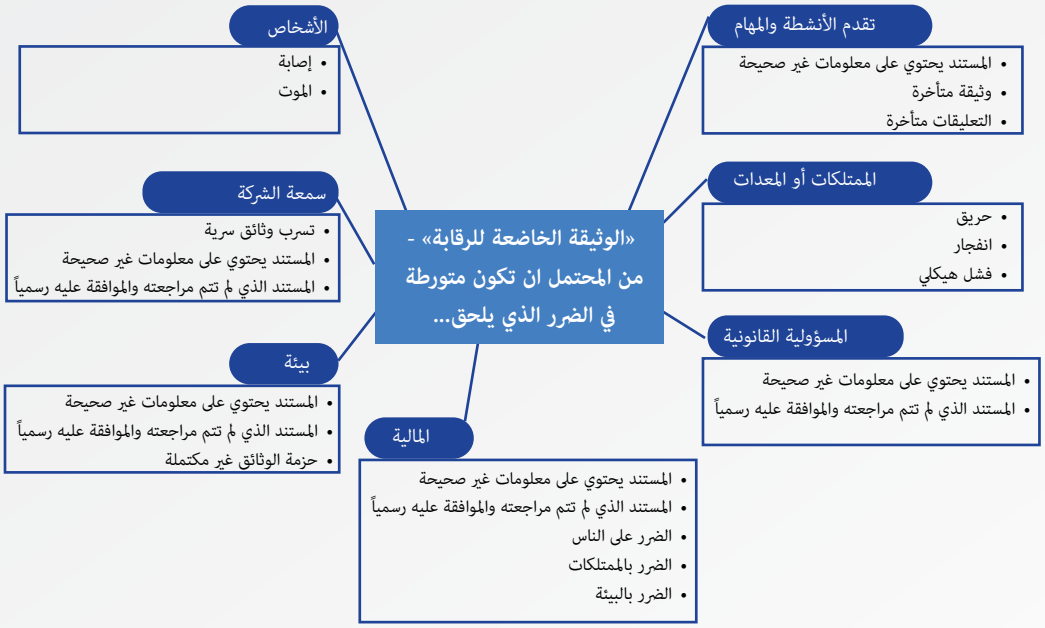
المعلومات الداخلية على مستوى الشركة ويجب حمايتها بضوابط محدودة. قد تتضمن المعلومات الداخلية كتيب الموظف والسياسات المختلفة والمذكرات على مستوى الشركة، إذا تم الكشف عنها، فإن المعلومات الداخلية يكون لها تأثير ضئيل على الأعمال.

سري:

المعلومات السرية على مستوى الفريق ويجب استخدامها داخل الشركة، قد تتضمن هذه المعلومات الأسعار أو مواد التسويق أو معلومات الاتصال. إذا تم الكشف عن المعلومات السرية، فقد تؤثر سلباً على عملك وعلى علامتك التجارية في النهاية.

مقيد:

المعلومات المقيدة حساسة للغاية ويجب أن يقتصر استخدامها على أساس الحاجة إلى المعرفة. عادةً ما تكون المعلومات المقيدة محمية بموجب اتفاقية عدم الإفشاء (NDA) لتقليل المخاطر القانونية. تتضمن المعلومات المقيدة الأسرار التجارية أو المعلومات التي يمكن تحديدها (PII) أو بيانات حامل البطاقة (بطاقات الائتمان) أو المعلومات الصحية. إذا تم الكشف عن ذلك، سيكون هناك تأثير مالي أو قانوني كبير على الأعمال.



فهم الفرق بين المستندات والسجلات؟

تُعرّف المستندات على أنها "معلومات مع الوسائط الداعمة لها"، في حين أن السجل عبارة عن "وثيقة توضح النتائج المحققة أو تقدم دليلاً على الأنشطة المنجزة". يوضح الجدول أدناه أمثلة لكل منها.

