أساسيات الأمن السيبراني

حقيبة المتدرب

IPAConnect
www.ipa.edu.sa

مركز برامج تقنية المعلومات
قطاع تقنية المعلومات

مُعد الحقيبة

أ. نوره الخليفي

المراجع العلمي

د. مي العتيبي

المراجعة الفنية

إدارة تصميم وتطوير البرامج
العام ١٤٤٣هـ

سجل تطوير الحقيبة

مُعد الحقيبة: أ. نوره الخليفي
تاريخ تطوير الحقيبة: ١٤٤٣هـ

إقرارٌوتعهد

إقرارٌتعهد حقوق ملكية فكرية

الحقيبة التدريبية تعود حقوق ملكيتها الفكرية لمعهد الإدارة العامة وتستخدم لأغراض التدريب بمعهد الإدارة العامة فقط. وعليه أتعهد بعدم استخدام محتوى الحقيبة التدريبية (مادة علمية، استبانات، حالات دراسية، صور، رسوم توضيحية، ...) خارج معهد الإدارة العامة أو مشاركتها مع الغير دون أخذ المو افقات الرسمية والنظامية الصريحة الإلزامية لذلك من صاحب حق الملكية الفكرية وبناءً عليه أتحمل كافة المسؤوليات القضائية الناتجة عن المطالبات والتعويضات المترتبة على الإخلال بذلك.

الفهرس

	المحتوى	الصفحة
	دليل البرنامج التدريبي	٨
	الموضوعات التدريبية	
	اليوم التدريبي الأول: الموضوع الأول (مقدمة في الأمن السيبراني)	
١	التحديات التي تواجه الأمن السيبراني	١٣
٢	أهمية الأمن السيبراني	١٥
٣	مصطلحات أمن المعلومات	١٨
٤	أنواع الهجمات المهددة للأمن السيبراني	٢٠
٥	أنواع المهاجمين	٢٢
	اليوم التدريبي الأول: الموضوع الثاني (تحليل وإدارة مخاطر تقنية المعلومات)	
١	أصول تقنية المعلومات	٢٥
٢	تحليل مخاطر تقنية المعلومات	٢٨
٣	تقييم مخاطر تقنية المعلومات	٢٩
٤	إدارة مخاطر تقنية المعلومات	٣١
	اليوم التدريبي الثاني: الموضوع الثالث (الضوابط الأمنية لحماية الأنظمة التقنية)	
١	البرمجيات الخبيثة	٣٥
٢	الإعدادات الأمنية لنظم التشغيل	٥٢
٣	الأمن المادي	٥٨
	اليوم التدريبي الثاني: الموضوع الرابع (إدارة الهوية والوصول)	
١	التحقق من الهوية	٦٢
٢	إدارة التحكم بالوصول	٧٠
	اليوم التدريبي الثالث: الموضوع الخامس (أمن الشبكات اللاسلكية)	
١	الهجمات المهددة للشبكات اللاسلكية	٧٦
٢	الاحتياطات الأمنية للشبكات اللاسلكية	٨٠
٣	الشبكات الافتراضية الخاصة VPN	٨٢
	اليوم التدريبي الثالث: الموضوع السادس (الحوسبة السحابية)	
١	تعريف الحوسبة السحابية	٨٤
٢	نماذج خدمات الحوسبة السحابية	٨٦
٣	البيئات الافتراضية Virtualization Environments	٨٩
٤	أمن الحوسبة السحابية	٩٤

اليوم التدريبي الرابع: الموضوع السابع (الضوابط الأمنية لحماية البرمجيات والتطبيقات)		
١	الثغرات الأمنية المهددة للبرمجيات والتطبيقات	١٠٠
٢	معايير التطوير الآمن للبرمجيات والتطبيقات	١٠١
٣	ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي	١٠٤
اليوم التدريبي الرابع: الموضوع الثامن (أمن المعلومات في الأجهزة المحمولة)		
١	التهديدات الأمنية للأجهزة المحمولة	١٠٨
٢	الضوابط الأمنية لحماية الأجهزة المحمولة	١١٣
اليوم التدريبي الرابع: الموضوع التاسع (التشفير)		
١	مقدمة في التشفير Cryptography	١١٦
٢	الشهادات الرقمية	١٢٢
٣	إدارة الشهادات الرقمية	١٢٤
٤	البنية التحتية للمفاتيح العامة	١٢٧
٥	البروتوكولات المشفرة لنقل البيانات	١٣١
اليوم التدريبي الخامس: الموضوع العاشر (الهندسة الاجتماعية)		
١	الأساليب النفسية	١٣٥
٢	أنواع هجمات الهندسة الاجتماعية	١٤٠
٣	الحماية من هجمات الهندسة الاجتماعية	١٤١
اليوم التدريبي الخامس: الحادي عشر (الاستجابة للأحداث والتعافي من الكوارث)		
١	فريق الاستجابة للحوادث الأمنية	١٤٣
٢	خطط الاستجابة للحوادث	١٤٥
٣	استمرارية الأعمال	١٤٨
اليوم التدريبي الخامس: الموضوع الثاني (الاستراتيجية الوطنية للأمن السيبراني في المملكة العربية السعودية)		
١	دور الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority	١٤٩
٢	الاستراتيجية الوطنية للأمن السيبراني	١٥٢
٣	سياسات ومعايير الأمن السيبراني	١٥٩
٤	نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية	١٦٤
الأنشطة التدريبية		
١	أسئلة ونقاش (١)	١٧
٢	عصف ذهني (١)	٢٤
٣	حالة دراسية (١)	٢٧
٤	حالة دراسية (٢)	٣٢
٥	تطبيق عملي (١)	٤٤
٦	تطبيق عملي (٢)	٤٧
٧	حالة دراسية (٣)	٦٠

٨	تطبيق عملي (٣)	٦٤
٩	تطبيق عملي (٤)	٦٧
١٠	تطبيق عملي (٥)	٧٢
١١	تطبيق عملي (٦)	٨١
١٢	أسئلة ونقاش (٢)	٨٨
١٣	أسئلة ونقاش (٣)	٩٧
١٤	تطبيق عملي (٧)	١٠٧
١٥	تطبيق عملي (٨)	١١٢
١٦	تطبيق عملي (٩)	١١٥
١٧	تطبيق عملي (١٠)	١٢١
١٨	تطبيق عملي (١١)	١٢٣
١٩	تطبيق عملي (١٢)	١٢٦
٢٠	عصف ذهني (٢)	١٣٦
٢١	عصف ذهني (٣)	١٤٢
٢٢	عصف ذهني (٤)	١٤٦
٢٣	تطبيق عملي (١٣)	١٦٣
٢٤	عصف ذهني (٥)	١٦٨
٢٥	حالة دراسية مطولة (٤)	١٦٩
	الجداول	
١	جدول (١): *الأنواع الأساسية لهجمات المهددة للأمن السيبراني*	٢٢
٢	جدول (٢): *تصنيف أنواع الأصول*	٢٧
٣	جدول (٣): *فئات التهديد*	٢٨
٤	جدول (٤): *مقياس احتمالية حدوث المخاطر*	٢٩
٥	جدول (٥): *أساليب إدارة المخاطر الأربعة*	٣٥
٦	جدول (٦): *أنواع أنظمة التشغيل الرئيسية*	٥٢
٧	جدول (٧): *تحليل الأمن المادي حسب مكونات الحماية*	٦٠
٨	جدول (٨): *تصنيف أنواع الخدمات السحابية*	٨٨
٩	جدول (٩): *مزايا مزودين خدمة.*	٩٧
١٠	جدول (١٠): *أنواع اختبارات البرمجيات والتطبيقات.*	١٠٣
١١	جدول (١١): *توصيات المركز الوطني الإرشادي للأمن السيبراني في ا لتعامل مع الأجهزة المحمولة*	١١٤
١٢	جدول (١٢): *المبادئ النفسية الأساسية الهندسة الاجتماعية.*	١٣٥
١٣	جدول (١٣): *اختبار:(صيد المتصيد).*	١٣٧

الأشكال

١	شكل ١ -العناصر الأساسية لأمن المعلومات	١٢
٢	شكل ٢ -قائمة أدوات الهجوم في واجهة نظام Kali Linux	١٤
٣	شكل ٣ -مصطلحات أمن المعلومات	١٩
٤	شكل ٤ -الإرسال الآمن للبيانات	٢٠
٥	شكل ٥ -حالات الهجوم	٢١
٦	شكل ٦ -مصفوفة تقييم المخاطر	٣٠
٧	شكل ٧-واجهة أحد برامج Keylogger	٤١
٨	شكل ٨-جهاز راصد لوحة المفاتيح	٤٢
٩	شكل ٩ -إعداد مكافح البريد المزعج (خطوة ١)	٤٨
١٠	شكل ١٠ -إعداد مكافح البريد المزعج (خطوة٢)	٤٨
١١	شكل ١١ -إعداد مكافح البريد المزعج (خطوة٣)	٤٩
١٢	شكل ١٢ -إعداد مكافح البريد المزعج (خطوة٤)	٥٠
١٣	شكل ١٣ -مانع النوافذ المنبثقة في Chrome	٥١
١٤	شكل ١٤ -شاشة Windows Settings	٥٥
١٥	شكل ١٥ -شاشة Update Status	٥٦
١٦	شكل ١٦-جهاز مسح بصمات الأصابع	٦٥
١٧	شكل ١٧ -عملية تسجيل الدخول باستخدام اسم المستخدم وكلمة المرور	٦٨
١٨	الشكل ١٨ -التحكم في الوصول التقديري في نظام ويندوز	٧٠
١٩	شكل ١٩-التوأم الشرير	٧٦
٢٠	شكل ٢٠-العنوان الفيزيائي	٧٩
٢١	شكل ٢١-الشبكة الافتراضية الخاصة VPN	٨٢
٢٢	شكل ٢٢ -الفروقات بين نماذج الخدمات السحابية	٨٧
٢٣	شكل ٢٣ -طبقات البيئة الافتراضية	٩٠
٢٤	شكل ٢٤ -برمجية التقنية الافتراضية المبنية على التجهيزات المادية	٩١
٢٥	شكل ٢٥ -برمجية التقنية الافتراضية المبنية على البرمجيات	٩٢
٢٦	شكل ٢٦-دورة حياة تطوير البرمجيات والتطبيقات	١٠٢
٢٧	شكل ٢٧ -رمز الاستجابة السريعةQR code	١١٠
٢٨	شكل ٢٨ -عملية التشفير	١١٦
٢٩	شكل ٢٩ -التشفير المتناظر Symmetric Cryptography	١١٨
٣٠	شكل ٣٠ -التشفير غير المتناظر Asymmetric cryptography	١١٩
٣١	شكل ٣١ - Certificate Revocation List (CRL)	١٢٥
٣٢	شكل ٣٢ -عملية تسجيل الشهادة الرقمية	١٢٨
٣٣	شكل ٣٣ -الاتصال بموقع من خلال بروتوكول http	١٣١
٣٤	شكل ٣٤ -رؤية المملكة ٢٠٣٠ والاستراتيجية الوطنية للأمن السيبراني	١٥٢

٣٥	**شكل ٣٥**-محاور وعناصر الإطار المرجعي لتطوير الاستراتيجية الوطنية للأمن السيبراني	١٥٣
٣٦	**شكل ٣٦** -الأهداف الاستراتيجية الوطنية للأمن السيبراني	١٥٧
٣٧	**شكل ٣٧** -مؤشرات الأداء	١٥٨
	المراجع العلمية	
١	**المراجع العربية**	١٧٤
٢	**المراجع الأجنبية**	١٧٤

دليل البرنامج التدريبي

الهدف العام للبرنامج	تنمية مهارات المتدربين في مجال تهديدات الأمن السيبراني والتعرف على المخاطر التي تواجه الفضاء السيبراني وتطبيق الحلول الأمنية المناسبة بكفاءة وفعالية.
الأهداف التفصيلية	من المتوقع بعد انتهاء المتدرب من البرنامج التدريبي أن يكون قادراً على: ١. يتعرف على المفاهيم الأساسية للأمن السيبراني بسهوله ويسر. ٢. يدير المخاطر التي تهدد الفضاء السيبراني بكفاءة وفعالية. ٣. يطبق الضوابط الأمنية اللازمة لحماية الأنظمة التقنية بدقة وإتقان. ٤. يميز بين آليات إدارة الهوية والتحكم في الوصول بكفاءة وفعالية. ٥. يطبق الضوابط الأمنية اللازمة لحماية الشبكات اللاسلكية بدقة وإتقان. ٦. يتعرف على أمن الحوسبة السحابية بسهولة ويسر. ٧. يطبق الضوابط الأمنية اللازمة لحماية البرمجيات والتطبيقات بكفاءة وفعالية. ٨. يطبق طرق حماية الأجهزة المحمولة بدقة وإتقان. ٩. يلم بآليات التشفير المعززة للأمن السيبراني بسهولة ويسر. ١٠. يتعرف على طرق الحماية من هجمات الهندسة الاجتماعية بشكل صحيح. ١١. يخطط لإجراءات الاستجابة للأحداث والتعافي من الكوارث لضمان استمرارية الأعمال بكفاءة وفعالية. ١٢. يساهم في تحقيق الاستراتيجية الوطنية للأمن السيبراني في المملكة العربية السعودية بشكل إيجابي.
مدة البرنامج	خمسة أيام تدريبية
عدد الساعات	٣٠ ساعة تدريبية
موضوعات البرنامج	١. مقدمة في الأمن السيبراني. ٢. تحليل وإدارة مخاطر تقنية المعلومات. ٣. الضوابط الأمنية لحماية الأنظمة التقنية. ٤. إدارة الهوية والوصول. ٥. أمن الشبكات اللاسلكية. ٦. أمن الحوسبة السحابية. ٧. الضوابط الأمنية لحماية البرمجيات والتطبيقات. ٨. أمن المعلومات في الأجهزة المحمولة. ٩. التشفير. ١٠. الهندسة الاجتماعية. ١١. التعافي من الكوارث والاستجابة للأحداث. ١٢. الاستراتيجية الوطنية للأمن السيبراني في المملكة العربية السعودية.

اليوم التدريبي الأول

الموضوع الأول: مقدمة في الأمن السيبراني.

الموضوع الثاني: تحليل وإدارة مخاطر تقنية المعلومات.

المخطط التدريبي لليوم الأول

الجلسة الأولى

- (٨:٠٠:٩:٣٠)
- مقدمة في الأمن السيبراني.

استراحة (٩:٣٠:١٠:٠٠)

الجلسة الثانية

- (١٠:٠٠:١١:٣٠)
- تحليل وإدارة مخاطر تقنية المعلومات (١).

استراحة (١١:٣٠:١٢:٣٠)

الجلسة الثالثة

- (١٢:٣٠:٢:٠٠)
- تحليل وإدارة مخاطر تقنية المعلومات (٢).

الموضوع الأول: مقدمة في الأمن السيبراني

مع بداية ظهور شبكة الإنترنت، لم يكن هناك قلق تجاه حدوث جرائم يمكن أن تُنتهك على الشبكة وبالتالي قد تهدد المعلومات التي يتم تبادلها من خلالها، وذلك نظرًا لمحدودية مستخدميها علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثون ومنسوبو الجامعات. لهذا فشبكة الإنترنت ليست آمنة في أصل تصميمها وبناءها. لكن مع توسع استخدام شبكة الإنترنت ودخول جميع فئات المجتمع إلى قائمة مستخدميها بدأت تظهر جرائم تستهدف الأمن المعلوماتي على الشبكة وأخذت تزداد مع الوقت وتعددت صورها وأشكالها مع تطور أساليب المخترقين وتنوع هجماتهم، لذلك ظهرت الحاجة الملحة إلى تطوير الأساليب والتقنيات الأمنية لحماية الفضاء السيبراني خاصة مع زيادة الاعتماد على شبكة الإنترنت في تقديم الخدمات الحكومية والتجارية وإنجاز المعاملات المالية وتبادل المعلومات السرية والحساسة.

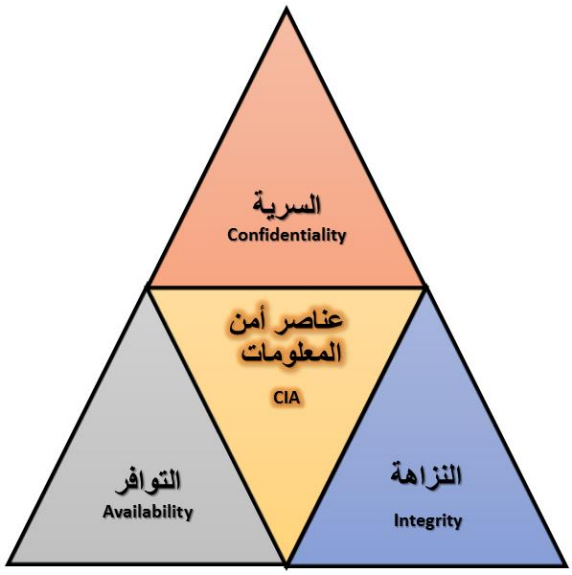
ولفهم الوضع العام بشكل أعمق، لنا أن نتخيل حجم الخسائر المادية التي تتكفلها الحكومات والقطاعات الخاصة وحتى الأفراد نتيجة ازدياد الهجمات الإلكترونية، حيث تم تقدير تكاليف الأضرار الناجمة عن الجرائم الإلكترونية عالمياً في عام ٢٠٢١ بحوالي ستة ترليون دولار، بمعنى أنه قد تم خسارة حوالي ٦٨٥ مليون دولار في كل ساعة في عام ٢٠٢١، ومن المتوقع ازدياد هذه التكاليف والتي قد تصل إلى ١٠,٥ ترليون دولار في عام ٢٠٢٥. مما يجعل قضايا الأمن السيبراني ذات أولوية عالية لتوفير الأمن المعلوماتي والتقني على كافة الأصعدة. (Cybersecurity Venture, ٢٠٢١).

يتكون الفضاء الإلكتروني من العناصر والمكونات التي تعتمد على تكنولوجيا الكمبيوتر والاتصالات، والمعلومات التي تستخدمها هذه المكونات أو تخزنها أو تتعامل معها أو تعالجها، إضافة إلى آليات الترابط بينها. (Stallings, ٢٠١٩).
لذلك، يتم وصف الأمن السيبراني على أنه مجموعة من الأدوات والسياسات والمفاهيم الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر وأفضل الإجراءات والممارسات والتقنيات المستخدمة لحماية الفضاء السيبراني وأصول المنظمة والمستخدم. حيث تتضمن أصول هذه الأصول أجهزة الكمبيوتر والمستخدمين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المرسلة والمخزنة في بيئة الفضاء الإلكتروني. يسعى الأمن السيبراني جاهدًا لضمان تحقيق وصيانة الخصائص الأمنية للمنظمة وأصول المستخدم ضد المخاطر الأمنية ذات الصلة في بيئة الفضاء السيبراني. تشمل الأهداف الأمنية العامة ما يلي: السرية والنزاهة والتوافر. (Stallings, ٢٠١٩)

كما يمكن أن يُعرّف أمن المعلومات بأنه حماية كل من المعلومات ونظم المعلومات من الأعمال غير المصرح بها كالوصول أو الاستخدام أو الإفشاء أو الإخلال أو التعديل أو التدمير وذلك لضمان السرية، النزاهة، التوافر، حيث يتحقق أمن المعلومات حماية الخصائص الثلاثة السابقة والمعروفة بـ(CIA). (أغروال، كامبو، بيرس، ٢٠١٨).

ويمكن تعريف العناصر الثلاثة لأمن المعلومات والموضحة في شكل (١) كما يلي: (القحطاني، ٢٠١٥):

١. **السرية:(Confidentiality)** وتعني الحفاظ على المعلومات من أن يطلع عليها غير الأشخاص المصرح لهم فقط، وبالتالي حماية البيانات الكشف غير المصرح به.
٢. **النزاهة:(Integrity)** وتعني الحفاظ على سلامة المعلومات من التعديل أو الحذف أو الإضافة غير المصرح به.
٣. **التوافر:(Availability)** وتعني أن تكون المعلومات قابلة للوصول إليها واستخدامها حين طلبها من الأطراف المخول لهم بذلك وفي أي وقت.



شكل (١): *عناصر أمن المعلومات CIA.*

بشكل عام، يشمل الأمن السيبراني أمن المعلومات الإلكترونية، وأمن البنى التحتية التقنية. بينما يهتم أمن المعلومات بصورة أشمل بأمن المعلومات الإلكترونية والمعلومات المادية أيضاً مثل المعلومات الموجودة بصورة ورقية. ومع ذلك، من الناحية العملية، غالبًا ما يتم استخدام مصطلحات الأمن السيبراني وأمن المعلومات بالتبادل. (Stallings, ٢٠١٩).

يجري التعامل مع المعلومات من خلال منظومة من المكونات الرئيسية التي تتولى تخزين المعلومات ومعالجتها ونقلها بأشكالها كافة، وهذه المكونات هي: المكونات المادية أو العتاد (Hardware)، المكونات البرمجية (Software)، والبيانات (Data)، والمستخدمون (Users)، والشبكات (Networks)، والإجراءات (Procedures). وتتعامل هذه المكونات مع المعلومات كمورد رئيس من موارد المنشأة يجب المحافظة عليه، وتأمينه ضد التعامل الخاطئ أو التعدي المعتمد. ويمكن إيضاح كل مكون كما يلي: (القحطاني، ٢٠١٥).

- المكونات المادية أو العتاد (Hardware): ويقصد بها الأجهزة والمعدات التقنية التي تحتوي على البرامج وتشغلها، وتحتفظ بالبيانات وتعالجها وترسلها، مثل الخوادم (Servers) والحاسبات الآلية بمختلف أنواعها، وأجهزة التخزين، وأجهزة الشبكة، إلى غير ذلك من التجهيزات المادية المحسوسة والتي يجب حمايتها من التلف أو الفقد أو السرقة.
- المكونات البرمجية (Software): ويقصد بها البرامج والأوامر التي يتم استخدامها في التحكم بالمكونات المادية، حيث تعتبر الوسيط بين المستخدم والمكون المادي، وتنقسم المكونات البرمجية إلى مكونين رئيسيين هما نظام التشغيل والبرامج.

- البيانات (Data): ويقصد بها ما يتم معالجته وتخزينه وإرساله عبر المكونات الأخرى، حيث تعتبر المادة الأساسية للمعلومات في شكلها المقروء والمفهوم.
- والمستخدمون (Users): وهم من يعمل على المكونات المادية، ويتعامل مع البرامج، ويدخل المعلومات، ويطبع التقارير، وينفذ الإجراءات، ويتواصل من خلال الشبكة. يمكن وصف المستخدمين بأنهم المحرك الحقيقي في منظومة أنظمة المعلومات والمستهدفين بالجزء الأكبر من أنظمة الحماية التابعة لها، والذين يجب أن يتمتعوا بمستوى عالٍ من التدريب والتأهيل وفق سياسة المنشأة العامة ووفق السياسات الأمنية الخاصة بالمعلومات.
- الشبكات (Networks): وهي منظومة من أجهزة الحاسب الآلي والبرامج وأجهزة الربط المتصلة فيما بينها بأحد وسائل نقل البيانات.
- الإجراءات (Procedures): وهي الأوامر المكتوبة لتنفيذ مهام محددة. تعد الإجراءات هي الرابط بين المستخدمين والمكونات المادية والبرمجية، فهي التي تحدد طريقة العمل الذي يُنفذ من خلال تلك المكونات بما يضمن أمن المعلومات في المنشأة، من خلال تحديد اختصاص كل مستخدم وما يمكنه من الاطلاع عليه.

العنصر الأول: تحديات التي تواجه الأمن السيبراني:

التحديات المتمثلة في الحفاظ على أمان أجهزة الكمبيوتر والأنظمة التقنية أكبر من أي وقت مضى، ليس فقط بسبب استمرارية الهجمات، ولكن أيضًا بسبب الصعوبات التالية التي نواجهها في الدفاع ضد هذه الهجمات:(Ciampa, ٢٠١٨)

- **الكم الهائل من الأجهزة المتصلة عالمياً:** اليوم تقريبًا كل جهاز تقني -ليس فقط أجهزة الكمبيوتر التقليدية ولكن حتى كاميرات المراقبة والمصابيح الكهربائية القابلة للبرمجة -متصل بالإنترنت. في عام ٢٠٢١، كان هناك ٤,٦٦ مليار مستخدم نشط على الإنترنت في جميع أنحاء العالم أي ما يشكل ٥٩,٥% من سكان الكرة الأرضية (https://www.statista.com/, ٢٠٢١). على الرغم من أن هذا يوفر فوائد هائلة، إلا أنه يجعل من السهل أيضًا على أي مهاجم حول العالم من شن هجومه بصمت ضد أي جهاز متصل بالإنترنت.
- **زيادة سرعة الهجمات:** يتمكن المهاجمين باستخدام الأدوات الحديثة المتاحة لهم من فحص ملايين الأجهزة في وقت قياسي للعثور على نقاط الضعف وشن الهجمات بسرعة غير مسبوقة. وبإمكان معظم هذه الأدوات من شن هجمات جديدة دون أي تدخل بشري، مما يزيد من سرعة مهاجمة الأنظمة.
- تقدم وتطور الهجمات: أصبحت الهجمات أكثر تعقيدًا من ذي قبل، مما يزيد من صعوبة اكتشافها وتشكيل الدفاعات ضدها، حيث يستخدم العديد من المهاجمين بروتوكولات مشتركة لتوزيع هجماتهم، مما يزيد من صعوبة تمييز الهجوم عن حركة نقل البيانات الطبيعية. تختلف أدوات الهجوم الأخرى في سلوكها بحيث يظهر نفس الهجوم بشكل مختلف في كل مرة، مما يزيد من تعقيد عملية اكتشاف الهجوم.
- **توافر أدوات الهجوم وبساطتها:** في السابق، كان المهاجم بحاجة إلى معرفة تقنية واسعة بالشبكات وأجهزة الكمبيوتر بالإضافة إلى القدرة البرمجية لكتابة البرامج الخاصة بتوليد الهجمات. ولكن اليوم الوضع لم يعد كذلك. حيث لا تتطلب أدوات وبرامج الهجوم الحديثة معرفة متطورة من قبل المهاجم. في الواقع، تحتوي العديد من الأدوات -مثل الأدوات

المتوفرة في واجهة نظام Kali Linux الموضحة في شكل (٢) على واجهة مستخدم رسومية (GUI) تتيح للمستخدم تحديد الخيارات بسهولة من القائمة. وهذه الأدوات متاحة بشكل عام مجانًا. بالإضافة إلى ذلك، غالبًا ما يبيع المهاجمون الذين يصنعون أدوات الهجمات هذه الأدوات لمهاجمين آخرين.

شكل (٢): قائمة أدوات الهجوم في واجهة نظام Kali Linux

- **اكتشاف الثغرات الأمنية بشكل أسرع:** يمكن الكشف عن نقاط الضعف في الأجهزة والبرامج واستغلالها بسرعة باستخدام أدوات وتقنيات هجوم جديدة. في كثير من الأحيان قد يجد المهاجم ثغرة أمنية ويبدأ بالاستفادة منها في شن هجومه من خلالها قبل أن يكتشفها المستخدمون أو أخصائي الأمن المعلوماتي. وهذا ما يسمى بالهجوم دون انتظار Zero Day Attack، حيث لا توجد مهلة تحذيرية قبل هذا التهديد الجديد.
- **التأخير في التحديثات الأمنية:** يعاني منتجو الأجهزة والبرمجيات من الارتباك في محاولة مواكبة تحديث منتجاتهم ضد الهجمات. حيث قد يتلقى أحد المعاهد المتخصصة في مجال أمن برامج مكافحة الفيروسات أكثر من ٣٩٠ ألف عملية إرسال من البرامج الضارة المحتملة كل يوم، وبهذا المعدل يتعين على منتجي برامج مكافحة الفيروسات إنشاء تحديثات وتوزيعها كل بضع ثوانٍ للحفاظ على حماية المستخدمين بشكل كامل.
- **ضعف توزيع التحديث الأمني:** منتجي البرمجيات السائدة والمنتشرة، مثل Microsoft و Apple وAdobe، لديهم نظام لإخطار المستخدمين بالتحديثات الأمنية لمنتجاتهم وتوزيعها بشكل منتظم، ولكن يتم اعتبارهم من منتجي البرامج القلة الذي استثمروا في أنظمة التوزيع المكلفة. لا يدرك المستخدمون عمومًا أن هناك تحديثًا أمنيًا موجودًا لمنتج ما مالم توجد وسائل موثوقة من المُنتج لتنبيه المستخدم. بالإضافة إلى أن هؤلاء المنتجون لا يقومون في كثير من الأحيان بإنشاء تحديثات أمنية صغيرة تعمل على تصحيح البرامج الموجودة؛ وبدلاً من ذلك، يقومون بإصلاح المشكلة في إصدار جديد تمامًا من البرنامج — ثم يطلبون من المستخدم الدفع مقابل الإصدار المحدث الذي يحتوي على التصحيحات والتحديثات الأمنية.

- **الهجمات الموزعة Distributed attacks:** يمكن للمهاجمين استخدام الملايين من أجهزة الكمبيوتر أو الأجهزة التي فرضوا سيطرتهم عليها في شن في هجوم ضد خادم أو شبكة واحدة. وذلك بالهجوم باستخدام نهج "many against one" والذي يستحيل تقريباً إيقافه نظرا لصعوبة تحديد مصدره وبالتالي حظره.
- **استخدام الأجهزة الشخصية في بيئة العمل:** تسمح العديد من المنظمات للموظفين باستخدام أجهزتهم الشخصية وتوصيلها بشبكة الشركة. وقد جعل ذلك من الصعب على أقسام تقنية المعلومات أن تتمكن من توفير مستوى الأمان المطلوب لمجموعة كبيرة جدا من الأجهزة التي لا يمتلكونها وليست تحت تحكمهم.
- **ضعف وعي المستخدم:** بشكل مستمر ومتزايد، يتعين على المستخدمين أن يقوموا باتخاذ قرارات أمنية صعبة فيما يتعلق بأنظمة الكمبيوتر الخاصة بهم، وأحيانًا تكون المعلومات قليلة أو معدومة لتوجيههم لاتخاذ القرار السليم. حيث أنه من المعتاد أن يتم طرح أسئلة تتعلق بالنواحي الأمنية على المستخدم، مثل هل تريد عرض المحتوى الآمن فقط؟ أو هل الملف المرفق آمن؟ أو هل تريد تثبيت هذه الوظيفة الإضافية؟ مع القليل من التوجيه أو بدون توجيه، يميل هؤلاء المستخدمون غير المدربين إلى تقديم إجابات للأسئلة واتخاذ قرارات دون فهم المخاطر الأمنية المحتملة.

العنصر الثاني: أهمية الأمن السيبراني:

الأمن السيبراني مهم للمؤسسات وكذلك للأفراد، وذلك لأنه يشكل درع حماية من عمليات سرقة البيانات ومحاولات انتحال الهوية، بالإضافة إلى تجنب العواقب القانونية لعدم تأمين المعلومات، والحفاظ على الإنتاجية، وإحباط الإرهاب السيبراني. (Ciampa, ٢٠١٨)

- **منع سرقة البيانات:** غالبًا ما يرتبط الأمن المعلوماتي بمنع سرقة البيانات، حيث غالبًا ما تستشهد المؤسسات بأن أحد أهدافها الرئيسية لأمن المعلومات هو حماية بياناتها من السرقة، كسرقة المعلومات المتعلقة بحقوق الملكية الفكرية الخاصة بالأعمال التجارية في المؤسسات أو سرقة قائمة العملاء التي يرغب المنافسون في الحصول عليها. أما على الصعيد الشخصي، فتعتبر سرقة البيانات الشخصية للأفراد مثل أرقام بطاقات الائتمان من مستهدفات المهاجمين وذلك لاستغلال هذه البيانات بهدف شراء البضائع عبر الإنترنت قبل أن تدرك الضحية أن رقم بطاقة الائتمان قد سُرق.
- **إحباط محاولات انتحال الهوية:** تتضمن عمليات انتحال الهوية سرقة المعلومات الشخصية لشخص آخر بغرض انتحال هوية الضحية، وغالبا ما يكون ذلك بهدف تحقيق مكاسب مالية، حيث يتمكن المهاجمين من انشاء حسابات بنكية أو إصدار بطاقات ائتمانية جديدة باسم الضحية، ثم يتم تحميل عمليات شراء كبيرة على هذه الحسابات والبطاقات، مما يترك الضحية مسؤولاً عن الديون ويدمر تصنيفه الائتماني.
- **تجنب العقوبات القانونية لعدم تأمين المعلومات:** في السنوات الأخيرة سنت قوانين وعقوبات للحد من الجرائم الإلكترونية وحماية المستخدمين منها. فقد تتعدى عقوبات الجرائم الإلكترونية الغرامات المالية وتصل للسجن سنوات عدة. كما لم تقتصر العقوبة على المهاجم فقط بل قد تكون المؤسسة أو المنظمة التي هوجمت وتسربت معلومات مستخدميها الخاصة أو السرية عرضة للمساءلة والعقاب نتيجة لعدم تأمين معلوماتهم بشكل كافي.

- **الحفاظ على الإنتاجية:** يحتاج تعافي الأجهزة والأنظمة التقنية بعد تعرضها للهجوم إلى الوقت والمال حتى تعود إلى وضعها الطبيعي وذلك مما يشكل استهلاك إضافي لموارد المؤسسات. بالإضافة إلى توقف إنتاجية الموظفين أثناء الهجوم أو بعده لأن أجهزة الكمبيوتر والشبكات لا تكون تعمل بشكل صحيح.
- **إحباط الإرهاب السيبراني:** يُعرف الإرهاب السيبراني بأنه أي "هجوم متعمد وذو دوافع سياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى عنف بأهداف غير قتالية من قبل مجموعات فرعية أو عملاء سريين". على عكس الهجوم المصمم لسرقة المعلومات أو تدميرها، تهدف هجمات الإرهاب الإلكتروني إلى إثارة الذعر أو إثارة العنف بين المواطنين. يتم توجيه الهجمات إلى أهداف مثل القطاع المصرفي والمنشآت العسكرية ومحطات الطاقة ومراكز مراقبة الحركة الجوية وأنظمة المياه. هذه أهداف مرغوبة من الإرهابيين لأنها يمكن أن تعطل بشكل كبير الأنشطة العادية لعدد كبير من السكان. على سبيل المثال، يمكن أن يؤدي تعطيل محطة طاقة كهربائية إلى شل الأعمال والمنازل وخدمات النقل والاتصالات على مساحة سكنية واسعة.

أسئلة ونقاش (١)

الهدف: أن يتعرف المتدرب على وضع الهجمات الإلكترونية عالمياً.

الزمن: ٥ دقائق

تزداد أعداد الهجمات سنوياً على مستوى العالم مع ازدياد مستوى صعوبتها وتنوع أشكالها، ولكن ما الذي يحدث الآن عالمياً؟

.....

.....

.....

.....

الإرشادات:

١. يعمل المتدربون على الدخول على الرابط https://threatmap.checkpoint.com/

٢. استعراض الخريطة الحية لوضع الهجمات في العالم واستعراض الإحصائية اليومية لها.

٣. يعمل المدرب على مناقشة النتائج مع المتدربين

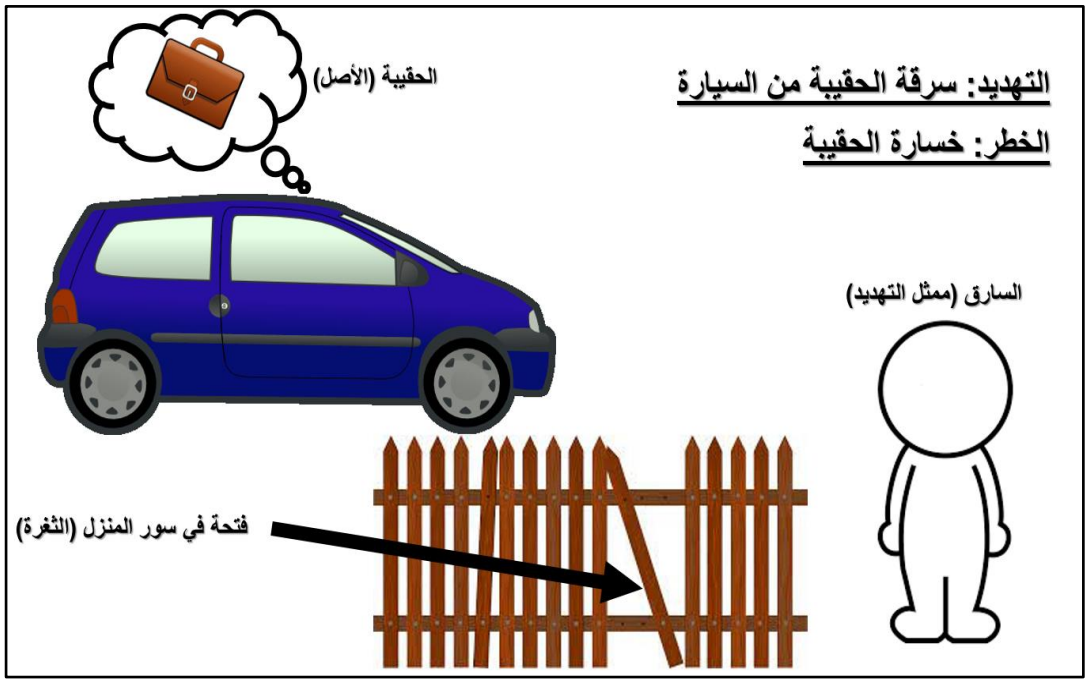
العنصر الثالث: مصطلحات أمن المعلومات:

يمكن تحديد المصطلحات الأساسية لأمن المعلومات كما يلي: (Ciampa, ٢٠١٨):

- **الأصل (Asset):** يتم تعريفه على أنه أي عنصر له قيمة ويجب حمايته. على مستوى المنظمات، تمتلك الأصول الصفات التالية: توفر قيمة للمنظمة؛ ولا يمكن استبدالها بسهولة دون تأثير كبير في استثمار المنظمة ونفقاتها ومواردها؛ ويمكن أن تشكل جزءًا من هوية المنظمة. بناءً على هذه الصفات، لا يمكن تصنيف جميع عناصر البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة كأصل. على سبيل المثال، الكمبيوتر المكتبي المعطل الذي يمكن استبداله بسهولة لا يُعتبر بشكل عام أحد الأصول ومع ذلك، يمكن أن تكون المعلومات الموجودة على هذا الكمبيوتر أحد أصول المنظمة.
- **التهديد (Threat):** يتم تعريفه بأنه أي حدث أو إجراء من الممكن أن تسبب بالضرر. وبناءً على ذلك فإن تهديدات أمن المعلومات هي عبارة عن أي أحداث أو أفعال من الممكن أن تمثل خطرًا على أصول المعلومات. التهديد في حد ذاته لا يعني أن الأمن قد تعرض للخطر؛ ولكن تجاهله قد يؤدي إلى التسبب في خسارة حقيقية في الأمن السيبراني، مثل تدمير المعلومات أو سرقتها أو تأخير نقلها، أو حتى فقدان السمعة.
- **ممثل التهديد (Threat actor):** وهو أي شخص أو عنصر لديه القدرة على تنفيذ تهديد. في الأمن المعلوماتي، يمكن أن يكون ممثل التهديد –والذي ممكن أن يطلق عليه مسمى (المهاجم) -شخص يحاول اقتحام شبكة كمبيوتر آمنة، وقد تكون أيضًا برامج ضارة تهاجم شبكة الكمبيوتر، أو حتى ظاهرة طبيعية مثل الإعصار الذي يمكن أن يدمر معدات الكمبيوتر ومعلوماته.
- **الثغرة (Vulnerability):** وهي أي خلل أو ضعف يسمح لممثل التهديد –أو المهاجم-بتجاوز الحواجز الأمنية، مثل وجود خلل برمجي في نظام التشغيل يسمح للمهاجم بالتحكم في جهاز كمبيوتر دون علم المستخدم أو إذنه.
- **الخطر (Risk):** وهو مدى احتمالية أن يتم استغلال الثغرة من قبل ممثل التهديد أو المهاجم. وفي الواقع لا يمكن أبدًا أن يُقضى على الخطر بشكل كامل لأن ذلك يكلف الكثير من الجهد والمال والوقت. لذلك يجب علينا دائمًا افتراض إمكانية حدوث الخطر. وبناءً عليه فهنالك أربعة خيارات أمام المنظمات في التعامل مع المخاطر وهي: قبول المخاطر، أو التقليل منها أو نقلها أو منعها.

ولتوضيح أفضل لمصطلحات أمن المعلومات، لنفترض السيناريو الموضح في شكل (٣): *مصطلحات أمن المعلومات*.

من خلال وجود خطر سرقة حقيبة من سيارة تم ركنها في داخل سور المنزل نتيجة تحطم جزء من السور الذي يمكن استغلاله من السارق للوصول إلى السيارة والحصول على الحقيبة.



شكل (٣): مصطلحات أمن المعلومات.

العنصر الرابع: أنواع الهجمات المهددة للأمن السيبراني:

يعتمد الإرسال الآمن للبيانات –كما هو موضح في
شكل *(٤): الإرسال الآمن للبيانات*-على أن المعلومات تُرسل من المُرسل الحقيقي لها إلى المُستقبل الحقيقي من دون تعرضها للتغيير او الحذف أو الاطلاع عليها من قبل أطراف غير مُصرح لها بذلك.

شكل (٤): الإرسال الآمن للبيانات.

ولكن في حال عدم تأمين عملية الإرسال، فمن الممكن أن تتعرض البيانات للانتهاك من خلال تعرضها لأحد حالات الهجوم التالية:

١. الاعتراض Interception: ويتم ذلك من خلال تمكن طرف غير مصرح له على مراقبة الاتصال بين المرسل والمستقبل للاطلاع على المعلومات السرية وهو ما يسمى بالتنصت على الاتصال Eavesdropping (شكل (٥): *حالات الهجوم*.

٢. - أ).

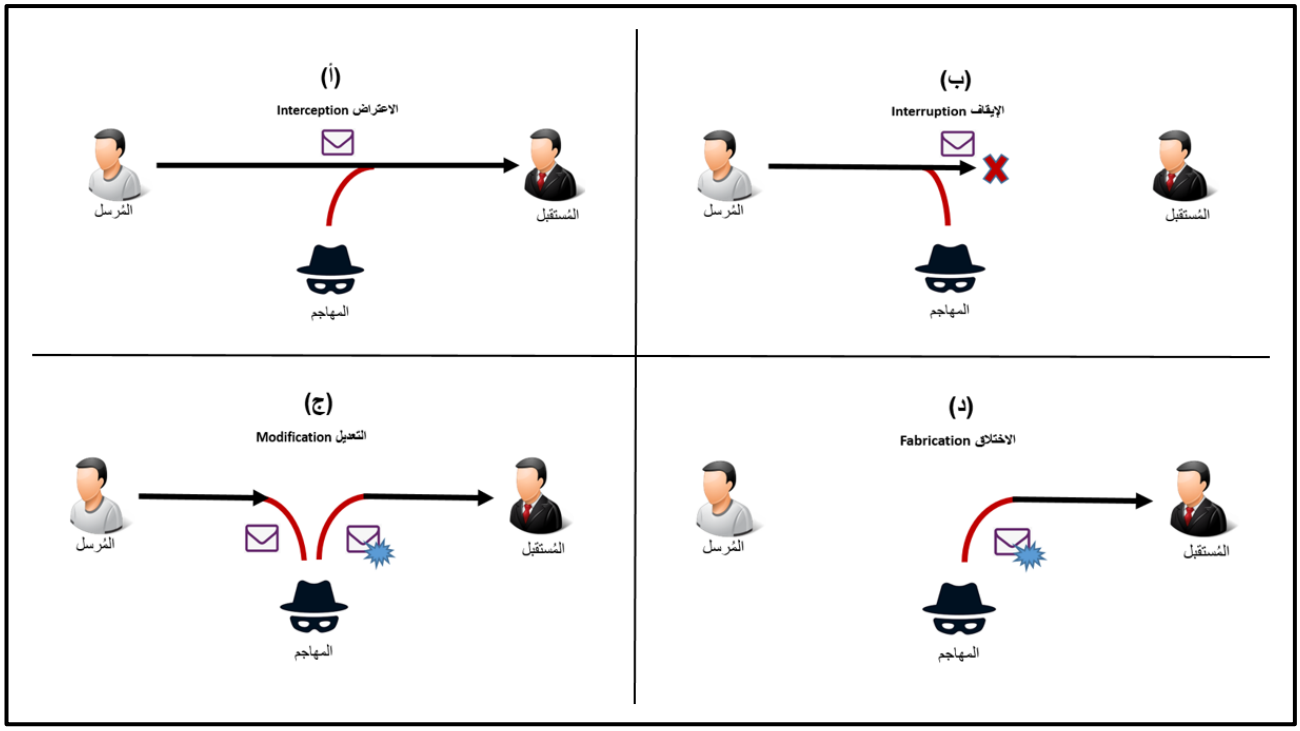
٣. الإيقاف Interruption: ويتم ذلك من خلال تمكن طرف غير مصرح له على قطع الاتصال بين المرسل والمستقبل بهدف إيقاف البيانات من الوصول إلى المستقبل وهو ما يسمى أيضًا برفض الخدمةDenial of service (شكل (٥): *حالات الهجوم*.