السجلات:	مستندات:
شهادات التدريب	كتيب التعليمات
نتائج التفتيش / المراجعة	الإجراءات الإدارية
نتائج الاستبيان	الرسومات التقنية
محضر الاجتماع	البيانات السياسية
تقرير المعايرة	العروض التقديمية
أمر الاستلام	الإيصالات المستلمة

تبرز هذه التعريفات بوضوح أنه في حين أن السجل دائمًا ما يكون مستندًا (وإن كان نوعًا خاصًا) ، فإن المستند ليس دائمًا سجلًا.
ترقيم المستندات هو تعريف تسلسل رقمي بمجموعات مختلفة ورموز تعريف محددة للمراسلات والمستندات الأخرى التي تتطلب التسجيل والإصدار والتتبع.

هيكل ترقيم المستندات

يتم ترقيم كل وثيقة أو رسم في مجموعات من الرموز والأحرف والأرقام المتسلسلة.
أمثلة: رقم تسلسل المستند
ID-Type-DNS-title
ID >رقم الموظف
Type >نوع الوثيقة
DSN >رقم تسلسل المستند
Title >ملخص محتوى الوثيقة
QUT – apr320201324 – srv – 562
562QUTapr320201324srv.docx
562QUTapr320201324srv.PDF
562QUTapr320201324srv.xlsx
توضيحات:
562:هو رقم الموظف الذي قدم هذه الوثيقة.
QUT: هو عرض أسعار.
apr320201324: يتم استخدامه كتاريخ ووقت ورقم تسلسل ، مما يعني أنه تم إنشاء هذا المستند في أبريل ٠٣ ٢٠٢٠ ، في الساعة ١:٢٤ م.
Srv: يعني الخادم.
يجب أن يكون لدى الشركة جدول يعكس الرموز المذكورة أعلاه وهيكل الترقيم (انظر الجدول أدناه)، لكل شركة حرية اختيار كيفية هيكلة المستند.

التوضيح	رمز
مذكرة	MEM
رسالة	LTR
ملحوظة	NTE
عرض أسعار	QUT
اقتراح	OFR
طلب الشراء	PR
أمر شراء	PO
خادم	SRV
كمبيوتر شخصي	PC
حاسوب محمول	LAP

النَسخ الإحتياطي : BACK UP POLICIES

عملية النسخ الاحتياطي (Backup) هي إجراء نسخة حفظ من الملفات الرقمية المهمة سواء كانت ملفات العمل أو الملفات الشخصية أو ملفات نظام التشغيل لحاسبك بغرض حفظها من الضياع في حال فقدان الملفات الأصلية عند الحاجة لها لأي سبب كان (كفقدانها مثلا في حال تلف الحاسب) أو بغرض استعادة حالة نظام التشغيل إلى وضع سابق لأي سبب كان .

صفات عملية النسخ الاحتياطي الناجحة

لكي تكون عملية النسخ الاحتياطي ناجحة يجب أن تحقق النقاط التالية:

١- يجب أن تكون عملية النسخ الاحتياطي أوتوماتيكية.
٢- يجب أن تكون عملية النسخ الاحتياطي دوريّة.
٣- يجب أن تكون النسخ الاحتياطية آمنة، أي أن المعلومات المحفوظة في النسخة الاحتياطية، لا يمكن التلاعب بها، ولا يمكن معاينتها من قبل غير المخولين لهم بذلك.
٤- يجب أن تكون النسخ الاحتياطية ذاتها في أمان، أي أنها غير معرضة للتلف، أو الضياع.

أمان النسخ الاحتياطية، طريقة النقاط الثلاث

١- يجب الاحتفاظ بثلاث نسخ احتياطية عن البيانات لهامة.
٢- تكون إحدى النسخ الثلاثة في مكان جغرافي غير النسختين الاخرتين (اثنتان في المكتب والثالثة في موقع اخر).
٣- تكون كل نسخة احتياطية موجودة على وسيطة تخزين مختلفة عن بقية النّسخ (كأن تكون إحداها مخزنة على DVD الثانية على القرص الصلب HDD والثالثة عبر التخزين السحابي Cloud Storage.