٤. -ب).

٥. التعديل Modification: ويتم ذلك من خلال تمكن طرف غير مصرح له على التقاط البيانات المرسلة من المرسل، وتغيير محتواها ومن ثم إعادة إرسالها إلى المستقبل الذي لا يعلم عن حدوث هذا التغيير (شكل (٥): *حالات الهجوم*.

٦. - ج).

٧. الاختلاق Fabrication: ويتم ذلك من خلال تمكن طرف غير مصرح له على انتحال هوية المرسل لإرسال بيانات مفبركة إلى المستقبل شكل (٥): *حالات الهجوم*.



شكل (٥): *حالات الهجوم*.

وبناءً على الحالات العامة للهجمات، فمن الممكن حصر الهجمات المهددة للأمن السيبراني في ١٢ نوعاً أساسياً من أنواع الهجمات كما هو موضح في جدول (١): *الأنواع الأساسية لهجمات المهددة للأمن السيبراني*، حيث تمثل هذه التهديدات خطرًا واضحًا وقائمًا على معلومات المنظمات وأفرادها وأنظمتها. وبناءً على ذلك، يجب على كل منظمة إعطاء الأولوية للتهديدات التي تواجهها بناءً على الوضع الأمني المعين الذي تعمل فيه، واستراتيجيتها التنظيمية فيما يتعلق بالمخاطر، ومستويات التعرض لأصولها، كما سيتم التطرق له لاحقا في هذه الحقيبة. (Michael E. Whitman, Herbert J. Mattord, ٢٠١٨)

جدول (١): الأنواع الأساسية لهجمات المهددة للأمن السيبراني.

نوع الهجمة	مثال توضيحي
التعدي على الملكية الفكرية	القرصنة، التعدي على حقوق النشر
ضعف جودة الخدمة	مشاكل من مزود خدمة الإنترنت (ISP) أو عدم ثبات الطاقة الكهربائية
التجسس	الوصول غير المصرح به و / أو جمع البيانات بطريقة غير شرعية
الظروف البيئية	الحرائق، والفيضانات، والزلازل
الأخطاء البشرية والأعطال	الحوادث، وأخطاء الموظفين
الابتزاز	الكشف عن المعلومات واستغلالها
التخريب	تدمير الأنظمة أو المعلومات
هجمات البرمجيات	الفيروسات والديدان وهجمات رفض الخدمة
أعطال أو أخطاء الأجهزة الفنية	تعطل المعدات والأجهزة
فشل وأخطاء البرمجيات	مشاكل التعليمات البرمجية من الأخطاء والثغرات Bugs
التقادم التقني	التقنيات القديمة أو غير المحدثة
السرقة	المصادرة غير القانونية للأجهزة أو المعلومات

العنصر الخامس: أنواع المهاجمين:

يستخدم مصطلح المهاجم (ممثل التهديد) بشكل عام لوصف الأفراد الذين يشنون هجمات ضد المستخدمين الآخرين وأجهزة الكمبيوتر الخاصة بهم. ينتمي العديد من المهاجمين إلى عصابات منظمة لهذا الغرض بحيث يتخذون من منتديات الويب المظلم (Dark Web) عبر الإنترنت منصة لهم لتنسيق الهجمات وتبادل المعلومات وشراء وبيع البيانات المسروقة وأدوات الهجوم الإلكتروني.

في السابق كانت أهداف المهاجمين تتمثل في إظهار مهاراتهم التقنية في التخطيط للهجمات وتنفيذها. أما اليوم، فقد أصبحت أهداف المهاجمين تتمحور حول تحقيق المكاسب المالية وذلك من خلال استغلال نقاط الضعف التي يمكن أن تدر دخلاً على المهاجم. غالبًا ما تركز الجريمة الإلكترونية بغرض الكسب المادي على فئتين: الأفراد أو الشركات والحكومات. على صعيد الأفراد، يقوم المهاجمون باستغلال البيانات المسروقة أو أرقام بطاقات الائتمان أو معلومات الحسابات المالية الإلكترونية للضحايا ويستخدمونها للاستفادة منها بطرق غير نظامية أو لإرسال ملايين رسائل البريد الإلكتروني المزعجة للترويج للمنتجات المزيفة والبرامج المقرصنة. أما على مستوى الشركات والحكومات. فيحاول المهاجمون الحصول على البيانات المهمة والسرية، مثل الأبحاث أو الخطط العسكرية، حتى يتمكنوا من بيعها بطرق غير مشروعة إلى طرف ثالث مستفيد من هذه المعلومات.

تختلف السمات المميزة لأنواع المهاجمين بشكل كبير. حيث يتميز بعضهم في كونهم يشكلون مجموعات منظمة متطورة للغاية وبموارد ضخمة، بينما البعض الآخر مجرد أفراد يرون فقط ما يمكنهم فعله بمواردهم البسيطة. بالإضافة إلى ذلك، قد يعمل بعض المهاجمين على تنفيذ هجماتهم من داخل المنظمات، بينما البعض الآخر من خارجها مع الأخذ بعين الاعتبار اختلاف الدوافع والمقاصد من تنفيذ الهجمات.

سابقاً، كان مصطلح المهاجم (hacker) يشير إلى الشخص الذي يستخدم مهارات الكمبيوتر المتقدمة لمهاجمة أجهزة الكمبيوتر، كما تم تقديم أنواع مختلفة من هذا المصطلح مثل قراصنة القبعة السوداء وقراصنة القبعة البيضاء. ومع ذلك، فإن هذا التصنيف للمصطلح لا يعكس بدقة الدوافع والأهداف المختلفة للمهاجمين. أما اليوم، فقد تم تصنيف أنواع المهاجمين بطريقة أكثر دقة بحسب الدوافع والأهداف إلى الأنواع التالية: (Ciampa, ٢٠١٨).

- **هواة النصوص البرمجية (Script Kiddies):** ويتم تعريفهم على أنهم أفراد يرغبون بتنفيذ الهجمات الإلكترونية ولكنهم يفتقرون إلى المعرفة بأجهزة الكمبيوتر والشبكات للقيام بذلك. فيقومون بشن هجماتهم عن طريق تنزيل برامج هجوم آلية متاحة مجانًا من مواقع الويب واستخدامها لأداء أنشطتهم الضارة. ولا يمكن الاستهانة بهذا النوع من المهاجمين حيث إن أكثر من ٤٠ بالمائة من الهجمات لا تتطلب أكثر من مهارات تقنية منخفضة أو معدومة ويتم إجراؤها غالبًا بواسطة هواة النصوص البرمجية.
- **الناشطين المخترقون (Hactivists):** ويتم تعريفهم على أنهم مجموعة تحركها أيديولوجية معينة وبالتالي يتم تنفيذ الهجمات الإلكترونية من أجل الترويج لمبادئهم أو معتقداتهم أو الدفاع عنها. يمكن أن تتضمن الهجمات التي تشنها هذه الفئة اقتحام موقع ويب وتغيير ملف محتويات الموقع كوسيلة للإدلاء ببيان أو فكر معين، بالإضافة إلى تنفيذ الهجمات كوسيلة للاحتجاج أو الانتقام.

- **المهاجمون القوميون (Nation State Actor):** بدلاً من استخدام جيش للتقدم عبر ساحة المعركة لضرب العدو، تستخدم الحكومات بشكل متزايد قواتها الخاصة باستخدام المهاجمين الذين ترعاهم الدولة لشن الهجمات الإلكترونية ضد أعدائها من الدول أو الشركات. المهاجمون التابعون للدولة معروفون بكونهم مهاجمون يتمتعون بموارد جيدة ومدربين تدريباً عالياً، وغالبًا ما يشاركون في حملات اقتحام متعددة السنوات تستهدف معلومات اقتصادية أو خاصة أو معلومات أمنية وطنية شديدة الحساسية.
- المهاجمون الداخليون (Insiders): أخطر أنواع التهديدات التي تهدد المنظمات غالباً ما يأتي من موظفيها ومتعهديها وشركائها التجاريين كمصدر للهجمات الإلكترونية. بناءً على أحد الدراسات، تم تحديد أن ٥٨ في المائة من انتهاكات المنظمات نُسبت إلى المهاجمين الداخليين الذين أساءوا استخدام حقهم في الوصول إلى معلومات المنظمة. (Ciampa, ٢٠١٨) بشكل عام، يصعب التعرف على هذه الهجمات لأنها تأتي من داخل المنظمة ولكنها قد تكون أكثر تكلفة من الهجمات من في الخارج. على الرغم من أن بعض الهجمات الداخلية تهدف إلى التخريب من قبل الموظفين الذين تم توبيخهم رسميًا أو تخفيض رتبتهم أو نتيجة رشوة أو ابتزاز، بالإضافة إلى أن معظم المهاجمين الداخليين ينطوون على سرقة البيانات. نظرًا لأن معظم هذه السرقات تحدث في غضون ٣٠ يومًا من استقالة الموظف، حيث يعتقد الجناة أن البيانات مملوكة لهم وليس للمنظمة.
- **المنافسون (Competitors):** حيث تعمل المنظمات على شن الهجمات على المنظمات المنافسة لسرقة المعلومات السرية. مثل سرقة بحث عن منتج جديد أو قائمة بالعملاء الحاليين لاكتساب ميزة تنافسية.

عصف ذهني (١)

الهدف: أن يتعرف المتدرب على أنواع المهاجمين. **الزمن:** ١٠ دقائق

يعمل وليد في أحد الشركات، وفي يوم من الأيام كان يتصفح بريده الإلكتروني من كمبيوتره في المكتب، ثم ذهب ليحضر له كوباً من القهوة وترك بريده الإلكتروني مفتوحاً ولم يسجل خروجه منه لأنه لن يغيب أكثر من خمس دقائق، ولكن زميله خالد في المكتب المجاور استغل فرصة غياب وليد واطلع على رسائل مهمة في البريد الإلكتروني وقام بتغيير كلمة المرور الخاصة بوليد أيضاً. لم يكتشف وليد أن هناك من غير كلمة المرور إلا في اليوم الثاني عندما حاول الدخول في الصباح على بريده الإلكتروني، فقام بالتواصل مع قسم الدعم الفني لتقنية المعلومات ليخبرهم بأنه قد تعرض لهجمة إلكترونية، ولكنهم أفادوه أن تغيير كلمة المرور تم بطريقة نظامية. ولم يستطع وليد إثبات تعرض بريده لوصول غير مشروع، خاصة وأنه لم يكن في المكاتب كاميرات مراقبة.

- ما نوع الهجمة في هذه الحالة؟

.....

.....

.....

.....

- وما نوع المهاجم؟

.....

.....

.....

.....

الإرشادات:

١. يُقسم المتدربين إلى مجموعات، بحيث تتكون كل مجموعة من أربعة متدربين.
٢. دراسة الحالة من قبل المجموعة ومحاولة الإجابة على الأسئلة السابقة.
٣. يعمل المتدرب على مناقشة وجهات النظر مع المتدربين.

الموضوع الثاني: تحليل وإدارة مخاطر تقنية المعلومات

العنصر الأول: أصول تقنية المعلومات:

تُعرف الأصول – كما ذكرنا سابقا-بأنها الموارد أو المعلومات التي نسعى للحفاظ عليها وفي جميع الحالات الأمنية، سواء تلك التي تتعلق بأمن المعلومات أم بأمن المنزل الشخصي، تبدأ تلك الحالات بالأصول التي تُعد ثمينة بما فيه الكفاية بالنسبة لك لبذل جهد خاص للحفاظ عليها من الضرر، وأمن المعلومات لا يختلف عن ذلك. فإذا كانت المعلومات أو الموارد ذات الصلة ثمينة بالنسبة للمنظمة، عندها تحتاج المنظمة لبذل جهد خاص لتأمين المعلومات.

ولكن هناك اختلافان مُهمان بين الأصول التقليدية وأصول المعلومات وهما: تعذر الرؤية، وقابلية التكرار. ففي معظم الحالات الأمنية التقليدية فإنه يمكننا رؤية العناصر التي يتعين علينا حمايتها مثل السيارة والمنزل، فنعمل على قفل السيارة لحمايتها من السرقة وتركيب نظام إنذار في المنزل لمراقبته ومنع اقتحامه، وفي كلتا الحالتين يمكن رؤية الأصول بالعين المجردة والضرر فيها واضح إذا حدث.

بينما الأصول في مجال أمن المعلومات ليست عناصر ملموسة يمكن رؤيتها. فالأصول في مجال أمن المعلومات هي البيانات والمعلومات المخزنة في أجهزة الكمبيوتر والهواتف النقالة وغيرهما من الأجهزة المختلفة. وإذا تمت سرقة البيانات عبر الشبكة فإنه لا يمكن رصد عملية نقل البيانات عبر الكاميرات والأجهزة الأمنية التقليدية. ويعمل المهاجمون عادة من دولة مختلفة على بُعد آلاف الأميال في مأمن من مراقبة أنظمة الأمن التقليدية.

أما فيما يتعلق بقابلية التكرار، فالأصول التقليدية تتواجد في مكان واحد فقط في الوقت الواحد، مثل أن يتم افتقاد السيارة بعد سرقتها مباشرة نظرا لعدم تواجدها، أما بالنسبة للمعلومات فيمكن سرقتها ونسخها من خلال تكرارها وبدون أن يتم ملاحظة ذلك. هذان الاختلافان بين الأصول التقليدية وأصول المعلومات تجعل من أمن المعلومات تحدياً مختلفاً إلى حد كبير عن الأمن التقليدي. فالأساليب الأمنية التقليدية مثل الأقفال والحراس ليست كافية وفعالة في الحفاظ على أمن المعلومات، فلن تقوم الأقفال التقليدية بفعل شيء يُذكر لمنع سرقة البيانات عبر الشبكة. فالأصول التقليدية – كالسيارة مثلا-يمكن استردادها وإعادتها إلى أصحابها، ولكن البيانات المسروقة يمكن نسخها إلى العديد من المواقع، وحتى لو تم تدمير بعض هذه النسخ، فإنه يكاد أن يكون من المستحيل أن نُنكر استفادة المهاجم من البيانات. وبناءً على ذلك، يتعين على ضوابط أمن المعلومات محاولة منع السرقة في المقام الأول، وكشف السرقات ومنعها عند حدوثها من خلال المراقبة المستمرة.

وبناءً على ما سبق، من الممكن تصنيف أصول تقنية المعلومات والمتواجدة في معظم المنظمات بشكل أو بآخر حسب ما يلي: (أغروال، كامبو، بيرس، ٢٠١٨)

- الأصول المعلوماتية: وهي المحتوى الإلكتروني المحفوظ والمملوك من قبل فرد أو منظمة. وفي الغالب تكون هذه الأصول هي أهم الأصول في المنظمة من وجهة نظر أمن المعلومات. وتشمل الأصول المعلوماتية الملفات الفردية كالصور والفيديو والملفات النصية، بالإضافة إلى البيانات الموجودة في قواعد البيانات، ويكون هذا النوع من الأصول مخزناً على أجهزة محلية مملوكة للمنظمة أو على أجهزة يمكن الوصول إليها في السحابة الإلكترونية.
- الأصول الوظيفية: تعد الموارد البشرية كالمبرمجين والمطورين أصولاً تنظيمية مهمة. حيث أن مسألة البحث والتعاقد مع الموظف الذي يمتلك المهارات المطلوبة تأخذ وقتا طويلا، هذا بالإضافة إلى الاستثمار في الموظف بعد التعاقد من خلال التدريب المناسب، مما يترتب عليه تكوين موظفين ذوي خبرة في مجالاتهم وقادرين على بناء شبكات اجتماعية داخل المنظمة. لذلك من مهام المنظمة تحديد الموظفين المميزين والعمل على إدارة المخاطر المتعلقة بهم، كرفع مستوى وعي الإدارة لأهمية هؤلاء الأفراد حتى تقوم بمزيد من الجهود لإشراكهم في العمل. أو من خلال نقل الخبرة بتدريب موظفين آخرين في المنظمة على مهارات متعددة للتصدي لبعض تلك المسؤوليات الهامة في حال فقد الأفراد المتميزين.
- أصول مكونات الحاسب المادية: وتشمل جميع القطع المادية (العتاد) المرتبطة بشكل مباشر أو غير مباشر في دعم أعمال المنظمة.
- الأصول البرمجية: وهي الأدوات البرمجية اللازمة لمعالجة معلومات المنظمة بغرض تحقيق أهداف المنظمة. وتحتاج الأصول البرمجية للحماية من أجل ضمان أن البيانات داخل المنظمة جاهزة للاستخدام لضمان المحافظة على الإنتاجية.

تشتمل هذا النوع من الأصول على الأصول البرمجية العامة لتطبيقات المستخدم مثل (Microsoft Office)، والبرمجيات الخاصة بالمنظمة مثل نظام إدارة الموارد البشرية، وأدوات التطوير، والبرمجيات المتعلقة بالأمن المعلوماتي.

- الأصول القانونية: وهي التنظيمات التعاقدية التي توجه استخدام أصول مكونات الحاسب المادية والأصول البرمجية داخل المنظمة، مثل اتفاقيات الدعم الفني وتراخيص البرمجيات.

حالة دراسية (١)

الهدف: أن يميز المتدرب بين أنواع الأصول المتعلقة بتقنية المعلومات. **الزمن:** ١٠ دقائق

يعمل خالد كمحلل أمني في أحد الجامعات، حيث يركز عمله على تحليل المخاطر المرتبطة بالنظام الخاص بعمادة القبول والتسجيل، حيث يقوم هذا النظام بتخزين معلومات الطلاب الشخصية والأكاديمية مثل الدرجات وبيانات الإرشاد الأكاديمي، بالإضافة إلى جداول المحاضرات. يستطيع الطلاب استعراض معلوماتهم من خلال هذا النظام بواسطة متصفح الإنترنت، ويستطيع كل من المشرفين الأكاديميين أعضاء هيئة التدريس من استعراض المعلومات بنظرة أعمق من خلال واجهة النظام الموزع على أجهزة الحاسب المكتبية، وإصدار التقارير بصيغة PDF لمتابعة أوضاع الطلاب. وبهدف تطوير النظام، يسعى المطور أحمد على إضافة خاصية تسجيل درجات الطلاب في النظام من خلال رفعها على شكل ملفات أكسل، تسهيلاً لعملية رصد الدرجات من قبل أعضاء هيئة التدريس.

الإرشادات:

١. يُقسم المتدربين إلى مجموعات، بحيث تتكون كل مجموعة من أربعة متدربين.
٢. دراسة الحالة من قبل المجموعات والعمل على تصنيف أنواع الأصول بحسب الجدول التالي:

جدول (٢): *تصنيف أنواع الأصول.*

الأصل	نوعه

العنصر الثاني: تحليل مخاطر تقنية المعلومات:

لحماية أصول وموارد تقنية المعلومات، يجب أن نكون قادرين على تحديد التهديدات والمخاطر التي قد تواجهها -وكلما كنا أكثر تحديدًا ودقة، كلما كان ذلك أفضل. تتمثل الخطوة الأولى في إدارة المخاطر في تحديد التهديدات التي قد تواجهها المنظمة. وتُعرف هذه العملية باسم تقييم التهديدات Threat Assessment. وقد عرفنا سابقاً تهديدات أمن المعلومات على أنها عبارة عن أي أحداث أو أفعال من الممكن أن تمثل خطرًا على أصول المعلومات وبالتالي احتمال تعرضها للضرر. وبناءً على ذلك، يتم تعريف عملية تقييم التهديدات على أنها عملية رسمية تتم على مستوى المنظمة لفحص مدى جدية تهديد محتمل على أحد الأصول وتقدير مدى احتمالية تنفيذه وحدوثه، وبشكل عام وهناك ثلاث أنواع أساسية من التهديدات التي يجب تحديدها وفحصها والموضحة فيما يلي: (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- التهديدات البيئية Environmental Threats

التهديدات التي تنشأ من البيئة الطبيعية المحيطة بالمنظمة مثل الفيضانات والأعاصير والحرائق.

- التهديدات البشرية Manmade Threats

التهديدات التي تكون من صنع الانسان مثل السرقة والتخريب.

- التهديدات الداخلية والخارجية Internal vs. External Threats

التهديدات الداخلية يكون مصدرها من داخل المنظمة مثل سرقة البيانات من أحد منسوبي المنظمة، بينما يكون مصدر التهديد الخارجي من خارج المنظمة مثل سرقة البيانات من أحد المخترقين من خارج المنظمة.