أبرز انواع النسخ الاحتياطي

-Full Backup النسخ الاحتياطي الكامل

وظيفة هذا النوع هو إجراء نسخة من جميع الملفات المشمولة في عملية النسخ الاحتياطي في كل مرة يتم فيها إجراء النسخ الاحتياطي.

- النسخ الاحتياطي التفاضلي أو التخالفي Differential Backup

يبدأ هذا النوع من النسخ الاحتياطي بنسخة احتياطية كاملة، ثم في المرات التالية من إجراء عملية النسخ الاحتياطي يتم نسخ فقط الملفات المضافة والملفات التي تم التعديل عليها منذ آخر عملية نسخ احتياطي كامل (Full Backup). يتم اجراء عملية نسخ احتياطي كامل كل عدد من مرات إجراء النسخ الاحتياطي التفاضلي.

- النسخ الاحتياطي التزايدي Incremental Backup

يبدأ هذا النوع من النسخ الاحتياطي بنسخة احتياطية كاملة ثم في كل مرة يتم فيها إجراء عملية النسخ الاحتياطي يتم نسخ الملفات المضافة والملفات التي تم التعديل عليها منذ عملية النسخ الاحتياطي السابقة.

شبكات الحاسوب

مقدمة تعريفية

تشكل شبكات الحاسوب مكوناً أساسياً في البنية التحتية لأنظمة المعلومات المحوسبة، فهي تضطلع بعدة أدوار مهمة تتمثل في ربط أجهزة الحاسوب وطرفياتها(كالطابعة والماسح الضوئي) ببعضها البعض من جهة وبأجهزة الاتصال المربوطة بخدمة الإنترنت من جهة أخرى، كما أن الشبكة تتيح للمستخدمين الوصول إلى البيانات سواء كانوا في نفس الموقع الجغرافي أو في أماكن جغرافية متعددة ومشاركة البيانات في الأعمال هي سمة بارزة زادت من قيمة الشبكات الحاسوبية، فالإنترنت هي شبكة مكونة من مجموعة كبيرة جدا من شبكات الإتصال والتي تتيح فرصة الحصول على البيانات وتقديم الخدمات للمستخدمين ضمن أوقات قياسية مقارنة مع طرق الحصول على البيانات التقليدية قبل ظهور خدمة الإنترنت، يتنوع المنتفعون من خدمة الإنترنت ما بين جهات حكومية كالمدرسين والطلاب في المؤسسات التعليمية ومراجعي الدوائر والمؤسسات الحكومية وموظفيها وجهات القطاع الخاص كالعملاء وكوادر الموظفين لدى المصارف وشركات التأمين، فالشبكة إذن هي المسار الذي يتيح للمستخدمين إمكانية الوصول إلى صفحات الانترنت وقواعد البيانات الخاصة بالجهات المختلفة، من الأهمية وجود بيانات تنتقل عبر الشبكات يستدعي حمايتها وصونها لأنها تمثل معلومات شخصية لأفراد وأصول للشركات وللمؤسسات الحكومية ولا يخول على الإطلاع عليها إلا من له الصلاحية، لذلك تولدت الحاجة في تبني معايير عالمية في أمن المعلومات، من باب حماية معلومات الأفراد والشركات والمؤسسات من العبث والاختراق والاستغلال وما يترتب عليه من إلحاق الضرر بهم وتعريضهم للخسائر.

أولاً: إدارة الشبكة

إدارة الشبكة هي في الأساس عملية إعداد شبكة وإدارتها واستكشاف أخطائها وإصلاحها، سواء للأغراض المنزلية أو التجارية. الغرض من إدارة الشبكة هو التأكد من إعداد جانب تكنولوجيا المعلومات في الشركة بطريقة مرنة ومعقولة ، والتي يمكن أن تقلل من الاضطرابات ، وتضمن الأداء العالي ، وتساعدك على تجنب مشاكل الأمان.