كما يمكن تقسيم مجالات التهديدات إلى عدة فئات كما هو موضح في شكل (٣) . (Ciampa, ٢٠١٨)

جدول (٣): *فئات التهديد.*

فئة التهديد	التوضيح	مثال
استراتيجي	التهديد الذي يؤثر على الأهداف الاستراتيجية طويلة المدى للمنظمة	سرقة الملكية الفكرية أو ظهور منافس في نفس المجال
الالتزام والامتثال	التهديدات التي تنشأ من الالتزام (أو عدم الالتزام) باللوائح والمعايير	عدم الالتزام بقوانين وتنظيمات الجهات التشريعية ذات العلاقة
مالية	التهديدات التي تنشأ نتيجة تأثير القرارات المالية	الأزمات المالية العالمية
تشغيلية	التهديدات التي تنشأ نتيجة الأحداث التي تؤثر على الأعمال اليومية للمنظمة	الحرائق أو انقطاع التيار الكهربائي
تقنية	التهديدات التي تنشأ نتيجة الأحداث التي تؤثر على أنظمة تقنية المعلومات	الفيروسات أو هجمات رفض الخدمة DoS
إدارية	التهديدات التي تنشأ نتيجة تغير الإجراءات المتعلقة بإدارة المنظمة	تغير الهيكل التنظيمي أو استقالة أحد صناع القرار في المنظمة

العنصر الثالث: تقييم مخاطر تقنية المعلومات:

يجب على المنظمة بعد أن تقوم بتقييم التهديدات التي من الممكن أن تتعرض لها، أن تقوم في الخطوة التالية بتقييم وحساب المخاطر حتى تستطيع مواجهتها بشكل أفضل. هناك طريقتان لحساب المخاطر. الأولى تعتمد على الحساب النوعي للمخاطر qualitative risks. حيث تستند هذه الطريقة على الحساب بناءً على التخمين القائم على الملاحظة. على سبيل المثال، إذا لوحظ أن قاعدة بيانات العملاء تحتوي على معلومات مهمة ومستهدفة، فسيتم تعيين قيمة أصول عالية لها ويتم تخصيص قيمة عالية للخطورة أيضًا. تحدد المخاطر النوعية عادةً قيمة عددية من (١-١٠) أو حسب تصنيف (مرتفع أو متوسط أو منخفض) يمثل المخاطرة. الطريقة الثانية تعتمد على الحساب الكمي للمخاطر quantitative risks، والذي يعتبر أكثر علمية ودقة، يستند الحساب الكمي للمخاطر على الاعتماد أرقام "ثابتة" مرتبطة بمخاطر تقنية المعلومات المرتبطة ببيانات ونتائج سابقة موجودة في المنظمة مثل عدد مرات فشل نظام معين. يمكن الاعتماد في حساب المخاطر الكمية على عنصرين: احتمالية حدوث الخطر Risk Likelihood وتأثير الخطر حال حدوثه Risk Impact. (Ciampa, ٢٠١٨)

- احتمالية حدوث الخطر Risk Likelihood:

يمكن التعبير عن مدى احتمالية حدوث الخطر بطريقة نوعية أو كمية لتحديد معيار يمثل إمكانية وقوع الخطر. ويمكن الاستعانة **خطأ! لم يتم العثور على مصدر المرجع.** والذي يُظهر مقياس تقييم لاحتمالية حدوث الخطر والمُوصي به من المعهد الوطني للمعايير والتكنولوجيا (The National Institute of Standards and Technology (NIST) .Emmett Dulaney and Chuck Easttom, ٢٠١٨)

جدول (٤): *مقياس احتمالية حدوث المخاطر.*

المقياس النوعي	المقياس الكمي	الوصف
مرتفع جدًا	١٠	يكاد يكون من المؤكد حدوث الخطر.
مرتفع	٨	من المُرجح جداً حدوث الخطر.
متوسط	٥	من المُرجح إلى حد ما حدوث الخطر.

منخفض	٢	من غير المحتمل حدوث الخطر.
منخفض جدا	٠	من المستبعد حدوث الخطر.

فعلى سبيل المثال، من الممكن أن تُقيم أحد الجهات الحكومية في المملكة تقييم (منخفض جداً -٠) لاحتمالية حدوث الزلازل، وتعطي تقييم (مرتفع -٨) لاحتمالية انقطاع التيار الكهربائي.

كما يمكن استخدام العديد من المعايير الكمية للتنبؤ باحتمالية حدوث المخاطر، بما في ذلك:

- متوسط الوقت بين الأعطال(Mean time between failures(MTBF : يحسب MTBF متوسط مقدار الوقت بين أعطال الأجهزة والمكونات، محسوبًا على أنه إجمالي وقت التشغيل الفعلي (لأجهزة ومكونات معينة) مقسومًا على إجمالي عدد مرات التعطل.
- متوسط وقت الإصلاح (Mean time to repair (MTTR: هو متوسط الوقت الذي يُستغرق للتعافي من أحد الأعطال. ويتم حسابه بقسمه إجمالي الوقت المستغرق للإصلاح على إجمالي عدد مرات التعطل.

كمثال على ذلك، لنفترض أن لدينا خادم Server للبيانات يعمل على مدار ٢٤ ساعة وبالتالي فهو يعمل ٧٢٠ ساعة في الشهر (٢٤ ساعة * ٣٠ يوم)، ولكن خلال شهر إبريل تعطل خادم البيانات ٣ مرات، المرة الأولى احتاج إصلاحه وإعادة تشغيله إلى ساعتين، والمرة الثانية تطلب إصلاحه ساعة من الزمن، أما في المرة الثالثة فلم يستغرق إصلاحه إلا نصف ساعة. بناءً على هذه المعطيات يتم حساب قيم MTBF وMTTR كما يلي:

$$MTBF = ٧٢٠/٣ = ٢٤٠ \text{ hours}$$
$$MTTR = (٢+١+٠,٥)/٣ = ١,٢ \text{ hours to repair}$$

- تأثير حدوث الخطر Risk Impact

يمكن تحديد مدى التأثير الذي سيسببه حدوث الخطر من خلال تقييم التكاليف والخسائر المالية الناتجة عن حدوث خطر ما، ومن المهم عند احتساب هذه الخسائر مراعاة جميع التكاليف الممكنة. على سبيل المثال، إذا فشل أحد الخوادم في العمل وتقرر استبداله بخادم جديد، فستشمل التكاليف المبلغ المطلوب لشراء خادم بديل، والأجر بالساعة للشخص الذي سيعمل على استبدال الخادم، وأجور الموظفين الذين لم يتمكنوا من أداء أعمالهم بسبب تعطل الخادم.

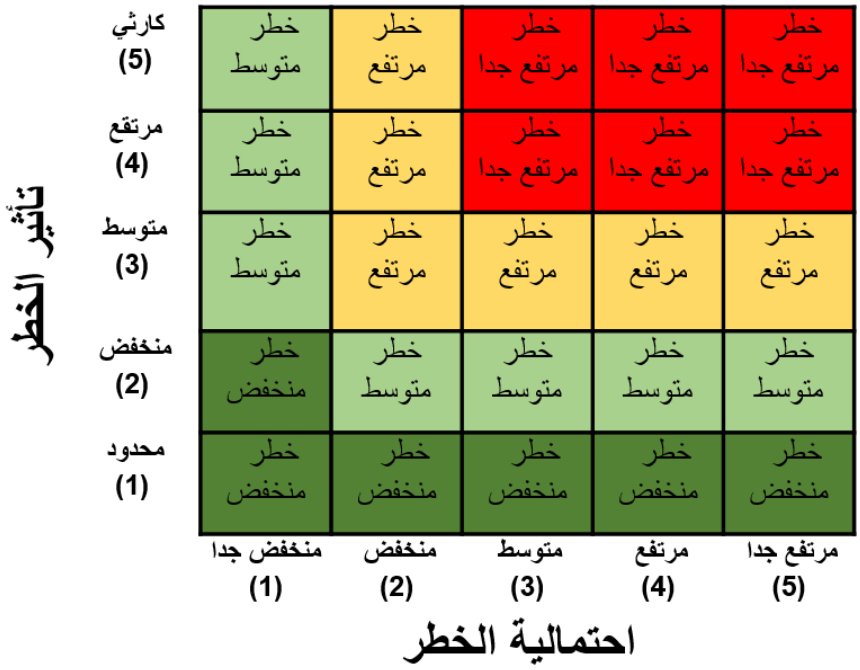
ولحساب التكاليف المالية للمخاطر بصورة كمية، يتم أولا تحديد قيمة الخسارة الفردية Single Loss Expectancy (SLE) وهي تقدير قيمة الخسارة النقدية المتوقعة في كل مرة يحدث فيها الخطر. يتم حساب SLE بضرب قيمة الأصل Asset Value (AV) في عامل التعرض(Exposure Factor (EF ، وهي نسبة قيمة الأصل التي من المحتمل أن يتم تدميرها بسبب خطر معين (معبرًا عنها كنسبة مئوية). وبالتالي تكون صيغة احتساب SLE هي: (Ciampa, ٢٠١٨)

$$SLE = AV * EF$$

فعلى سبيل المثال، لو كان لدينا أجهزة كمبيوتر بقيمة ٥٠,٠٠٠ ريال (AV)، ومن المتوقع تعطل ٧% منها في حال ارتفاع قوة التيار الكهربائي بشكل مفاجئ (EF)، فيمكن احتساب الخسارة المادية في كل مرة يرتفع فيها التيار الكهربائي (SLE) بالشكل التالي:

$$SLE = ٥٠,٠٠٠ * ٠,٠٧ = ٣٥٠٠ \text{ SR}$$

وبناءً على ما سبق، يمكننا الآن تقييم المخاطر بتقدير كل من قيم احتمالية حدوث الخطر Risk Likelihood وتأثير حدوث الخطر Risk Impact، وذلك باستخدام المصفوفة الموضحة في شكل (٦)، حيث يمكننا بناءً عليها تحديد إجراءات إدارة المخاطر ووضع الأولويات المناسبة لها. (Ciampa, ٢٠١٨)



شكل (٦): مصفوفة تقييم المخاطر.

العنصر الرابع: إدارة مخاطر تقنية المعلومات:

بمجرد تحليل وتقييم المخاطر المتوقع احتمالية حدوثها في المنظمة، يكون لدينا أربعة أساليب مختلفة يمكننا الاختيار فيما بينها لإدارة المخاطر والتعامل معها، وهي تجنب مخاطر أو تحويلها أو تقليلها أو قبولها، وفيما يلي إيضاح لكل أسلوب من أساليب إدارة المخاطر: (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- تجنب المخاطر Risk Avoidance:

يتضمن أسلوب تجنب المخاطر على اتخاذ القرار بعدم الانخراط والانشغال في الإجراءات المرتبطة بأحد المخاطر التي تم تحديدها، وذلك من خلال تجنب وقوع الخطر في الأصل. على سبيل المثال، قد تقرر المنظمة أن العديد من المخاطر التقنية قد يكون مصدرها مرفقات البريد الإلكتروني، وبالتالي تتخذ المنظمة القرار بوقف استقبال مرفقات البريد الإلكتروني من خارج المنظمة ومنعها من الدخول إلى الشبكة. كنوع من تجنب المخاطر.

- تحويل المخاطر Risk Transference:

يعتمد أسلوب تحويل المخاطر، على أن يتم تحويل الخطر إلى طرف آخر أو مشاركة عبء الخطر معه. مثل نقل بعض خدمات المنظمة إلى السحابة الإلكترونية، التي تستضيفها جهة خارجية. بهذا القرار تكون المنظمة قد طبقت شكل من أشكال تحويل المخاطر من خلال الاعتماد على مزود خدمة الحوسبة السحابية في وقت التشغيل وكفاءة الأداء وتطبيق تدابير الأمن المعلوماتي.

- تخفيف المخاطر Risk Mitigation:

يتم من خلال أسلوب تخفيف المخاطر اتخاذ أي خطوات أو تدابير وقائية تعمل على تقليل احتمالية حدوث المخاطر. يتضمن هذا الأسلوب مثلاً تثبيت برامج مكافحة الفيروسات، وتثقيف المستخدمين حول التهديدات المحتملة، ومراقبة حركة مرور الشبكة، وإضافة جدار حماية Firewalls، وما إلى ذلك.

- قبول المخاطر: Risk Acceptance

غالبًا ما يكون قبول المخاطر هو الخيار الذي يجب عليك اتخاذه عندما تتجاوز تكلفة تنفيذ أي من الأساليب الأخرى قيمة الضرر الذي قد يحدث إذا تحقق الخطر. للتأهل حقًا كقبول، قبول المخاطر ليس أكثر من الاعتراف بوجود خطر واختيار عدم القيام بأي شيء حيال ذلك. لا يعني ذلك بالضرورة أن المنظمة ستتأثر بالمخاطر، ولكن فقط أن ندرك أن مثل هذا الاحتمال موجود.

حالة دراسية (٢)

الهدف:

الزمن: ١٠ دقائق

- أن يحلل المتدرب المخاطر التي تهدد تقنية المعلومات.
- أن يطبق أساليب إدارة المخاطر التي تهدد تقنية المعلومات.

عُينت كرئيس لقسم تقنية المعلومات في أحد المنظمات الكبرى، وبعد فحصك للبنية التحية التقنية للمنظمة اتضح لك بأن أحد الخوادم الرئيسية أصبح قديماً ويجب استبداله بخادم جديد. الخادم الحالي يعمل بشكل جيد حالياً ولكنك تعتقد بأنه سيكون من الحكمة الترقية قبل حدوث أي شيء كارثي ومفاجئ. ولكن المشكلة تكمن في أن إجراءات شراء خادم جديد تتطلب موافقة مدير إدارتك الذي يركز على توفير أكبر قدر ممكن من الأموال في المنظمة، بالإضافة إلى أنه يأمل في أن يتم النظر في ترقيته قريباً. وبالتالي، فهو لا يريد في الوقت الحالي أن يتم إنفاق أي أموال دون داع. ولكنك تعرف مديرك جيدًا أنع في حال حدوث أي مشكلة تقنية فإنه لن يتردد في إلقاء اللوم عليك من أجل المحفظة على حياته المهنية.

بناءً على ذلك، كيف يتم تطبيق أساليب إدارة المخاطر الأربعة من قبلك كرئيس للقسم على هذه الحالة؟

الإرشادات:

١. يُقسم المتدربين إلى مجموعات، بحيث تتكون كل مجموعة من أربعة متدربين.

٢. دراسة الحالة من قبل المجموعات والعمل على تطبيق أساليب إدارة المخاطر الأربعة بحسب الجدول التالي:

جدول (٥): *أساليب إدارة المخاطر الأربعة.*

الأسلوب	الوصف

اليوم التدريبي الثاني

الموضوع الثالث: الضوابط الأمنية لحماية الأنظمة التقنية.

الموضوع الرابع: إدارة الهوية والوصول.

المخطط التدريبي لليوم الثاني

الجلسة الأولى

- (٨:٠٠:٩:٣٠)
- الضوابط الأمنية لحماية الأنظمة التقنية (١).

استراحة (٩:٣٠:١٠:٠٠)

الجلسة الثانية

- (١٠:٠٠:١١:٣٠)
- الضوابط الأمنية لحماية الأنظمة التقنية (٢).

استراحة (١١:٣٠:١٢:٣٠)

الجلسة الثالثة

- (١٢:٣٠:٢:٠٠)
- إدارة الهوية والوصول.

الموضوع الثالث: الضوابط الأمنية لحماية الأنظمة التقنية

العنصر الأول: البرمجيات الخبيثة:

ماهية البرمجيات الخبيثة:

البرمجيات الخبيثة (Malware) هي برمجيات تدخل لنظام الحاسب بدون علم المستخدم أو إذنه بهدف تنفيذ إجراءات وعمليات ضارة أو مزعجة. مع استمرار تطور الدفاعات الأمنية من أجل صد البرمجيات الخبيثة، استمرت البرمجيات الخبيثة أيضًا في التطور فأصبحت أكثر تعقيدًا. (Ciampa, ٢٠١٨)

تتمثل إحدى طرق تصنيف الأنواع المختلفة البرمجيات الخبيثة من خلال تحديد السمة الأساسية التي يمتلكها البرنامج الخبيث. هذه السمات يمكن حصرها في الانتشار والتداول، والعدوى، والاختفاء، القدرة على التجسس.

وفيما يلي عرض لكل سمة بالتفصيل: (Ciampa, ٢٠١٨)

- **الانتشار والتداول:** بعض البرامج الخبيثة لها القدرة على الانتشار السريع إلى أنظمة أخرى لتؤثر على عدد كبير من المستخدمين. يمكن أن تنتشر البرامج الخبيثة من خلال الشبكة التي تتصل بها جميع الأجهزة، أو من خلال محركات أقراص USB التي يتم مشاركتها بين المستخدمين، أو عن طريق إرسالها كمرفق بالبريد الإلكتروني. كما يمكن أن يتم نشر البرامج الخبيثة تلقائيًا أو قد تتطلب اتخاذ إجراء من قبل المستخدم. تندرج فيروسات الحاسب والديدان تحت هذا النوع.
- **العدوى:** بمجرد وصول هذه الفئة البرمجيات الخبيثة إلى النظام، فإنها تعمل عل إصابته ودمج نفسها فيه. فقد يتم تشغيل البرمجية الخبيثة مرة واحدة فقط، أو قد تظل على النظام ويتم تشغيلها لعدد لا نهائي من المرات بحيث ترفق ببرنامج حميد أو قد تعمل كبرنامج قائم بحد ذاته. تعتبر أحصنة طروادة وبرامج الفدية من أشهر برمجيات هذه الفئة.
- **الاختفاء:** بعض البرامج الخبيثة لها سمة أساسية في إخفاء نفسها وبالتالي تجنب اكتشافها من قبل برامج مكافحة البرمجيات الخبيثة. تحاول بعض البرمجيات الخبيثة تجنب اكتشافها عن طريق تغيير نفسها، أو من تضمين نفسها في العمليات الحالية أو من خلال تعديل نظام التشغيل الأساسي على جهاز المستخدم. من أشهر البرمجيات في هذا المجال برامج التحكم الخفي في الحاسب (RootKit).
- **القدرة على التجسس أو التدمير:** تتمثل قدرات هذه الفئة في جمع البيانات وحذفها أو تعديل إعدادات أمان النظام أو السيطرة عليه شن الهجمات من خلاله. يندرج تحت هذه الفئة برامج التجسس والإعلانات والقنابل المنطقية والأبواب الخلفية والبوت نت.

أنواع البرمجيات الخبيثة:

بناءً على التصنيف السابق لسمات البرمجيات الخبيثة، نستعرض أشهر الأنواع منها فيما يلي:

الفيروسات Computer Viruses:

بدأ ظهور الفيروسات في السبعينات من القرن الميلادي الماضي، وكانت بداياته بسيطة جدًا، ولم تكن على مستوى الخطورة التدميرية الحاصلة في عصرنا الحاضر. تعتبر الفيروسات هي أكبر فئات البرامج الضارة من ناحية عدد الأشكال المعروفة، ومن ناحية أثرها على بيئة الحاسب. ولذلك فإن كلمة "فيروسات" تميل لأن تكون مرادفًا في ذهن العامة لكل أنواع البرامج غير السوية أو الشرعية.

وسبب تسمية فيروسات الحاسب الآلي بهذا الاسم هو تشابهها الكبير مع الفيروسات التي تصيب الإنسان. فإن فيروس الحاسب الآلي بعد أن يصيب الجهاز – من خلال انتقاله من جهاز لآخر-يدخل في مرحلة الحضانة أو الركود، ثم يبدأ بعد ذلك بالانتشار من خلال استنساخ نفسه إلى أن تظهر أعراضه على الجهاز، ثم يظهر بعد ذلك الدمار الذي يسببه، سواء كان الدمار كبيرًا أو بسيطاً. فيروس الحاسب الآلي هو برنامج يتم إعداده لينسخ نفسه وينتشر ذاتيًا دون علم وتعاون مع المالك أو المستخدم للجهاز ويقوم بتعديل البرامج الأخرى لكي تحتوي على نسخة معدلة منه. وعليه يمكن تعريف الفيروسات بصورة عامة بأنها البرامج التي تقوم بإقحام نفسها بنفسها في مادة أخرى قد تكون برنامجًا أو قرصًا أو وثيقة أو رسالة بريد إلكتروني أو نظام حاسب آلي أو أي صيغة معلوماتية. ولدى كثير من الناس انطباع بأن أي شيء لا يسير على ما يرام في الحاسب الآلي يكون: سببه فيروس. ابتداءً من فشل القرص الصلب وحتى أخطاء الاستخدام. والحقيقة أنه ليس بالضرورة أن ينتج عن الفيروس ضررًا ما. فقد يتم بناء الفيروسات لكي تكون وسيلة نقش إلكتروني لعلامة تخلد أسم مصممه في العالم. وفي بعض الأحيان يتم عرض اسم مصمم الفيروس في أي مناسبة مع عنوانه ورقم هاتفه، واسم الشركة التي ينتمي إليها، من أجل الشهرة فقط بدون إلحاق أي ضرر. (David Kim, Michael G. Solomon, ٢٠١٤)

لا تحدث فيروسات الحاسب الآلي أو تنتج طبيعية، وإنما هي برامج يكتبها مبرمجون. وكذلك فهي لا تظهر من خلال بعض التطورات الإلكترونية فقط، وإنما تكتب بصورة متعمدة عن طريق أناس متخصصين. وتبقى الفيروسات مختبئة داخل البرنامج المصاب؛ لتبدأ بالعمل والتكاثر والانتشار. أي إنها لا تبدأ بعملها حتى تتم استثارتها من قبل المستخدم. هناك عدة خصائص لفيروسات الحاسب الآلي تميزها عن غيرها من البرامج الضارة، وتساعدها على الانتشار وإصابة أجهزة الحاسب الآلي الأخرى دون علم مستخدميها، وهي:

- **التخفي:** ويعني القدرة على الارتباط ببرامج أو ملفات أخرى تبدو سليمة ومألوفة للمستخدم، بحيث يلحق الفيروس نفسه بالملف المصاب خفية ليصبح جزأً منه. ومن أشهر طرق تخفي الفيروسات ما يلي :
  - التخفي في مرفقات البريد الإلكتروني.
  - التخفي في الملفات التي يتم تحميلها من مواقع الإنترنت، خاصة تلك التي تقوم بتشغيل ملفات الصوتيات والفيديو وتبادلها.
  - التخفي وراء الروابط والأوامر الموجودة في صفحات الإنترنت والبريد الإلكتروني.
  - التخفي وراء روابط وملفات الإعلانات والبريد الدعائي.
  - التخفي مع البرامج المنسوخة بشكل غير قانوني.