هناك خمسة مجالات أساسية لوجود نظام فعال لإدارة الشبكة:

١- إدارة الشبكة - تتضمن إدارة الشبكة الاحتفاظ بجرد لموارد ومعدات الشبكة ، بما في ذلك الكابلات والمحاور وأجهزة التوجيه والخوادم وأجهزة الكمبيوتر، بالإضافة إلى ذلك ، قد يعني ذلك إعداد الشبكات ومراقبة أدائها وتحديث البرامج واستكشاف الأخطاء وإصلاحها، ويتضمن أيضاً إعداد أدوات إدارة الشبكة وأنظمة التشغيل والبرامج المستخدمة عبر الشبكة بالكامل.
٢- تشغيل الشبكة - تتمحور العمليات حول الحفاظ على تشغيل

الشبكة بسلاسة وبدون مشاكل، ويشمل مراقبة الشبكة لمشاكل الأداء والأخطاء ، وكذلك إصلاح المشكلات قبل أن تؤثر على المستخدمين النهائيين ، أو على الأقل في الوقت المناسب.

٣- صيانة الشبكة - تشمل الصيانة إصلاح وتحديث معدات الشبكة (بما في ذلك أجهزة التوجيه وكابلات الإرسال والخوادم ومحطات العمل والمحولات)، كما يتضمن تحديث البرامج وتصحيحها بشكل مستمر، إلى جانب تنفيذ السياسات الوقائية وتحديث إجراءات التحكم في الوصول وتحسين التكوينات الخاطئة.

٤- التزويد بالشبكة - تتمحور مهمة التوفير حول تخصيص وتكوين موارد الشبكة لتناسب خدمة أو حاجة معينة. على سبيل المثال ، قد يستقبل المشروع الكثير من الأشخاص القادمين من خارج الموقع ، مما قد يزيد من الحاجة إلى النطاق العريض. إذا كان الفريق بحاجة إلى مساحة تخزين إضافية أو قدرات نقل الملفات ، تقع المسؤولية على عاتق تكنولوجيا المعلومات، يعمل مسؤول الشبكة على توفير الموارد لتلبية الاحتياجات المتزايدة والمتغيرة للأعمال.

٥- أمان الشبكة - من المهم الحفاظ على أمان الشبكة حتى تعمل الشبكة بطريقة صحيحة لتلبية احتياجات العمل. يتضمن هذا تثبيت برامج حماية الشبكة والحفاظ عليها ، ومراقبة سلوك IP والشبكة ، وتتبع أجهزة نقطة النهاية ، وحل مشكلات أو خروقات الأمان بسرعة.

ثانياً: أنواع شبكات الحاسوب

تقسم شبكات الحاسوب تبعا لوجود مادة فيزيائية تربط بين نقاط وأجهزة الإتصال من عدم وجودها إلى نوعين: شبكات سلكية وشبكات لاسلكية ، إذ تستخدم الشبكات السلكية أنواعا مختلفة من الكوابل لإتمام عملية الاتصال، ولكل نوع من الكوابل مواضع استخدام، فعلى سبيل المثال تستخدم كوابل Unshielded Twisted-Pairs (UTP) داخل المباني لوصل الأجهزة بالخوادم الرئيسة عبر مقاسم الإتصال Switches وتوفر هذه النوعية من الكوابل مسافة اتصال تصل إلى ١٠٠ متر، بينما تستخدم كوابل Shielded Twisted-Pairs (STP) خارج المباني وهي كوابل تماثل كوابل UTP من حيث المادة الفيزيائية الناقلة وعدد الأسلاك الداخلية الدقيقة ومسافة الإتصال الممكنة، لكنها تختلف من حيث أنها مدعمة بعدة طبقات خارجية بغرض حماية هذه الكوابل من الظروف الجوية واحتمالية التعرض للاحتكاك مع الأسطح والأجسام الخارجية، لكن الربط لمسافات أطول وبكفاءة أعلى خصوصا بين مزودي خدمة الإنترنت والجهات المشتركة للحصول على الخدمة يتطلب اللجوء إلى أنواع مختلفة من الكوابل، ومنها كوابل الألياف الضوئية والتي تمنحنا القدرة على نقل البيانات إلى آلاف الكيلومترات وتتمتع بقدرة كبيرة على مقاومة الحرارة والظروف الجوية، وقد حلت كوابل الألياف الضوئية مكان الكوابل المحورية Co-axial Cables والتي تتراوح مسافات الاتصال بين ١٨٠ متر إلى ٥٠٠ متر، فلم تعد تلبي الحاجة للربط مع أماكن جغرافية متباعدة وبسرعات أكبر عدا أنها تحتاج إلى أجهزة إعادة بث للإشارة Repeaters إن أردنا الوصول لمسافات تزيد عن ٥٠٠ متر،وارتفاع كلفة هذه الكوابل وعدم مرونتها وصعوبة تشكيلها وتطويعها بحسب الحاجة.

ثالثاً: الشبكات اللاسلكية Wireless Networks

ما تقدم كان مقدمة تعريفية عن مفهوم الشبكة في مجال تكنولوجيا المعلومات والاتصالات ICT، وتم تبيان أن الشبكة تكون إما سلكية وتتطلب كوابل لاستكمال ربطها بغرض تحقيق الخدمة المطلوبة للمستخدمين، لكن ما يدعو للتوضيح وبصورة ملحة هو النوع الثاني من الشبكات وهو الذي لا يستخدم كوابل لربط المستخدم بمصادر البيانات وبخدمة الإنترنت وهي ما تسمى Wireless Networks وهي تقسم إلى عدة أنواع:

١.شبكات المناطق الشخصية Wireless Personal Area Networks (WPAN)

وهي شبكات لاسلكية تصل بين مجموعة من الأجهزة ضمن مساحة صغيرة نسبياً، وغالبا ما تكون هذه المساحة ضمن نطاق يخدم شخصاً أو مجموعة محدودة من الأشخاص ولا ترتقي لتوفير الخدمة لعدد كبير وضمن مساحة جغرافية كبيرة، وأبرز مثال على هذا النوع هو تقنية البلوتوث Bluetooth، التي تمكن أجهزة الحاسوب والمحمول من الاتصال ومشاركة البيانات.

٢.شبكات المناطق المحلية (Wireless Local Area Networks)(WLAN)

وهي الشبكات الأكثر استخداماً وانتشاراً مابين الشبكات اللاسلكية، وتستخدم للربط على نطاقات أكبر من شبكات المناطق الشخصية، وينتفع منها المستخدمون منها في المنازل ومكاتب العمل وقد يصل نطاق التغطية فيها لعدة كيلومترات، تعتمد هذه الشبكات على معيار يسمى IEEE 802.11 والذي يخولها من الانتفاع من خدمة الربط فيما بينها وبين الانترنت، ويشيع استخدام مصطلح Wi-Fi كبديل عن IEEE 802.11 مع أن Wi-Fi هي شعار لشركة تستخدم معيار IEEE 802.11 للربط بين مجموعة من الأجهزة وللوصول إلى الإنترنت، والصواب علمياً أن لا نستخدم Wi-Fi لأنها تسمية خاصة بشعار شركة وليست معيارا من معايير معهد مهندسي الكهرباء والإلكترونيات(IEEE).

٣. شبكات المناطق الكبيرة Wireless Metropolitan Area Networks (WMAN)

هي شبكات تربط مجموعة شبكات صغيرة مع بعضها البعض، وتكون الشبكات الصغيرة إما شبكة سلكية أو لاسلكية، ومحصلة ما يتم ربطه هو شبكة كبيرة تغطي مساحة لحرم جامعي أو قرية أو حتى مدينة.

يطلق تعبير WiMAX على هذا النوع من الشبكات، وإن رجعنا لمعايير معهد مهندسي الكهرباء والإلكترونيات فإن ما يتم تداوله بين المهندسين المختصين في إنشاء وتفعيل هذه التقنية هو معايير IEEE 802.16d و IEEE 802.16e.

٤.شبكات الأجهزة المحمولة (الخلوية) Cellular Phones' Networks

عادة يتم تبادل بيانات الاتصال بين الأجهزة الخلوية في هذه الشبكات بحسب تكنولوجيا (Global System for Mobile Communications) والتي توفر إتصالا آمنا بين المستخدمين وتحمي بيانات المكالمات الصوتية من الانتهاك وإساءة الاستخدام.