- **التضاعف:** ويعني ذلك أن ينسخ الفيروس نفسه عدة نسخ تصل في بعض الأحيان إلى ملايين النسخ، بمعنى أنه يتكاثر ليصيب أكبر قدر ممكن من الملفات والبرامج داخل نفس جهاز الحاسب الآلي أو داخل الأجهزة الأخرى المرتبطة به. وتبدأ عملية التضاعف عندما يتم تحميل برنامج الفيروس إلى ذاكرة الحاسب الآلي ويقوم المعالج بتنفيذه .
- **الانتشار:** ويعني انتقال الفيروس من جهاز إلى آخر عبر شبكات الحاسب الآلي أو وسائط التخزين المختلفة. ومعنى ذلك أن لدى الفيروس القدرة على نقل نفسه عند استثارته، كتشغيل أمر النسخ، أو عند اكتشاف اتصال الحاسب الآلي المصاب بحاسب آلي آخر. ومن أشهر طرق انتشار الفيروسات ما يلي:
  - تحميل ملفات مصابة من مواقع شبكة الإنترنت أو زيارة مواقع تقوم بنشر الفيروسات بشكل تلقائي.
  - فتح مرفقات بريد إلكتروني مصابة.
  - أن يقوم المستخدم بنسخ ملفات مصابة دون علمه، وتخزينها على وسائط تخزين خارجية تنتشر معها، أو يقوم بإرسالها عبر الشبكة "كاستخدام المجلدات المشتركة"، فتنتشر عبرها.
  - أن يقوم الفيروس بنسخ نفسه، ثم إرفاق تلك النسخة مع أي ملف آخر عند استثارته.

وبناءً على ذلك يمكن استنتاج بأنه طريقة عمل الفيروس تعتمد على أنه في كل مرة يتم فيها تشغيل البرنامج المصاب أو فتح ملف البيانات -إما عن طريق المستخدم أو نظام تشغيل الكمبيوتر -يقوم الفيروس بإجراءين. أولاً، يقوم بتحميل الرمز البرمجي الخاص به code (والذي يطلق عليه اسم توقيع الفيروس) لتنفيذ النشاط الضار. مع الإشارة إلى أن الفيروسات في السابق لا يتعدى نشاطها أكثر من عرض رسالة مزعجة على شاشة الكمبيوتر، إلا أن الفيروسات الحديثة تعد أكثر ضررًا. حيث يمكنها إتلاف الملفات أو حذفها، ومنع البرامج من التشغيل، أو سرقة البيانات لإرسالها إلى كمبيوتر آخر، والتسبب في تعطل الكمبيوتر بشكل متكرر، وحتى إيقاف تشغيل إعدادات أمان الكمبيوتر. ثانياً، يعمل الفيروس على إعادة إنتاج نفسه عن طريق إدخال رمزه في ملف آخر على نفس الكمبيوتر. يمكن للفيروس أن ينسخ نفسه فقط على الكمبيوتر المضيف الذي يوجد عليه؛ ولا يمكن أن ينتشر تلقائيًا إلى كمبيوتر آخر بمفرده، حيث يعتمد على تصرفات المستخدمين للانتشار إلى أجهزة الكمبيوتر الأخرى. نظرًا لارتباط الفيروسات بالملفات، فإنها تنتشر عندما يقوم المستخدم بنقل هذه الملفات إلى أجهزة أخرى. على سبيل المثال، قد يرسل المستخدم ملفًا مصابًا كمرفق بريد إلكتروني أو ينسخ ملفًا مصابًا إلى محرك أقراص USB ويعطي محرك الأقراص إلى مستخدم آخر. بمجرد وصول الفيروس إلى جهاز كمبيوتر جديد، يبدأ في إصابته. وبالتالي، يجب أن يكون للفيروس ناقلان: ملف يرفق به ومستخدم لنقله إلى أجهزة كمبيوتر أخرى. (Ciampa, ٢٠١٨)

يوجد أنواع كثيرة جدًا من الفيروسات، ولكن ما يهمنا هنا هو الأنواع "أو المجموعات" الرئيسة الأكثر انتشارًا، التي يشكل كل نوع منها مجموعة من الفيروسات لها نفس البنية وتقوم بمهام متشابهة إلى حدٍ كبير، وهذه الأنواع هي:

- فيروسات قطاع بدء التشغيل (Boot sector viruses): يوجد لكل نظام تشغيل قطاع في القرص الصلب، مخصص لبدء عملية التشغيل (الإقلاع). وعادة ما يكون هذا القطاع هو القطاع الأول(Track ٠) ، وعند وجود أي خلل فيه فإن الحاسب الآلي لن يستطيع البدء بالتشغيل. وهذا النوع من الفيروسات تصيب قطاع بدء التشغيل في القرص الصلب، وتكمن خطورة هذا النوع من الفيروسات في إصابتها لمكان مهم جدًا يتم من خلاله توجيه الجهاز لتنفيذ البرامج التي يتم من خلالها استكمال تجهيز جهاز الحاسب الآلي للعمل. وبدلًا من ذلك يقوم الفيروس بتوجيه الحاسب الآلي لتنفيذ الكود الخاص بالفيروس، وبالتالي يفشل الجهاز في عملية الإقلاع ولا يمكنه العمل .

- فيروسات الملفات(File infecting viruses) : هي الفيروسات التي تصيب الملفات بشتى أنواعها فيمكن أن تصيب ملفات نظام التشغيل كملف (command.com) في نظام الويندوز أو أي ملف آخر. وعادة ما ينتج عن هذه الفيروسات زيادة في أحجام الملفات.
- الفيروسات الجزئية الكبيرة الماكرو (Macro viruses): الماكرو عبارة عن سلسلة من الإرشادات التي يمكن تجميعها معًا كأمر واحد. غالبًا ما يتم استخدام وحدات الماكرو لأتمته مجموعة معقدة أو سلسلة متكررة من المهام. يمكن كتابة وحدات الماكرو باستخدام لغة برمجة نصية للماكرو، مثل Visual Basic for Applications (VBA)، ويتم تخزينها في مستند المستخدم (مثل ورقة عمل Excel .xlsx أو ملف وورد Word .docx). وبمجرد فتح المستند، يتم تنفيذ تعليمات الماكرو، سواء كانت هذه التعليمات حميدة أو فيروسات ماكرو (Ciampa, ٢٠١٨). وعلى الرغم من أن الفيروسات الجزئية الكبيرة تصيب ملفات البيانات، إلا أنها عمومًا لا تعد من فيروسات الملفات. والسبب في ذلك أن فيروسات الملفات قد تصيب البرامج وملفات البيانات، بينما لا تصيب فيروسات الجزئية الكبيرة إلا ملفات البيانات فقط.
- فيروسات البريد الإلكتروني: وهي الفيروسات التي تنتقل بواسطة البريد الإلكتروني. فبإضافة بعض الوظائف (عن طريق الفيروس) لبرنامج مقدم خدمة البريد الإلكتروني مثل أوتلوك (Outlook) أصبح للفيروس إمكانية الانتشار عبر العالم خلال ساعات فقط.

<u>ديدان الحاسب الآليComputer Worms :</u>

دودة الحاسب الآلي (Computer Worm) هي عبارة عن برنامج مستقل بذاته، وله ملف خاص به. فالدودة تعتبر برنامجاً تطبيقياً متكاملاً يمكن أن يعمل لوحده، ولا يحتاج لأن يضيف نفسه لملف آخر، على خلاف الفيروسات. ويمكن للدودة أيضاً أن تعمل بمفردها وتحمّل نفسها في ذاكرة الحاسب. وتبدأ بالعمل بشكل آلي.

ومن الفوارق الأصلية، هي أن الديدان تستخدم الشبكات وروابط الاتصالات كوسيلة أساسية لانتشارها، وهي خلافاً للفيروسات لا تلتحم مباشره بالملفات القابلة للتنفيذ. وتصيب الديدان أجهزه الحاسب الآلي المرتبطة بشبكات الحاسب الآلي المصابة بدون أي تدخل من المستخدم أو قيامه باستثارتها كفتح ملف معين أو تشغيل برنامج، كما هي الحال في الفيروسات. فقد تنتقل الديدان إلى الجهاز بمجرد تصفح بعض مواقع الإنترنت، أو بمجرد فتح بريد إلكتروني (إذا لم يكون الجهاز محمياً ببرنامج حماية محدّث). وأصل مصطلح برنامج "دودة" يتلاءم فنياً مع طرق انتشار الديدان في الوقت الحاضر. فنجد أن برنامج الدودة يتكون من أجزاء (رأس وجسم كما في الدودة الطبيعية) تعمل في أجهزة حاسب متفرقة، تتواصل فيما بينهما عبر الشبكة، فيمكن أن تجد رأس البرنامج في جهاز، وذيله في جهاز آخر بعيد.

لم تضع دودة الإنترنت يونيكس موريس (UNIX/Morris) الإنترنت عامة والبريد الإلكتروني خاصة في حالة شبه توقف فقط، بل لقد استطاعت تشغيل الإصدارات الحديثة لنظام يونيكس وترويجها في منصات أقراص صلبة محددة. وخلال هذه العاصفة البريدية، تأثرت الكثير من الأجهزة بالفصل بين البريد الإلكتروني وقائمة توزيع البريد، وتم فقد بعض رسائل البريد نهائياً. ومعظم البريد تم تأخيره، وفي بعض الأحوال تم توجيهه نحو طرق أقل كفاءة؛ مما تسبب في فقده أو تأخيره. وفي الحالات الأخرى التي تأثرت في الأجهزة الرئيسية بالمشكلة كانت ببساطة أبطأ في نقل البريد. وكذلك توقفت في بعض الأجهزة الأخرى برامج نقل البريد، وخرجت من الخدمة مع تأخير ملحوظ في إرسال البريد. ومن المفارقة في هذه العاصفة، أن البريد الإلكتروني يشكل الوسيلة الأساسية التي

يحاول مختلف الأطراف التعامل مع المشكلة من خلاله، وكانوا يحاولون استخدامه للتواصل فيما بينهم؛ مما زاد الأمر سوءاً. وعند دخول رأس الدودة إلى النظام، يتم تغذيته بالبرنامج الرئيسي، (الجسم)، من الموقع الذي تمت إصابته مسبقاً. وتم استخدام برنامجين (رأس وجسم)، أحدهما في الموقع المصاب، والآخر في الموقع المستضيف (الجديد). وإذا لم يستطع أي من البرنامجين العمل، تزيل الدودة نفسها بنفسها، وإن كان المستضيف الجديد غير مناسب، فإن الدودة ستبحث عن مستضيفين آخرين وتوصيلات أخرى (القحطاني، ٢٠١٥).

من أهم خصائص الديدان هي قدرتها على الانتشار والتكاثر عبر الاتصال بشبكات الحاسب الآلي. ومن أهم الطرق التي تنتشر بها الديدان ما يلي:

- مرفقات البريد الإلكتروني.
- التحميل التلقائي عند زيارة بعض مواقع الإنترنت التي من خلالها تنتشر الديدان، أو عند استخدام أحد الارتباطات داخل البريد الإلكتروني.
- التسلل عبر الثغرات الأمنية في أنظمة التشغيل أو برامج الحماية.

في السابق، كانت الديدان مصممة ببساطة لتنتشر بسرعة مما يتسبب إبطاء الشبكات واستهلاك مواردها-كونها وسيلة انتشارها الأساسية-ولكنها لا تعمل على افساد الأنظمة التي أصابتها. ولكن اليوم، أصبحت الديدان قادرة على أن تترك وراءها كم من الأنظمة المصابة وبأضرار جسيمة. وبناءً على ذلك، لا تقل أضرار الديدان عن الفيروسات من ناحية الاتلاف والتدمير، أو فقد البيانات التي تسببها. ومن أهم أضرار الديدان الحديثة ما يلي:

- تتيح للمهاجم أن يستخدم الحاسب الآلي المصاب لمهاجمة أجهزة أخرى، أو مواقع الإنترنت، أو إرسال بريد إلكتروني، أو تحميل برامج ضارة إليه.
- يمكن من خلالها فتح باب خلفي (Back Door) في الجهاز المصاب، حيث يمكن التحكم به من خلال ذلك الباب.
- يمكن للديدان أن تنسخ نفسها، وترسل نسخة إلى كل بريد إلكتروني في عناوين البريد المخزنة في جهاز الحاسب الآلي المصاب.

أحصنة طروادة: Trojan Horses

وفقا للأسطورة القديمة، فاز الإغريق بحرب طروادة عن طريق إخفاء الجنود في حصان خشبي كبير مجوف قدم كهدية لمدينة طروادة. فحينما أُدخِل الحصان إلى المدينة المحصنة، زحف الجنود من الحصان أثناء الليل وهاجموا المدافعين المطمئنين، ومن هنا جاءت التسمية. حصان طروادة الحاسوبي (Trojan Horses) هو برنامج قد أعلن بأنه يقوم بأداء نشاط معين لكنه في الحقيقة يقوم بنشاط آخر، وفي بعض الأحيان يقوم بأداء كلًا من النشاطين المعلن عنه والخبيث. على سبيل المثال، قد يقوم مستخدم بتنزيل برنامج قد أعلن بأنه تقويم مجاني للتاريخ الهجري. لكن عندما تم تشغيله فإنه بالإضافة لتثبيت التقويم الهجري قام بمسح الجهاز باحثًا عن أرقام بطاقات الائتمان وكلمات المرور، فيرتبط عن طريق الشبكة بنظام عن بعد ليرسل له تلك المعلومات. إذاً فبرامج حصان طروادة هي برامج قابلة للتنفيذ وتحوي عادة على أوامر برمجية خبيثة خفية.

برامج الفدية Ransomware:

تعد برنامج الفدية (Ransomware) أحد أسرع أنواع البرامج الضارة انتشارًا، وتعمل على أساس منع جهاز المستخدم المصاب بها من العمل بشكل صحيح وكامل حتى يتم دفع رسوم. تقوم برامج الفدية بتضمين نفسها على الكمبيوتر بطريقة لا يمكن تجاوزها، وحتى إعادة التشغيل تؤدي إلى تشغيل برنامج الفدية مرة أخرى.

غالباً ما تعرض برنامج الفدية على شاشة المستخدم رسائل تتظاهر بأنها من جهة رسمية وموثوقة، وتقوم بادعاء سبب نظامي لحظر جهاز الكمبيوتر الخاص بالمستخدم. مثل أن يزعم برنامج الفدية أنه تابع لمنظمة قانونية أو تنفيذية وأنه بناءً على قيام المستخدم بإجراء سلوك غير قانوني من خلال جهاز ه فإنه يجب عليه على الفور دفع غرامة عبر الإنترنت عن طريق إدخال رقم بطاقة الائتمان الخاصة به.

كما أن هناك نوع آخر من هذا النوع من برامج الفدية يتظاهر بأنه تابع لأحد شركات تطوير البرمجيات ويعرض تحذيرًا وهميًا بانتهاء صلاحية ترخيص برنامج ما أو أن هناك مشكلة في الكمبيوتر مثل فشل وشيك في محرك القرص الصلب أو الإصابة بالبرمجيات الخبيثة. هذا النوع من برامج الفدية يخبر المستخدمين أنه يجب عليهم تجديد تراخيصهم على الفور أو شراء برامج إضافية عبر الإنترنت لإصلاح مشكلة غير موجودة.

ولكن مع انتشار برامج الفدية، توقف المهاجمون الان عن التظاهر بأن برنامج الفدية تابع لجهة رسمية أخرى. وبدلاً من ذلك، يقومون ببساطة بحظر جهاز الكمبيوتر الخاص بالمستخدم ويطالبون بدفع رسوم مقابل رفع الحظر، ويقوم المهاجمون بتحديد السعر الذي يرونه مناسباً للدفع لإلغاء حظر جهاز الكمبيوتر، حيث يجب أن يكون المبلغ صغيرًا بما يكفي بحيث يستطيع معظم الضحايا الدفع -على مضض-مقابل إلغاء حظر أجهزتهم، ولكن هذا المبلغ سوف يقدر بثروة لو حصل المهاجمين على المبالغ من آلاف الضحايا.

لا تزال برامج الفدية تشكل تهديدًا خطيرًا للمستخدمين حيث قدرت أحد التقارير الحديثة أنه تم دفع مليار دولار كفدية في عام واحد، ومع ذلك فإن ٤٢ في المئة فقط من أولئك الذين دفعوا الفدية تمكنوا بعد ذلك من استرداد بياناتهم.
(Ciampa, ٢٠١٨)

برامج التحكم الخفي في الحاسب Rootkit:

برامج التحكم الخفي في الحاسب (Rootkit) هي مجموعة من الأدوات البرمجية التي يستخدمها المهاجم لاختراق نظام الحاسب، أو للحصول على امتيازات خاصة لأداء وظائف غير مصرح بها، ومن ثم إخفاء كل آثار وجودها. تعمل برامج التحكم الخفي في الحاسب عن طريق استبدال أوامر نظام التشغيل بإصدار محدث من الأوامر والذي صمم خصيصًا لتجاهل النشاطات الخبيثة وبالتالي عدم القدرة على كشفها. على سبيل المثال، مضاد الفيروسات في جهاز الحاسوب مكلف بفحص ملفات في مجلدات معينة، وهذا التكليف عادة ما يكون بأمر من نظام التشغيل، هنا تعمل برامج التحكم الخفي في الحاسب على تحديث تلك الأوامر بحيث تجعل مضاد الفيروسات يتجاهل المجلدات التي تحوي ملفات خبيثة. فمضاد الفيروسات يأخذ بأوامر نظام التشغيل على أنها أوامر تعزز أمن الحاسوب فلا يستطيع التفرقة بين الأوامر المعززة لأمن الحاسوب والعكس. وهذا ما قد نتج عنه مشكلة رئيسة، وهي أن المستخدمين لم يعودوا يثقوا بأجهزتهم وأنظمتها. أما عن تحديد واكتشاف وجود برامج التحكم الخفي في الحاسب فهو أمر صعب. مع أن هنالك برامج متاحة للتحقق من وجود تلك التقنية

في الحاسب، لكن ومع ذلك بعض من البرامج التي تستخدم تلك التقنية تستطيع إخفاء نفسها عن البرامج التي تسعى لكشفها أيضًا.

برامج التجسس: Spyware

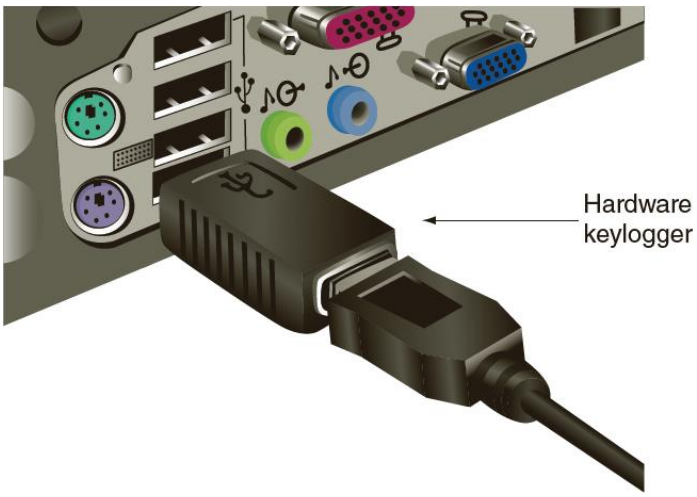
تعرف برامج التجسس (Spyware) على أنها برامج تتبع نشرها وتثبيتها على الجهاز دون موافقة المستخدم أو تحكمه، وتعمل على مراقبة المستخدمين سراً عن طريق جمع المعلومات دون موافقتهم باستخدام موارد الكمبيوتر، بما في ذلك البرامج المثبتة بالفعل على الكمبيوتر، لجمع ونشر المعلومات الشخصية أو الحساسة، وعادة ما يتم تضمين برامج التجسس في شكل مكونات مجانية خفية، أو برامج مشاركة يمكن تنزيلها من شبكة الإنترنت. وبمجرد تثبيت برنامج التجسس يبدأ بمراقبة حركة المستخدم، وينقل المعلومات من وراء الكواليس لجهة أخرى.

أحد أنواع برامج التجسس هو برنامج راصد لوحة المفاتيح(Keylogger) الذي يلتقط بصمت كل ضغطة مفتاح يكتبها المستخدم على لوحة مفاتيح الكمبيوتر ويخزنها. يمكن للمهاجم بعد ذلك البحث في النص الملتقط عن أي معلومات مفيدة مثل كلمات المرور أو أرقام بطاقات الائتمان أو المعلومات الشخصية. يمكن أن يكون برنامج keylogger برنامجًا أو جهازًا صغيرًا. الأكثر شيوعًا هي برامج keyloggers - شكل (٧): *واجهة أحد برامج Keylogger*.

-وهي برامج مثبتة على الكمبيوتر تلتقط المعلومات الحساسة بصمت وبدون علم المستخدم. تتخطى برامج الـ Keyloggers اليوم مجرد التقاط نقرات المستخدم على لوحة المفاتيح. يمكن لهذه البرامج أيضًا أن تجعل لقطات الشاشة لكل ما هو موجود على شاشة المستخدم وتشغيل كاميرا الويب الخاصة بالكمبيوتر بطريقة سرية لتسجيل صور المستخدم.

شكل (٧): *واجهة أحد برامج Keylogger*.

تتمثل مزايا برامج تسجيل المفاتيح في أنها لا تتطلب الوصول المادي إلى كمبيوتر المستخدم ويمكن غالبًا تثبيتها عن بُعد من خلال أحصنة طروادة أو بواسطة فيروس، ويمكنها بشكل روتيني إرسال المعلومات التي تم التقاطها إلى المهاجم من خلال اتصال الكمبيوتر بالإنترنت. فيما يتعلق بأجهزة راصد لوحة المفاتيح فهي عبارة عن أجهزة يتم توصيلها بين السلك الخاص بلوحة مفاتيح الكمبيوتر ومنفذ USB، كما هو موضح في شكل (٨): *واجهة أحد برامج Keylogger*.. ويصعب اكتشاف وجود هذا الجهاز نظرًا لأن يشبه قابس لوحة المفاتيح الأصلي، وغالبًا ما يكون منفذ USB الخاص بلوحة مفاتيح الكمبيوتر على الجزء الخلفي من الكمبيوتر. بالإضافة إلى ذلك، فإن الجهاز بعيد عن متناول برامج مكافحة البرامج الضارة بالكمبيوتر وبالتالي لا يصدر أي إنذارات. ولكن نظرًا لأن المهاجم الذي قام بتثبيت جهاز keylogger يجب أن يعود لاحقًا للحصول عليه أجل الوصول إلى المعلومات التي جمعها، فنادرًا ما يتم استخدام أجهزة تسجيل المفاتيح في الأجهزة اليوم. (Ciampa, ٢٠١٨)



شكل (٨): واجهة أحد برامج Keylogger.