رابعاً: أمن الشبكات اللاسلكية Wireless Networks Security

١. أساسيات في تحديد مفهوم أمن الشبكة اللاسلكية

ينضوي تحت لواء أمن الشبكات اللاسلكية مجموعة من المفاهيم والتي تشكل منظومة أمن الشبكة، وهذه المفاهيم توضح كيف تتم عملية حماية البيانات وتشفيرها وضمان وصولها للأطراف المعنية دون تعقيد وضمن الإجراءات المعمول بها تقنياً.

تشكل مفاهيم سرية البيانات والتحقق من الهوية وصحة البيانات وتوفر الشبكة لب موضوع أمن الشبكة اللاسلكية، ويجب مراعاة الشروط والضوابط لتحقيق هذه المفاهيم ضمن المعايير والسياسات المصرح بها لحماية وضبط البيانات المتداولة.

تعني سرية البيانات Confidentiality إخفاء البيانات عن الأطراف غير المصرح لهم الإطلاع عليها، بينما تقوم عملية التحقق من الهوية Identification بمطابقة اسم المستخدم وكلمة المرور المرسلة مع ما هو مخزن أصلا لدى أجهزة الاتصال اللاسلكية المتاح للاتصال عبر المنطقة الجغرافية المتاحة، وتتم المطابقة بينهما لتحديد الموافقة على عملية الإتصال من عدمها، أما صحة البيانات Data Integrity فهي تشمل عملية التأكد من سلامة البيانات وعدم تعرضها لتخريب أو تغيير أثناء نقلها عبر الشبكة اللاسلكية، وتوفر الشبكةAvailability هي قدرة الشخص الوصول إلى نقاط الإتصال اللاسلكية الخاصة بالشبكة.

يقوم مبدأ أمن الشبكات بشكل عام على تبني مستويات مختلفة من الحماية، حيث يتخصص كل مستوى بمجموعة من الخيارات التي ترمي إلى تأكيد أمنية المعلومات وضمانها، ويقصد بأمن الشبكات حماية أنظمة المعلومات. ما يجدر ذكره والوقوف عنده أن الشبكات اللاسلكية أقل أمنا من الشبكات السلكية لذلك وجب أن يتم وضع سياسات لحماية المعلومات والتي هي تعتبر أصولاً لدى المؤسسات والشركات ولايمكن التفريط بها وتعريضها للخطر.

تنتشر عناوين الشبكات اللاسلكية لكل من هو في النطاق الجغرافي المتاح، وهذا يعد سببا من أسباب محاولات العديد من الناس الوصول لهذه الشبكات، طلبا للحصول على خدمات الربط مع شبكة الإنترنت دون مقابل، ومحاولة للوصول إلى بيانات الأفراد والشركات للاستفادة منها واستغلالها بطريقة غير شرعية وتخريب وإلحاق الضرر بها كذلك.

تقوم مجموعة بروتوكولات بتوفير خدمة الإتصال للشبكات اللاسلكية وإن وجدت أية ثغرة في هذه البروتوكولات فقد تُعرض الشبكة برمتها لخطر الاختراق، فعلى سبيل المثال حدثت في ٢٠١٧ ثغرة في بروتوكول WPA2 وهو المسؤول عن تشفير وإغلاق موزعات الإشارة مما عرض الشبكات اللاسلكية العاملة على معيار IEEE 802.11 للخطر وانتهاك خصوصية البيانات.

٢.طرق حماية الشبكات اللاسلكية

أ. برامج مراقبة بيانات الشبكة Packet Sniffers

تقوم بمراقبة حركة البيانات الداخلة والخارجة بواسطة برامج مراقبة البيانات عبر الشبكات، مثل برنامج الجدار الناري Firewall وأنظمة كشف التسلل Intrusion Detection Systems، من حيث تتبع وترصد هذه البرامج عمليات الاختراق غير المصرح بها، وذلك بعد تحليل للبيانات الداخلة والخارجة، وتفيد هذه البرامج في الكشف عن مواطن الضعف في الشبكة وتحديد عناوين المحتويات المشكوك فيها ليتسنى حجب تلك العناوين.