برمجيات الإعلانات Adware:

برمجيات الإعلانات (Adware) هي برمجيات من شأنها أن توفر محتوى الإعلان بطريقة غير متوقعة وغير مرغوب فيه من قبل المستخدم. وعادةً ما تعرض تلك البرمجيات لافتات الإعلانات، والإعلانات المنبثقة، أو تفتح نوافذ متصفح ويب جديدة في حين اتصال المستخدم بالإنترنت. وغالبًا ما يقاوم المستخدمين برمجيات الإعلانات للأسباب التالية:

- برمجيات الإعلانات قد تعرض محتوى غير المرغوب فيه، مثل مواقع القمار أو المحتوى الإباحي.
- تكرار الإعلانات المنبثقة قد يعيق إنتاجية المستخدم.
- الإعلانات المنبثقة يمكن لها أن تبطئ من أداء الجهاز وقدد تتسبب بخسارة أو تلف البيانات أيضاً .
- يمكن للإعلانات الغير المرغوب فيها أن تكون مصدرًا للإزعاج.

ويمكن أن تشكل برمجيات الإعلانات خطراً أمنياً أيضاً. فالعديد من تلك البرمجيات تعمل على تتبع نشاطات المستخدم. فتقوم بمراقبة وتعقب جميع نشاطات المستخدم على الإنترنت ومن ثم تقوم بإرسال سجل من هذه النشاطات لطرف ثالث دون إذن المستخدم أو حتى معرفته. على سبيل المثال، يمكن لبرمجيات الإعلانات تتبع مستخدم يقوم بزيارة مواقع لبيع السيارات على الإنترنت ومن ثم يبحث عن نوع محدد منها. عند إذن ستصنف تلك البرمجيات هذا المستخدم على أنه مستخدم يرغب في شراء سيارة جديدة، فتجمع معلوماته وتبيعها لشركات الإعلان عن سيارات للبيع.

كما أنه نظرًا للزيادة المطردة في حجم الإعلانات على العديد من مواقع الويب، فقد أدى ذلك إلى رد مقاومة عنيفة لها من قبل المستخدمين. حيث يزداد يوما بعد يوم عدد المستخدمين الذين يقومون بتثبيت برامج حظر الإعلانات في متصفحات الويب الخاصة بهم لمنع الإعلانات من الظهور. حيث نما حظر الإعلانات بنسبة ٤١ في المائة في جميع أنحاء العالم في عام واحد (١٩٨ مليون مستخدم)، وتشير التقديرات إلى أن حظر الإعلانات يكلف ناشري مواقع الويب ما يقرب من ٢٢ مليار دولار كل عام. ولمكافحة ذلك، يقوم المسوقون عبر الويب بشكل متزايد بإضافة خدمات تجبر المستخدم على الدفع لمشاهدة المحتوى بدلاً من مشاهدة الإعلانات، وعرض تنبيهات ودية للمستخدمين حول الغرض من الإعلانات (أن الإعلانات هي الثمن الذي يجب دفعه مقابل المحتوى المجاني)، أو يلاحظ أنه سيتم حظر المحتوى إذا اكتشف الموقع استخدام أدوات منع الإعلانات. (Ciampa, ٢٠١٨)

القنابل المنطقية Logical Bombs:

القنبلة المنطقية (Logical Bomb) عبارة عن برنامج أو جزء من برنامج يظل خامدًا حتى يتم تشغيله بواسطة حدث منطقي محدد، كوصول التقويم في جهاز الحاسوب لتاريخ محدد مسبقًا، أو عند انخفاض المستوى الوظيفي لموظف ما تحت رتبة معينة. في حين تم تشغيل البرنامج فسيقوم بعدة نشاطات خبيثة. على سبيل المثال، القنبلة المنطقية قد تكون مزروعة في نظام الرواتب للشركة من قبل موظف، ويكون قد صممها بحيث تبدأ نشاطاتها بعد ثلاثة أشهر من إزالة اسمه من القائمة (وذلك يعني أنه استقال أو قامت الشركة بطرده) .

الباب الخلفي Backdoor :

يُمِّكن الباب الخلفي (Backdoor) المهاجم من الوصول إلى جهاز كمبيوتر أو برنامج أو خدمة من خلال التحايل على إعدادات الأمن والحماية الخاصة به (Ciampa, ٢٠١٨). تسمح الأبواب الخلفية المثبتة على جهاز الكمبيوتر للمهاجم بالعودة لاحقًا وتجاوز إعدادات الأمان مجدداً. فهو عبارة عن حساب ينشأ بسرية والذي يسمح بالوصول إلى الجهاز عن بعد دون دراية المستخدم أو إذنه ويكون من الصعب اكتشاف وجوده.

البوت نت: Bot net

تعرف البوت نت (Bot net) على أنها البرامج التي تسمح بوضع الكمبيوتر المصاب تحت جهاز التحكم المهاجم عن بعد بغرض استخدامه لشن هجمات. يُعرف الكمبيوتر المصاب باسم الروبوت أو الزومبي. عندما يتم تجميع المئات أو الآلاف أو حتى الملايين من أجهزة الكمبيوتر الروبوتية في شبكة كمبيوتر منطقية، فإنها تنشئ شبكة الروبوتات الواقعة تحت المهاجم.

تتلقى أجهزة الكمبيوتر الروبوتية المصابة تعليمات -من خلال بنية والتحكم من قبل المهاجم-فيما يتعلق بأجهزة الكمبيوتر التي يجب مهاجمتها وكيف. وذلك من خلال عدة طرق للاتصال بين الروبوتات والمهاجم مثل تسجيل الدخول التلقائي إلى موقع ويب أو إرسال أوامر الهجوم من خلال منشورات تويتر وفيسبوك. ومن المهم الإشارة إلى أن هناك عدداً مذهلاً من الروبوتات والشبكات المتحكمة فيها في جميع أنحاء العالم. وفقًا لقسم الإنترنت التابع لمكتب التحقيقات الفيدرالي، يتم كل ثانية إصابة ١٨ جهاز كمبيوتر في جميع أنحاء العالم وإضافتها إلى شبكة الروبوتات، والتي تصل إلى مئات الملايين من أجهزة الكمبيوتر المخترقة كل عام. (Ciampa, ٢٠١٨)

تطبيق عملي (١)

الهدف: أن يتعرف المتدرب على البرمجيات الخبيثة بشكل أعمق. **الزمن:** ١٥ دقيقة

يعمل المتدربون على استعراض العديد من البرمجيات الخبيثة التي ظهرت منذ ٢٠ عامًا وملاحظة تأثيرها البسيط أو المزعج. بواسطة البحث من خلال متصفح الانترنت على "Malware Museum" للوصول إلى المواقع التي تعمل على أرشفة هذه البرمجيات، واستكشاف البرمجيات الخبيثة المعروضة وملاحظة ما تقوم بفعله (مع العلم بأن جميع البرمجيات الخبيثة المعروضة في هذا من المواقع تعتبر غير فعالة ولن تضر بجهاز الكمبيوتر).

الإرشادات:

١. يقوم المتدربون بالدخول على الرابط التالي https://archive.org/details/malwaremuseum&tab=collection
٢. يقوم المتدربون بالنقر على مجموعة من البرمجيات الخبيثة المعروضة وملاحظة ما يفعلونه
٣. يقوم المدرب بمناقشة النتائج مع المتدربين.

الحماية من البرمجيات الخبيثة:

ترتكز وسائل الحماية من البرمجيات الخبيثة على مبدأين: أولاً، الحرص على استخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة والتأكد من تحديثها باستمرار. ثانياً، الاعتماد على سلوك المستخدم، وذلك من خلال رفع وعيه في عدم فتح الملفات أو الروابط المشبوهة، والتأكيد على حمل فحص لكل قرص أو بريد إلكتروني أو ومستند يصل إليه قبل فتحه. (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

يمكن للبرمجيات الخبيثة أن تصيب كل من ملفات المستخدم وكذلك ملفات نظام التشغيل. لذلك، تساعد برامج مكافحة البرمجيات الضارة في الحماية من هذه العدوى. تشمل هذه البرامج كل من برامج مكافحة الفيروسات (Antivirus)، وبرامج مكافحة البريد المزعج (Antispam)، وبرامج مكافحة التجسس (Antispyware). (Ciampa, ٢٠١٨)

برامج مكافحة الفيروسات (Antivirus):

برنامج مكافحة الفيروسات هو عبارة عن برنامج أو تطبيق يتم تثبيته على نظام التشغيل لحمايته من الفيروسات وكذلك الديدان وأحصنة طروادة من خلال فحص النظام والملفات لشكل مستمر للبحث عنها. معظم الفيروسات لها خصائص شائعة بين عائلات الفيروسات. حيث يعمل برنامج مكافحة الفيروسات من خلال البحث عن هذه الخصائص، أو توقيعاتها، لتحديد الفيروسات وتحييدها قبل أن تؤثر على الجهاز أو الملفات، كما تعمل الإصدارات الحديثة من برامج مكافحة الفيروسات في البحث عن مشاكل ملفات تعريف الارتباط (Cookies) أيضًا. تقوم برامج مكافحة الفيروسات على التعرف على الآلاف من الفيروسات والديدان المعروفة بناءً على أكوادها البرمجية. حيث تعمل الشركات المنتجة لبرامج مكافحة الفيروسات بشكل مستمر على تحديث ملفات قاعدة بيانات الخاصة بها والتي تحتوي على بيانات التعريف لجميع الفيروسات المنتشرة والتدابير المضادة لها. ونتيجة لذلك إذا حافظ المستخدم على تحديث برنامج مكافحة الفيروسات على جهازه، فربما لن يكون عرضة بشكل كبير لهجمات الفيروسات والديدان. (Emmett Dulaney and Chuck Easttom, ٢٠١٨).

تعتمد طبيعة عمل برامج مكافحة الفيروسات على فحص جهاز كمبيوتر بحثًا عن أي عدوى بالإضافة إلى مراقبة نشاط الكمبيوتر ومسح المستندات الجديدة التي قد تحتوي على فيروس (يتم إجراء هذا الفحص عادةً عند فتح الملفات أو إنشاؤها أو إغلاقها). إذا تم اكتشاف فيروس، تتضمن الخيارات عمومًا تنظيف الملف المصاب، أو عزله، أو حذفه.

تستخدم العديد من برامج مكافحة الفيروسات المراقبة القائمة على التوقيع (التحليل الثابت)، حيث برنامج مكافحة الفيروسات بفحص الملفات عن طريق محاولة مطابقة أنماط الفيروسات المعروفة مع الملفات التي يحتمل أن تكون مصابة. تحتوي معظم برامج مكافحة الفيروسات على محرك فحص الفيروسات وقاعدة بيانات لتوقيعات الفيروسات المعروفة. ولكن يتمثل ضعف هذا النهج بأنه يجب على مطور برنامج الحماية أن يبحث باستمرار عن فيروسات جديدة، واستخراج توقيعات الفيروسات الخاصة بها، وتوزيع قواعد البيانات المحدثة هذه على جميع المستخدمين، ولكن نظرا للتزايد المطرد لصناعة الفيروسات وانتشارها، أصبح من الصعوبة أن يتم تحديث قاعدة البيانات الخاصة بتوقيعات الفيروسات على مدار الساعة، كما أنه يمكن أن تؤدي أي قاعدة بيانات غير محدثة إلى زيادة احتمالية الإصابة. لذلك، أصبح النهج الأحدث لبرامج الحماية هو المراقبة الاسترشادية (التحليل الديناميكي)، والتي تستخدم مجموعة متنوعة من التقنيات لتحديد خصائص وسلوك الفيروس بدلاً من محاولة إجراء المطابقات مع التوقيعات. الفرق بين التحليل الثابت والكشف عن التحليل الديناميكي مشابه لكيفية فحص أفراد أمن المطارات في بعض الدول للإرهابيين. يمكن التعرف على إرهابي معروف يحاول المرور عبر الأمن من خلال مقارنة وجهه بصور الإرهابيين المعروفين

(تحليل ثابت). ولكن ماذا عن إرهابي جديد لا توجد له صورة؟ يمكن لأفراد الأمن النظر إلى خصائص الشخص – مثل حصوله تذكرة ذهاب فقط، وعدم حمله أي أمتعة، وإظهار العصبية الشديدة -كمؤشرات محتملة على أن الفرد قد يحتاج إلى استجواب.
إحدى تقنيات المراقبة الاسترشادية المستخدمة هي محاكاة الكود التي يتم فيها من خلال إنشاء بيئة افتراضية تحاكي وحدة المعالجة المركزية وذاكرة الكمبيوتر. يتم تنفيذ أي رمز برنامج مشكوك فيه في البيئة الافتراضية (لا يتم تنفيذ رمز فيروس فعلي بواسطة وحدة المعالجة المركزية الحقيقية) لتحديد ما إذا كان فيروسًا أو لا.
بناءً على ذلك، من الواجب على المستخدم الحرص على تثبيت أحد برامج مكافحة الفيروسات المتوفرة بشكل مجاني أو مدفوع والتأكد من تحديثه باستمرار، مع الاشارة على ضرورة الاطلاع على مزايا كل برنامج واختيار الأفضل حسب متطلبات المستخدم.
كما يمكن الاستعانة بموقع https://www.antivirusguide.com/ للاطلاع على أفضل مكافحات الفيروسات حسب آخر تصنيف.

تطبيق عملي (٢)

الهدف: أن يتعرف المتدرب على آليات الفحص للكشف عن وجود البرمجيات الخبيثة. **الزمن:** ١٥ دقيقة

يعمل المتدربون على استخدام موقع VirusTotal، وهو خدمة مجانية عبر الإنترنت تقوم بتحليل الملفات وعناوين URL لتحديد البرمجيات الخبيثة المحتملة. يقوم VirusTotal بفحص أي نوع من الملفات والبيانات. تم تصميم VirusTotal للحصول على «رأي ثانٍ» بخصوص وضع ملف أو عنوان URL قد تم تصنيفه على أنه (مشبوه) بواسطة البرامج الأخرى لمكافحة البرمجيات الخبيثة.

الإرشادات:

١. يستخدم المتدربون برنامج Microsoft Word لإنشاء مستند يحتوي على الفقرة التالية "Virus Total Explore"
٢. يتم حفظ المستند كـ VirusTotal.docx.
٣. يتم تحويل هذا المستند إلى ملف PDF. يتم النقر فوق ملف ومن قم النقر على حفظ باسم. ضمن حفظ كنوع: يتم تحديد PDF (*.pdf). يتم حفظ هذا الملف بصيغة YourName-VirusTotal.pdf.
٤. يتم فتح متصفح الويب وإدخال عنوان www.virustotal.com
٥. يجب التأكد من تواجدنا في تبويب ملف (File)، ومن ثم يتم النقر فوق اختيار ملف (Choose File).
٦. يتم اختيار الملف الذي تم انشاؤه سابقا YourName-VirusTotal.pdf ومن ثم النقر فوق فتح (Open).
٧. يتم النقر من خلال الموقع على رفع الملف (Confirm Upload).
٨. يبدأ الموقع بفحص الملف.
٩. يتم الانتظار لحين انتهاء الموقع من فحص الملف واستعراض النتائج، من خلال المرور على قائمة مطوري برامج مكافحة الفيروسات والبرمجيات الخبيثة واستطلاع نتائج فحوصاتهم بخصوص هذا الملف. وجود العلامة الخضراء تعني أنه لم يتم الكشف عن برامج ضارة.
١٠. من الممكن إعادة نفس الخطوات على أحد المواقع لفحصه من خلال اختيار تبويب URL.

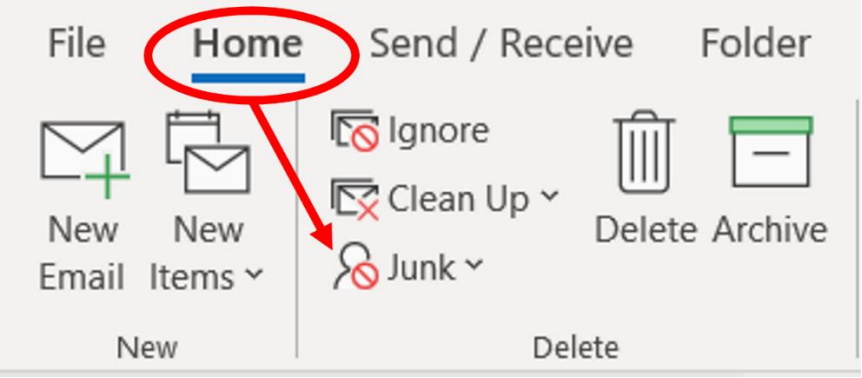
برامج مكافحة البريد المزعج (Antispam):

يعمل هذا النوع من البرامج على مراقبة البريد الإلكتروني بحثًا عن البريد المزعج (العشوائي) أو أي محتوي غير مرغوب فيه لمنع وصول هذه الرسائل إلى المستخدم، علماً بأن أغلب مزودي خدمة البريد الالكتروني يوفرون هذه الخدمة دون تدخل المستخدم. ومع ذلك، لا يزال بإمكان بعض الرسائل غير المرغوب فيها المرور. لذلك يمكن للمستخدمين تثبيت برامج تصفية البريد المزعج على أجهزة الكمبيوتر الخاصة بهم أو تكوين ضبط إعدادات برنامج عميل البريد الإلكتروني المحلي (Microsoft Outlook) لاحتجاز الرسائل غير المرغوب فيها.

هناك طرق مختلفة لتصفية الرسائل غير المرغوب فيها على عميل البريد الإلكتروني المحلي أو على متصفح الويب. يقوم العديد من مستخدمي البريد الإلكتروني بحظر أنواع محددة من ملفات المرفقات التي يحتمل أن تكون خطرة، مثل.exe و.bat و.vbs و .com. يمكن للمستخدمين أيضًا إنشاء قوائم للمرسلين المعتمدين أو غير المعتمدين، ويمكن تصفية البريد الإلكتروني حسب المنطقة أو البلد.

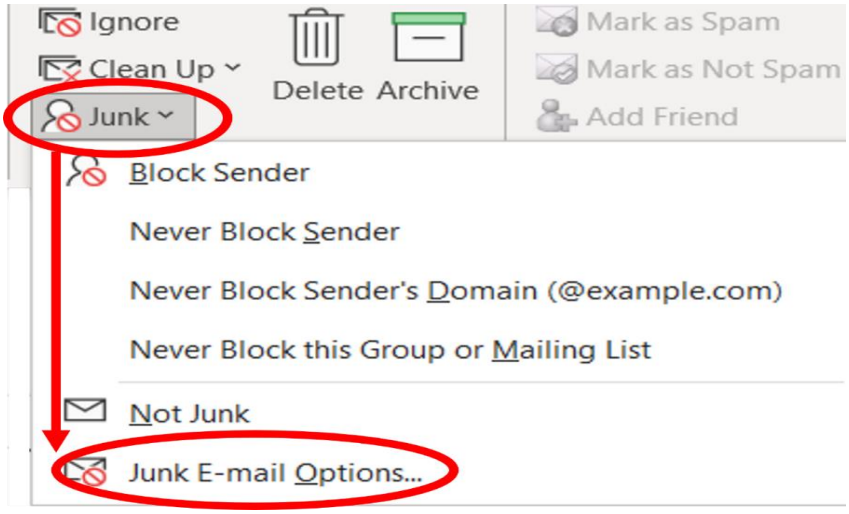
نستعرض فيما يلي خطوات ضبط إعدادات برنامج عميل البريد الإلكتروني المحلي (Microsoft Outlook) لفترة الرسائل غير المرغوب فيها:

١. من الواجهة الأساسية لبرنامج Outlook، يتم اختيار الخيار Junkفي التبويب Home شكل (٩): *إعداد مكافح البريد المزعج (خطوة ١).*.



شكل (٩): إعداد مكافح البريد المزعج (خطوة ١).

٢. يتم اختيار الخيار Junk E-mail Options الموضحة في شكل (١٠)



شكل (١٠): إعداد مكافح البريد المزعج (خطوة ٢).

٣. من تبويب Options في النافذة المنبثقة، يتم اختيار مستوى التصفية المطلوب شكل (١١): *إعداد مكافح البريد المزعج (خطوة٣).*

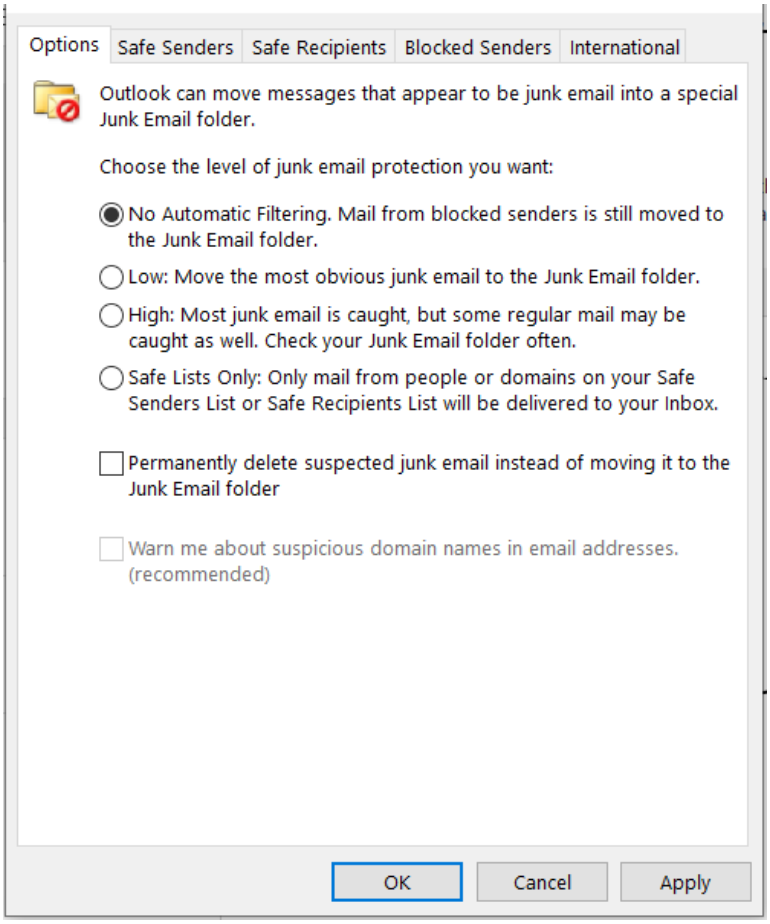
٤. حسب ما يلي ثم الضغط على Apply:

a. بدون تصفية: على الرغم من أن هذا الأمر يمنع تشغيل "عامل تصفية البريد الإلكتروني غير الهام" التلقائي، إلا أنه لا يزال يتم تقييم الرسائل باستخدام أسماء المجالات وعناوين البريد الإلكتروني في قائمة المرسلين المحظورين.

b. منخفض: إذا لم تتلق العديد من الرسائل غير المرغوب فيها، أو تريد تصفية الرسائل الأكثر وضوحًا فقط، فحدد هذا الخيار.

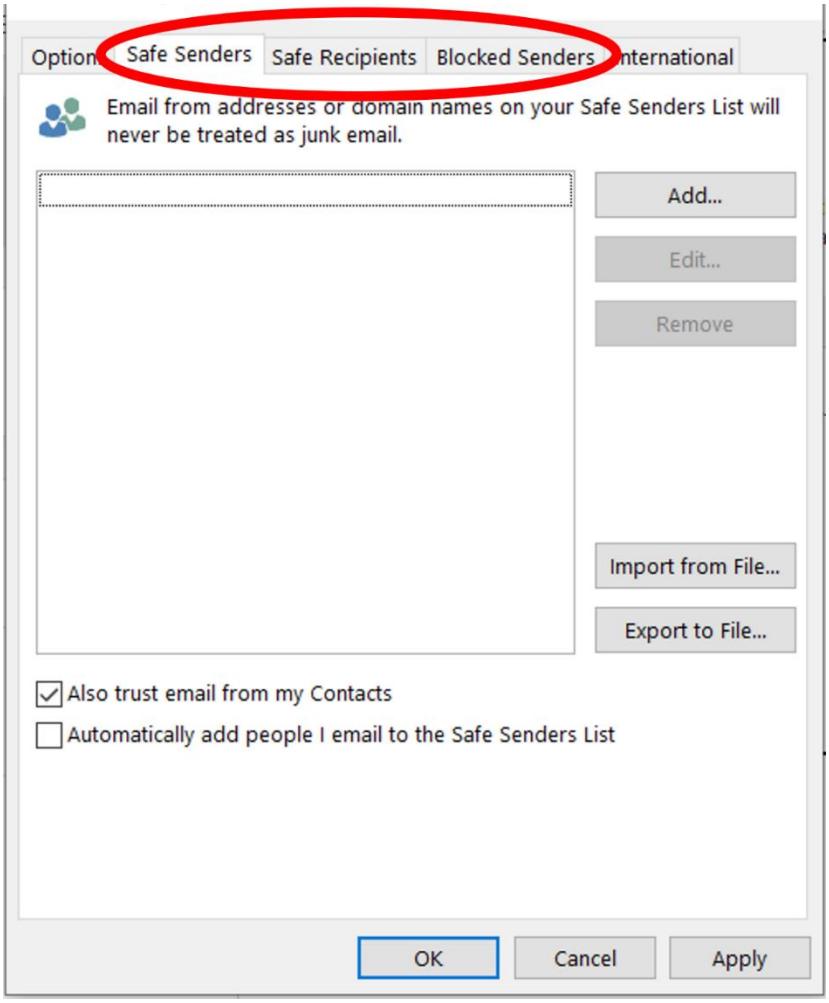
c. عالي: إذا تلقيت الكثير من الرسائل غير المرغوب فيها، ولكنك لا تريد تقييد الرسائل الواردة من المرسلين على القوائم الآمنة، فحدد هذا الخيار. نوصي بالتحقق من مجلد البريد الإلكتروني غير الهام من وقت إلى آخر للتأكد من عدم نقل الرسالة التي تريدها عن طريق الخطأ.

d. القوائم الآمنة فقط: هذا هو الخيار الأكثر تقييداً. يتم تصنيف أي رسالة غير مرسلة من شخص خزينة "قائمة المرسلين" الخاصة بك أو ليست إلى قائمة بريدية في قائمة المستلمين خزينة، كرسالة غير هام.



شكل (١١): *إعداد مكافح البريد المزعج (خطوة٣).*

٥. يتم قوائم للمرسلين المعتمدين أو غير المعتمدين من خلال إضافة القوائم في التبويبات الموضحة في شكل (١٢): *إعداد مكافح البريد المزعج (خطوة ٤)*..



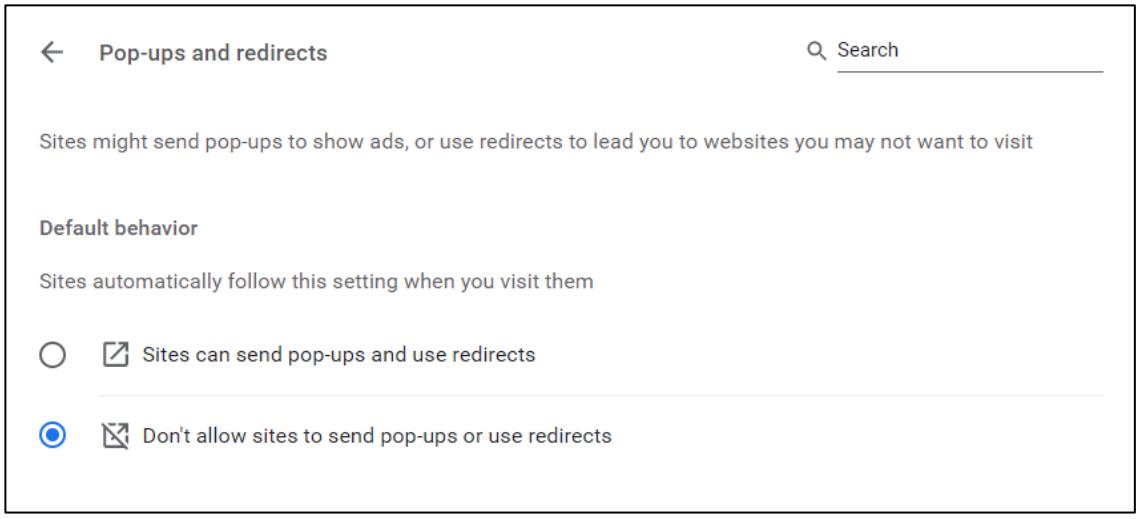
شكل (١٢): *إعداد مكافح البريد المزعج (خطوة ٤).*

برامج مكافحة التجسس (Antispyware):

تساعد برامج مكافحة التجسس على منع إصابة أجهزة الكمبيوتر بأنواع مختلفة من برامج التجسس. أحد الأنواع الشائعة من برامج مكافحة التجسس هو مانع النوافذ المنبثقة (popup blocker). النافذة المنبثقة هي نافذة متصفح ويب صغيرة تظهر عبر صفحة ويب، ويتم إنشاء معظم النوافذ المنبثقة بواسطة المعلنين وإطلاقها بمجرد زيارة موقع ويب، مع الإشارة إلى أن بعض النوافذ المنبثقة تكون لتفعيل بعض خدمات المتصفح. باستخدام مانع النوافذ المنبثقة، يمكن للمستخدمين في كثير من الأحيان تحديد مستوى الحظر، بدءًا من حظر جميع النوافذ المنبثقة إلى السماح بنوافذ منبثقة محددة. يمكن أن يكون مانع النوافذ المنبثقة جزءًا من حزمة مكافحة التجسس، أو برنامج منفصل، أو ميزة مدمجة في متصفح الويب يمنع ظهور الإعلانات المنبثقة.

وسنستعرض فيما يلي خطوات تغيير الإعدادات التلقائية للنوافذ من متصفح Chrome:

١. افتح متصفح Chrome، انقر على رمز المزيد ⋮ في أعلى يسار الشاشة ثم Settings.
٢. ضمن خيار "Privacy and Security"، انقر على إعدادات Site Setting.
٣. انقر على خيار Pop-ups and redirects.
٤. حدّد الخيار الذي تريد ضبطه كإعداد تلقائي كما في شكل (١٣): *مانع النوافذ المنبثقة في Chrome*.



شكل (١٣): مانع النوافذ المنبثقة في Chrome.

برامج حماية نقطة النهاية (Endpoint protection):

تُعرف هذه البرامج على أنها صورة مطورة وشاملة من برامج الحماية من الفيروسات، وهي تعنى بأكثر من مجرد حماية لنظام الكمبيوتر من الإصابة بالفيروسات، حيث تقدم Endpoint protection المزايا التالية: (أغروال، كامبو، بيرس، ٢٠١٨).

- الحماية من الفيروسات والبرمجيات الخبيثة.
- دعم ومراقبة جدران الحماية.
- كشف التسلل إلى الجهاز.
- سلامة الملفات.
- الحماية من سرقة الهوية.
- مراقبة وصول الأطفال.

العنصر الثاني: الإعدادات الأمنية لنظم التشغيل:

يتكون نظام التشغيل (Operating System OS) من عدد كبير من برامج الحاسوب التي تتكون من مئات الآلاف من الأوامر وربما تصل إلى أكثر من مليون أمر لذلك يمكن ملاحظ أن مجلد نظام التشغيل على حاسبك يشغل مساحة كبيرة من وحدة التخزين. نظراً للعدد الكبير من البرامج التي يتكون منها نظام التشغيل ولتشعب عملياتها، فإن الشركات المنتجة لها كانت في الماضي تنتج إصدار جديد كل بضعة أشهر لكي تعالج المشاكل التي توجد في أوامر النظام ولكي تضيف مزيداً من الخصائص. الطريقة السابقة لم تعد تصلح مع نظم التشغيل الحديثة فالشركات المنتجة لها قد تحتاج إلى تحديث وتطوير برامجها كل يوم.

قدمت شبكة الإنترنت حلاً لتحديث نظم التشغيل حيث أتاحت للشركات المنتجة لها طريقة سهلة وسريعة لكي يستطيع المستخدم تحديث النظام الذي يتعامل معه على حاسوبه. باستخدام هذه الطريقة لم تعد الشركات تسعى إلى إصدار نسخة جديدة من نظم التشغيل كل بضعة أشهر، فنظام التشغيل يمكن أن يعيش لسنوات طويلة طالما تتمكن الشركات المنتجة لها من علاج المشاكل التي تظهر به ومن تقديم خدمات جديدة عن طريق مواقعها على شبكة الإنترنت.

هناك أنواع عدة واستخدامات مختلفة لأنظمة التشغيل، يمكن حصر الأنواع الرئيسية منها في جدول (٦) (Ciampa, ٢٠١٨).

جدول (٦): *أنواع أنظمة التشغيل الرئيسية.*

نوع نظام التشغيل	استخدامه	أمثلة
أنظمة تشغيل محطات العمل	نظام يدير الأجهزة والبرامج على جهاز كمبيوتر العميل.	Mac Microsoft Windows, Apple OS, Ubuntu Linux
أنظمة تشغيل الخوادم	النظام الذي يتم تشغيله على الخوادم الموجودة على الشبكة لإتاحة وإدارة الموارد لمستخدمي الشبكة.	Microsoft Windows Server, Mac OS Server, Red Hat Apple Linux
أنظمة تشغيل الأجهزة المحمولة	نظام تشغيل للهواتف المحمولة والهواتف الذكية والأجهزة اللوحية وغيرها من الأجهزة المحمولة.	Google Android, Apple iOS, Microsoft Windows Mobile
أنظمة تشغيل الشبكات	نظام يعمل على أجهزة الشبكة مثل جدران الحماية (Firewalls) أو أجهزة التوجيه (Routers) أو أجهزة التبديل (Switches).	Cisco Internetwork Operating System (IOS), Juniper JUNOS, MikroTik RouterOS

على الرغم من أن أنظمة التشغيل مزودة بخدمات حماية مصممة لرفع مستوى الأمان، إلا أنه يجب حماية نظام التشغيل نفسه. يتضمن تأمين نظام التشغيل إعداده بالتكوين المناسب (OS Configuration)، وتنفيذ أدوات إدارة التصحيح (Patch Management)، واستخدام برامج مكافحة البرمجيات الخبيثة (التي تم استعراضها سابقاً).

تكوين إعدادات الأمان لنظام التشغيل (OS Security Configuration):

يعتمد أمان نظام التشغيل على التكوين المناسب لميزات الأمان المضمنة فيه. تحتوي أنظمة التشغيل الحديثة على مئات من إعدادات الأمان المختلفة التي يمكن تكوينها وإعدادها. يجب أن يتضمن تكوين أمان نظام التشغيل النموذجي ما يلي: (Ciampa, ٢٠١٨)

- تعطيل المنافذ والخدمات غير الضرورية: تركز إحدى تكوينات أمان نظام التشغيل الأساسية على تعطيل المنافذ والخدمات غير الضرورية، أو "إيقاف تشغيل" أي خدمة لا يتم استخدامها، مثل Microsoft Windows ASP.NET State Service. كما أن إغلاق أي منافذ TCP غير ضرورية يؤدي إلى تعزيز مستوى الأمان في نظام التشغيل.
- تعطيل الحسابات / كلمات المرور الافتراضية: تتضمن بعض أنظمة التشغيل على حسابات افتراضية أو غير ضرورية. على سبيل المثال، يتضمن Microsoft Windows ١٠ على حساب Administrator افتراضي، حيث يمكن استخدامه على أجهزة الكمبيوتر الجديدة لتشغيل البرامج والتطبيقات قبل إنشاء حسابات المستخدمين. بالإضافة إلى ذلك، قد تأتي بعض الحسابات بكلمات مرور افتراضية يجب الحرص على تغييرها.
- تفعيل الحد الأدنى من الوظائف والعمليات: ينص هذا المفهوم يجب منح المستخدم الحد الأدنى من مجموعة الأذونات المطلوبة لأداء المهام الضرورية؛ يجب تكوين جميع الأذونات الأخرى على أنها غير متاحة للمستخدم. على سبيل المثال، يجب ألا يكون لدى المستخدم القدرة على تعديل ميزات أمان النظام مثل إيقاف تشغيل جدار حماية على جهاز العميل.
- تحديد القائمة البيضاء / القائمة السوداء للتطبيقات: يتمثل الأسلوب الأكثر شيوعًا لأمان نظام التشغيل على جهاز العميل في استخدام القائمة البيضاء / القائمة السوداء للتطبيقات. تعتمد عملية الإدراج في القائمة البيضاء على تطبيقات معتمدة ومحددة مسبقا لتشغيلها على نظام التشغيل بحيث يتم تقييد أو رفض أي عنصر لم يتم اعتماده أو الموافقة عليه كرفض افتراضي (default-deny). ويكون وضع القائمة السوداء على النقيض من القائمة البيضاء، حيث إنشاء قائمة بالبرامج غير المعتمدة بحيث يمكن السماح بتشغيل أي عنصر غير موجود في قائمة التطبيقات المدرجة في القائمة السوداء بشكل افتراضي (default-allow).

بعد تحديد تكوين الأمان (Security Configuration) بشكل مناسب على أحد أجهزة المستخدمين، يمكن استخدام أدوات لأتمتة عملية نشر تكوين الأمان على بقية الأجهزة بدلاً من إعادة إنشاء نفس تكوين الأمان على كل كمبيوتر.

في Microsoft Windows، يعد قالب الأمان عبارة عن مجموعة من إعدادات تكوين الأمان. تتضمن هذه الإعدادات عادةً سياسات الحساب (account policies) وحقوق المستخدم (user rights) وإعدادات سجل الأحداث (event log settings) والمجموعات (restricted groups) وخدمات النظام (system services) وأذونات الملفات (file permissions) وأذونات التسجيل (registry permissions). بمجرد تكوين جهاز عميل واحد بشكل صحيح، يمكن تطوير قالب أمان من ذلك العميل واستخدامه للنشر على أنظمة أخرى.

أدوات إدارة التصحيح (Patch Management):

لمعالجة الثغرات الأمنية في أنظمة التشغيل التي تم اكتشافها بعد إطلاق النظام، يعمل مطورو أنظمة التشغيل عادةً على إطلاق تحديثات "إصلاح" لأنظمتهم والتي يمكن أن تأتي بأشكال متنوعة. تصحيح الأمان (Security Patch) بشكل عام هو عبارة عن تحديث أمان تم إصداره لبرنامج ما بهدف إصلاح ثغرة أمنية فيه.

تتضمن إدارة التصحيح الفعالة (Patch Management) نوعين من أدوات إدارة التصحيح لإدارة هذه الإصلاحات والتحسينات. النوع الأول يتضمن أدوات لتوزيع التصحيح (Patch Distribution)، بينما النوع الثاني يتضمن استقبال التصحيح (Patch Reception)، وسيتم فيما يلي استعراض كل منهما: (Ciampa, ٢٠١٨)

- أدوات توزيع التصحيح Patch Distribution:

توزع أنظمة التشغيل الحديثة، مثل Red Hat Linux و Apple mac OS وMicrosoft Windows، التصحيحات بشكل متكرر. ومع ذلك، يمكن أن تؤدي هذه التصحيحات في بعض الأحيان إلى حدوث مشكلات جديدة، مثل منع تطبيق خاص بأعمال المنظمة من العمل بشكل صحيح. عادةً ما تختبر المنظمات التي لديها هذه الأنواع من التطبيقات ملفات التصحيحات عند إصدارها للتأكد من أنها لا تؤثر سلبًا على أي تطبيقات خاصة بها. في هذه الحالات، تؤخر المؤسسة تثبيت التصحيح من خدمة التحديث التلقائي عبر الإنترنت من مطور نظام التشغيل حتى يتم اختبار التصحيح بدقة. ولكن كيف يمكن للمنظمة منع موظفيها من تثبيت أحدث تصحيح حتى انهاء الاختبار، في ظل قيام جميع المستخدمين بتنزيل التصحيحات الضرورية وتثبيتها؟ الجواب هو خدمة تحديث التصحيح الآلي (automated patch update service). تُستخدم هذه الخدمة لإدارة التصحيحات داخل المؤسسة بدلاً من الاعتماد على خدمة التحديث من خلال الإنترنت. تتكون خدمة تحديث التصحيح الآلي عادةً من مكون مثبت على خادم واحد أو أكثر داخل شبكة المنظمة. ولكن نظرًا لأن هذه الخوادم مرتبطة ببعضها وبالتالي يمكنها نسخ المعلومات فيما بينها، فيجب عادةً توصيل خادم واحد فقط من الخوادم بخدمة التحديث عبر الإنترنت الخاصة بالمطور.

تتمثل مزايا خدمة تحديث التصحيح الآلي فيما يلي:

- ممكن أن يؤدي تنزيل التصحيحات من خادم محلي بدلاً من استخدام خدمة التحديث التلقائي عبر الإنترنت إلى توفير النطاق الترددي والوقت لأنه لا حاجة هنا لكل جهاز كمبيوتر من الاتصال بالخادم الخارجي الخاص بالمطور.
- يمكن للمختصين داخل المنظمة من الموافقة على تحديثات أنظمة العميل أو رفضها، أو فرض تثبيت التحديثات إلا بحلول تاريخ محدد، والحصول على تقارير حول التحديثات التي يحتاجها كل جهاز كمبيوتر.
- يمكن للمختصين الموافقة على التحديثات من أجل "الفحص" فقط؛ هذا يسمح لهم بمعرفة أجهزة الكمبيوتر التي تتطلب التحديث دون تثبيته.

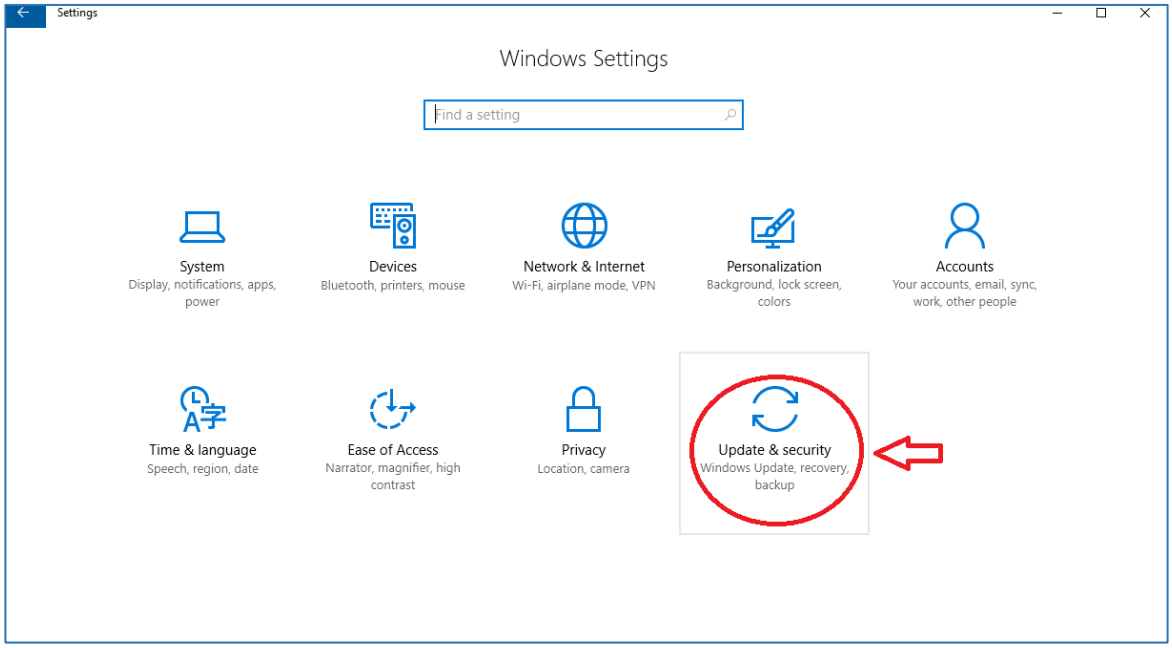
- استقبال التصحيح Patch Reception:

سمحت الإصدارات القديمة من أنظمة التشغيل للمستخدمين بتهيئة كيفية تلقيهم للتصحيحات. على سبيل المثال، قبل Windows ١٠، كان لدى مستخدمي Microsoft عدة خيارات فيما يتعلق بقبول التصحيحات أو رفضها. تضمنت هذه الخيارات تثبيت التحديثات تلقائيًا، أو أن يختار المستخدم ما يود تنزيله وتثبيته من هذه التحديثات، أو إيقاف استقبال التحديثات بشكل تام. ومع ذلك، فقد أدى هذا النهج في كثير من الأحيان إلى تجاهل المستخدمين لتحديثات أمنية مهمة وبالتالي تعريض أجهزة الكمبيوتر الخاصة بهم للخطر. ولكن التوجه السائد الآن، هو عدم تقديم أي خيارات للمستخدمين فيما يتعلق بالتحديثات لتصحيحات؛ بدلاً من ذلك، يتم تنزيل التصحيحات تلقائيًا وتثبيتها متى توفرت. هذا يضمن أن يظل نظام التشغيل محدث دائمًا.