ب. أدوات فحص مواطن الضعف Vulnerability Scanners

تهدف هذه الأدوات إلى الوصول إلى نقاط الضعف المحتمل حدوث ضرر إثر وجودها، وتتم تحديث هذه الأدوات باستمرار لتبقى في حالة تحري دائم عن أماكن الخلل والتطبيقات المرتبطة بها.

ج. الإعدادات الافتراضية Virtual Settings

تهدف هذه الإعدادات إلى اختبار البروتوكولات وكلمات المرور والبروتوكولات العاملة لتقديم الخدمة، وعادة ما يستهدف المخترقون هذه الإعدادات والتي تعمل في الخلفية.

د. سياسة إختيار وتغيير كلمات المرور Passwords Security Policy

حيث لا بد من استخدام كلمات مرور معقدة للمرور إلى الأنظمة وللاتصال مع الشبكة اللاسلكية وتتكون كلمة المرور المعقدة والمعيارية من حروف وأرقام ورموز، وذلك يُصعب من مهمة المخترق في محاولته التنبؤ بكلمات المرور من خلال خوارزميات تعقب كلمات المرور الذي يلجأ إليه المخترقون، كما أنه يجب أن يراعى عدم استخدام كلمات مرور متكررة على أنظمة وتطبيقات متعددة، فذلك يسهل من عملية الاختراق.

هـ. الصلاحيات Authorities

يجب أن تخضع الصلاحيات المعطاة إلى مصفوفة الصلاحيات الخاصة بالمستخدمين، كلٌ حسب مهمته ودوره، ولا يجوز منح صلاحيات على تطبيق أو ضمن مستوى حماية ممن لا يحق له ذلك.

و. تفعيل التنبيهات Alerting Activation

تقوم هذه التنبيهات بإرسال رسائل إلى مدير النظام أو من ينوب عنه لإخطاره بوجود محاولة اختراق، بهدف معالجة الخلل في أسرع وقت وبما يضمن عدم التسلل وإيقاع الضرر في كافة محتويات نظام المعلومات.

ز. فلترة العناوين MAC Filtering

يعتبر معرفا ماديا لكل جهاز على الشبكة، وتقوم هذه الفلترة بإضافة قائمة العناوين MAC Addresses وذلك للسماح بوصول العناوين المحددة والتي يجب أن تمر من خلال الشبكة اللاسلكية، ومنع كل عنوان غير مدرج ضمن قائمة العناوين MAC Addresses list.

٣. نصائح لحماية الشبكة اللاسلكية من الإختراق

أ. لا تجعل الأجهزة التي لديها قابلية الاتصال لاسلكيا بالانترنت معلنة للجميع، ويتم ذلك بتوقيف SSID Broadcasting وذلك لمنعه من الإعلان عن نفسه والكشف عن هويته.

ب. عدل اسم SSID الخاصة بأجهزة الاتصال اللاسلكي وذلك في سبيل منع اختراق الشبكة.

ج. فعل خاصية التشفير – إن وجدت- ضمن الإعدادات لحماية الشبكة اللاسلكية.

د. للحصول على إشارة أقوى دائما تأكد من وجود خاصية Wireless N على أقل تقدير بينما إن كان هناك إمكانية لشراء أجهزة اتصال لاسلكي بخاصية Wireless AC فستكون سرعة الاتصال أعلى لكن كلفة هذه الأجهزة أكبر.

هـ. إجعل جهاز الاتصال اللاسلكي الموزع للإشارة (الراوتر) قريب من طرفيات وأجهزة الاستخدام، فكلما زادت المسافة بين الراوتر والأجهزة كلما كانت الإشارة أقوى وكانت الأجهزة أسهل في وصولها للعناوين المطلوبة.

و.إن كان هناك مستخدمون تتجاوز كمية استخدامهم الحدود الطبيعية من حجم الحزمة فيمكن تخصيص سرعة الاتصال وتحديدها من خلال خاصية(QoS) Quality of Services.