على سبيل المثال، مع إصدار نظام التشغيل Windows ١٠ ، غيرت Microsoft بشكل كبير إجراءات تحديث الأمان وخيارات المستخدم. حيث تشمل هذه التغييرات ما يلي:

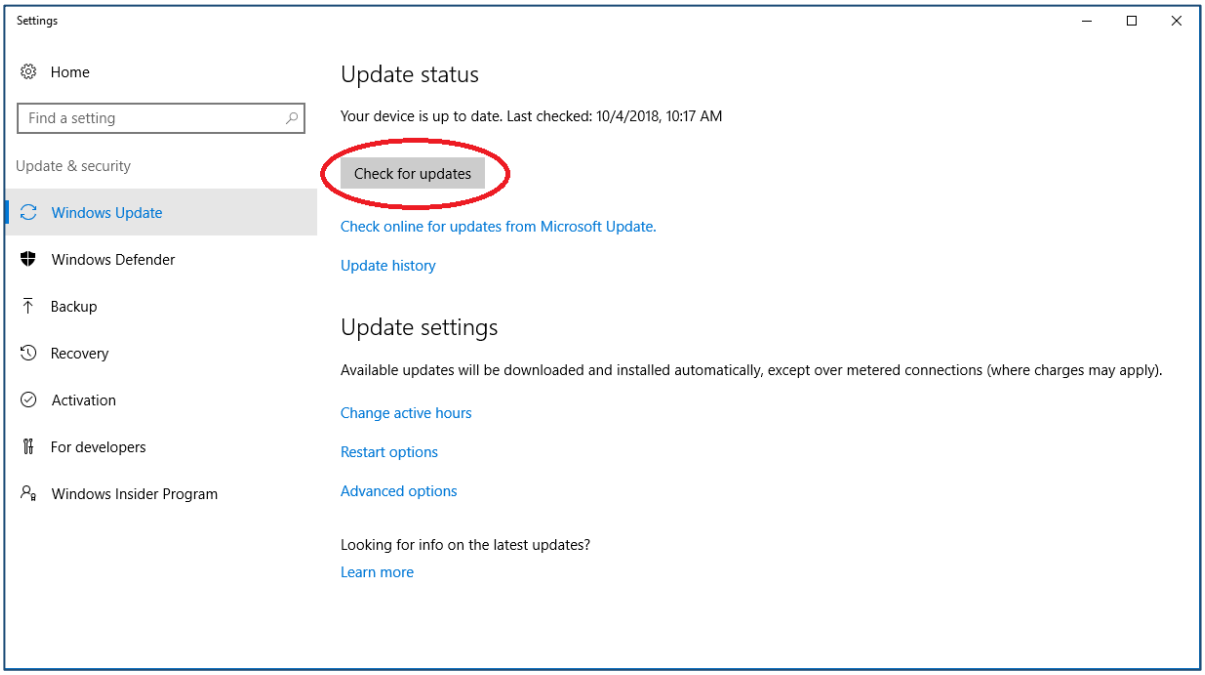
- **التحديثات الإجبارية:** حيث لا يمكن للمستخدمين رفض أو تأخير التحديثات الأمنية. بل يتم تنزيل جميع التحديثات وتثبيتها تلقائيًا.
- لا توجد تحديثات انتقائية: على عكس الإصدارات السابقة منWindows ، لا يمكن للمستخدمين تحديد تحديثات Windowsالفردية لتنزيلها وتثبيتها. ومع ذلك، يمكن للمستخدمين تحديد ما إذا كانوا يرغبون في تلقي تحديثات لمنتجات Microsoftالمثبتة الأخرى مثلOffice .
- **توزيع أكثر كفاءة:** إذا كان هناك العديد من أجهزة Windows ١٠ متصلة من خلال شبكة، فلن يضطر كل جهاز إلى تنزيل التحديثات عبر الإنترنت بشكل فردي. بدلاً من ذلك، بمجرد تنزيل أحد الأجهزة للتحديثات، يمكن توزيعها على الأجهزة الأخرى عبر الشبكة المحلية.
- **إعادة تعيين الأجهزة بشكل محدث:** مع الإصدارات السابقة من Microsoft Windows، إذا كان جهاز الكمبيوتر بحاجة إلى إعادة تعيين إلى الإعدادات الأصلية، فيجب إعادة تثبيت جميع التصحيحات اللاحقة، وهي عملية غالبًا ما تستغرق ساعات من الوقت وتتطلب من المستخدم أن يكون على الكمبيوتر لإدارة عمليات إعادة التشغيل المتعددة. مع نظام التشغيل Windows ١٠، ستقوم "إعادة تعيين جهاز الكمبيوتر" بتثبيت برنامج Windows بآخر تحديث له.

يمكن الوصول إلى إعدادات التحكم بالتحديثات في Windows ١٠ من خلال الدخول على Windows Settings ومن ثم النقر على خيار Update & Security شكل (١٤): *شاشة Windows Settings*



شكل (١٤): *شاشة Windows Settings*

ومن ثم الاطلاع على التحديثات وتثبيتها من شاشة Update Status من خلال النقر على زر Check for Updates



شكل (١٥): *شاشة Update Status*

بشكل عام، تركز Microsoft على المجالات الرئيسية السبعة التالية لرفع مستوى الأمن للمستخدمين الشخصيين: (Michael E. Whitman, Herbert J. Mattord, ٢٠١٨)

١. استخدام برنامج مكافحة الفيروسات والبرمجيات الخبيثة.
٢. استخدام كلمات مرور قوية.
٣. التحقق من إعدادات الأمان في البرامج والتطبيقات المستخدمة.
٤. تحديث مستويات الأمان في البرامج والمنتجات ونظام التشغيل.
٥. تفعيل جدران الحماية (Firewalls).
٦. تنفيذ عمليات النسخ الاحتياطي للنظام والملفات بشكل دوري.
٧. حماية الأجهزة من تغيرات الطاقة الكهربائية (الارتفاع المفاجئ في الطاقة أو فقدانها) من خلال استخدام الموصلات الكهربائية المناسبة.

أما على مستوى المؤسسات الصغيرة، فتوصي Microsoft بما يلي:

١. حماية أجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمولة من خلال الحرص على تحديث البرامج بشكل دوري، وتثبيت برامج الحماية من الفيروسات والبرمجيات الخبيثة، والتأكد من إعداد جدران الحماية (Firewalls).
٢. الحفاظ على أمان البيانات وذلك بإجراء عمليات النسخ الاحتياطي بشكل دوري ومنتظم لحماية بيانات الأعمال المهمة وتعيين صلاحيات الوصول واستخدام آليات التشفير لتشفير البيانات.
٣. استخدم الإنترنت بأمان من خلال تحديد قواعد وسياسات الاستخدام الآمن للإنترنت وذلك لتقليل الثغرات ومخاطر الهجمات التي يكون مصدرها مواقع الويب والنوافذ المنبثقة.
٤. حماية الشبكة من الوصول غير المصرح له (سواء الوصول المادي أو الوصول عن بعد) من خلال مراقبة الشبكات بشكل مستمر واستخدام كلمات مرور قوية للوصول إليها، وخاصة الشبكات اللاسلكية.
٥. حماية الخوادم من الوصول غير المصرح له.
٦. التأكد من أمان التطبيقات الخاصة بالمنظمة والمرتبطة بالأعمال والخدمات الأساسية.
٧. إدارة أجهزة الكمبيوتر بشكل مركزي من خلال الخوادم وبتحديد إجراءات إدارية متوافقة مع حاجة العمل.

العنصر الثالث: الأمن المادي:

يتطلب الأمن المعلوماتي حماية كل من البيانات والأصول المادية على حد سواء. تؤدي الحماية المادية (Physical security) دوراً أساسياً في منظمة الأمن المعلوماتي، فهي تحمي أنظمة المعلومات من المخاطر المادية المباشرة، كالوصول إلى مناطق غير مسموح بها، والسرقة، والتخريب المتعمد، وعبث المعتدين والفضوليين، إضافة إلى حمايتها من الأخطار الطبيعية كالحرائق، والفيضانات، والزلازل. فمهما وضعنا من تجهيزات مركزية وبرمجيات حماية، ومهما كلف ذلك من مبالغ كبيرة، فإنها لن تؤدي دورها إذا سُرقت أو خُربت. لذلك تولي المنظمات الحكومية والخاصة اهتماماً كبيراً بالأمن المادي لمواقعها بشكل عام، ولأنظمة المعلومات ومصادرها بشكل خاص. (القحطاني، ٢٠١٥).

التهديدات المادية:

لدى الأمن المادي مجموعة من التهديدات المادية التي تختلف طبيعتها عن التهديدات التقنية الموجهة للمعلومات. حيث يمكن حصر التهديدات المادية في الأقسام التالية: (القحطاني، ٢٠١٥).

- تهديدات بشرية: كالوصول غير المشروع إلى مناطق محظورة، والتخريب، والسرقة.
- تهديدات مصادر الخدمات الرئيسية: كانقطاع التيار الكهربائي أو تذبذبه، أو انقطاع وسائل الاتصال.
- تهديدات طبيعية: مثل الحرائق، والفيضانات، والزلازل، وموجات الغبار، والحرارة الشديدة، أو البرودة الشديدة.
- تهديدات عسكرية أو إجرامية: كالصواريخ، والمتفجرات، والعمليات الإرهابية.

بناءً على طبيعة التهديدات المادية، يتوجب لها توفير مستويين من الحماية والأمن، الأمن المادي الإداري والأمن المادي التقني، وفيما يلي استعراض كل مستوى منهما بالتفصيل. (القحطاني، ٢٠١٥)

الأمن المادي الإداري:

يتمثل الأمن المادي الإداري في اتخاذ الإجراءات والتدابير التي من شأنها الحفاظ على مصادر المعلومات والأجهزة التي تحتويها، حيث تتوزع إجراءات الأمن والحماية على مستوى طبقات تبدأ من الخارج إلى الداخل وصولاً إلى الأصل المعلوماتي المراد حمايته. ومن هذه الإجراءات الإدارية ما يلي:

- وضع نقاط حراسة ومراقبة خارجية على أسوار المباني المشتملة على مصادر معلومات (كمراكز البيانات)، ويراقب من خلال هذه النقاط أفراد مدربون ومؤهلون لهذه المهمة.
- وضع اللوحات والعلامات الإرشادية والتحذيرية في الأماكن المناسبة.
- التحكم بالدخول للمرافق من خلال استخدام الأبواب والأقفال المناسبة، سواء ميكانيكية أو الكترونية.
- التحكم بدخول الأفراد باستخدام أنظمة مناسبة للتحقق من الهوية، مثل الدخول بعد تسجيل بصمة اليد للموظفين أو تسجيل بيانات الزوار في سجل مُعد لهذا الغرض.
- تثقيف العاملين وتدريبهم بشكل دوري على الإجراءات والقواعد الأمنية، والتأكد من كفاءتهم وقيامهم بواجباتهم.
- تحديد المسؤوليات والصلاحيات الخاصة بالأمن المادي وتوزيعها على الأشخاص والإدارات المعنية.
- رفع التقارير الدورية عن الأمن المادي بالإضافة إلى الملاحظات والاقتراحات للقيادات العليا.
- تطبيق خطط إدارة المخاطر وتحديد إجراءات الاستجابة للأحداث والتعافي من الكوارث والمتعلقة بالأمن المادي.

الأمن المادي التقني:

يُعنى الأمن المادي التقني بتوفير المعدات الآلية والأجهزة التي توفر الحماية التقنية ضد الأعطال والخلل في الموارد الأصلية، ومنها:

- استخدام دوائر مراقبة مغلقة، من خلال إنشاء شبكات للكاميرات الرقمية لمراقبة جميع المداخل والمخارج والممرات ومراكز البيانات وغرف الأجهزة والخوادم. يجب أن تكون لدى هذه الدوائر القدرة على تخزين مقاطع الفيديو بشكل منتظم وموثق بالتاريخ والوقت للرجوع إليها عند الحاجة.
- استخدام بوابات كشف المعادن في الأماكن المناسبة، للكشف عن المعادن المخفية من قبل المتسللين.
- استخدام حساسات قياس درجات الحرارة والرطوبة، وربطها بالأنظمة التي تعالج مخرجاتها وتقارنها بالحدود الطبيعية المسموح بها، حتى يتم اتخاذ الإجراء اللازم.
- استخدام أجهزة كشف الحرائق وتسربات المياه لحماية الأجهزة من الحالات الطارئة والأعطال في البنية التحتية للمبنى، حيث يتم ربط هذه الأجهزة بنظام إنذار يعمل على إصدار صوت أو ارسال رسالة نصية أو بريد الكتروني لأشخاص محددين، بالإضافة إلى اتخاذ الأجراء المناسب بشكل آلي مثل تشغيل أنظمة إطفاء الحرائق آلياً أو إغلاق مصادر المياه.
- استخدام أنظمة مراقبة الأبواب والأقفال وربطها بأنظمة الإنذار التي ترصد حالاتها إن كانت مفتوحة أو مغلقة، أو الكشف في حال وجود خلل فيها.

وبناءً على ذلك، لابد من الإشارة إلى ضرورة تكامل الأمن المادي الإداري والتقني لتوفير طبقات حماية متتالية محيطة بالأصل المعلوماتي المراد حمايته، حيث أن توزيع الحماية على مستوى طبقات يجعل من الصعب على المهاجم تجاوز هذه الطبقات بسهولة، حيث أنه لو تمكن من تجاوز أحد الطبقات فإنه ليس بالضرورة أن يتمكن من تجاوز الطبقة التي تليها.

حالة دراسية (٣)

الهدف: أن يحلل المتدرب الأمن المادي في بيئات العمل.

الزمن: ١٠ دقائق

قم بإجراء تحليل للأمن المادي في جهة عملك. ما هي نقاط القوة؟ ما هي نقاط الضعف؟ وما هي التوصيات التي ستقدمها لتحسين مستوى الأمان المادي؟

الإرشادات:

١. دراسة الحالة من قبل المتدربين بشكل فردي والعمل على تحليل الأمن المادي حسب المكونات الموضحة في الجدول التالي.

٢. مناقشة النتائج مع المتدربين.

جدول (٧): *تحليل الأمن المادي حسب مكونات الحماية.*

مكون الحماية	متوفر؟		ملاحظات
	نعم	لا	
• حراس أمن للمناطق الحيوية			
• نظام مراقبة بالكاميرات			
• غرف خاصة بالأجهزة التقنية			
• آلية متابعة للدخول للمبنى			
• أجهزة كشف حرائق			
• أجهزة كشف تسربات المياه			
• توفر اللوحات الإرشادية			
• أبواب و أقفال للمناطق الحساسة			

الموضوع الرابع: إدارة الهوية والوصول

يرتكز الأمن المعلوماتي على حماية كل من المعلومات ونظم المعلومات من الأعمال غير المصرح بها كالوصول غير المشروع من الأشخاص أو العناصر غير المصرح لها بذلك، وذلك لضمان السرية (Confidentiality) والتي تعتبر أحد الخصائص الثلاثة لأمن المعلومات والمعروفة بـ(CIA). ولتحقيق السرية لابد من التحقق من هوية المستخدم (Authentication) ليتم اتخاذ القرار الصحيح من السماح له بالوصول إلى البيانات والأنظمة أو عدم السماح له بذلك بناءً على هويته وصلاحياته وهو ما يُعرف بمرحلة التفويض أو الترخيص (Authorization).

وحتى نتمكن أكثر من إيضاح مفاهيم الهوية والوصول، لنفترض السيناريو التالي، كلٌ منا يحتاج إلى الدخول إلى بريده الإلكتروني لإرسال واستقبال الرسائل أو الوصول إلى أحد الأنظمة التقنية لتنفيذ بعض المهام أو الخدمات، غالباً ما يتم ذلك من خلال الخطوات التالية:

- **أولاً**، نحتاج إلى تحديد هويتنا (Identification) من خلال إدخال مُعرف فريد خاص بنا ويميزنا عن بقية المستخدمين، كأن نقوم بإدخال اسم المستخدم.
- **ثانياً**، بعد أن قمنا بتحديد الهوية، نحتاج إلى إثبات مرجعيتها لنا، كأن نقوم بإدخال كلمة المرور مثلاً، حيث سيعمل النظام على مطابقة هذه المدخلات والتأكد من صحتها، وذلك من خلال عملية التحقق من الهوية أو المصادقة (Authentication).
- **ثالثاً**، في حال مطابقة البيانات السابقة ومصادقة الهوية، سيعمل النظام على تسجيل دخول المستخدم والسماح له بالوصول إلى الخدمات أو العمليات المصرح له بالصول إليها فقط حسب صلاحياته، وهو ما يعرف بعملية الترخيص (Authorization).
- **أخيراً**، يتم تسجيل كافة العمليات التي قام بها المستخدم على النظام في ملفات وسجلات خاصة بعرف تعرف باسم Log files، وهي سجلات يتم من خلالها الاحتفاظ بجميع المعلومات الخاصة بالمستخدمين والعمليات التي قاموا بها وموارد النظام التي تمكنوا من الوصول لها وذلك بهدف المتابعة والتدقيق والمحاسبة (Accounting).

كما تجدر الإشارة إلى أنه غالباً ما يستخدم مصطلح AAA للإشارة إلى العمليات الأساسية لإطار التحكم بالوصول للموارد التقنية، المتمثلة في عمليات المصادقة والتفويض والمحاسبة (Authentication, Authorization, and Accounting).

العنصر الأول: التحقق من الهوية Authentication:

تُعرف عملية التحقق من الهوية (المصادقة) على أنها العملية التي يتم من خلالها التحقق من هوية الشخص وأنه الشخص المعني لا غيره. تقنياً، يُعرف التحقق من الهوية على أنه التحقق من أن المستخدم للنظام هو بالفعل من ادعى أنه ذلك المستخدم وفي حال نقل المعلومات فإنه يجب التحقق من هوية المرسل لضمان أن المعلومات قادمة من مصدرها الحقيقي، وكذلك يجب التحقق من هوية المستلم لضمان أن المعلومة ذاهبة إلى وجهتها الصحيحة. ولكن لا بد من الإشارة إلى أن عملية التحقق من الهوية هي مرحلة لاحقة لمرحلة تحديد الهوية (Identification) والتي تتم من تحديد هوية المستخدم بحيث تكون فريدة وغير قابلة للتكرار، مثل تحديد اسم المستخدم. (القحطاني، ٢٠١٥)

يمكن تطبيق آليات التحقق من الهوية باستخدام واحد أو أكثر من الطرق الخمس التالي:

- المصادقة باستخدام شيء تعرفه، مثل كلمات المرور.
- المصادقة باستخدام شيء لديك، مثل الهواتف المحمولة.
- المصادقة باستخدام شيء تملكه، مثل بصمات الأصابع.
- المصادقة باستخدام شيء تفعله، مثل طريقة الطباعة على لوحة المفاتيح.
- المصادقة باستخدام موقعك الجغرافي.

وفيما يلي توضيح لآليات المصادقة الخمس والتعرف على مزايا وعيوب كل آلية. (Ciampa, ٢٠١٨)

(ماذا تعرف؟)

تعتبر كلمات المرور من أكثر طرق المصادقة شيوعاً باستخدام آلية (ماذا تعرف؟). حيث يطلب من المستخدمين في معظم الأنظمة والأجهزة بتعريف أنفسهم من خلال ادخال اسم المستخدم (والذي لا يعتبر معلومة سرية) وكلمة المرور لإتمام عملية إثبات هوية المستخدم. تُعرف كلمة المرور أنها مجموعة سرية من الأحرف والأرقام والرموز التي يجب أن يكون المستخدم فقط على علم بها. على الرغم من استخدام كلمات المرور على نطاق واسع، إلا أن الحماية التي توفرها تعتبر ضعيفة إلى حد ما نظرا لوجود العديد من الهجمات التي تستهدفها.

تتضمن الهجمات التي تستهدف كلمة المرور محاولات لتخمين كلمات المرور أو ما يُعرف تقنيا بكسر كلمة المرور. هناك عدد من الطرق والهجمات لمحاولة كسر كلمات المرور كما يلي: (Michael E. Whitman, Herbert J. Mattord, ٢٠١٨)

- الهجوم القسري Brute force attack:

حيث يتم من خلال هذه الهجمة محاولة تخمين كل مزيج ممكن أن يشتبه بكونه كلمة المرور، ويعتبر هذا النوع بطيئًا حيث إنه يستغرق وقتا للتخمين.

- الهجوم باستخدام القاموس Dictionary attack:

هو نوع من الهجوم القسري الذي يضيق النطاق باستخدام قاموس كلمات المرور الشائعة ويتضمن معلومات متعلقة بالمستخدم المُستهدف، مثل أسماء العائلة والأقارب والأرقام المألوفة كأرقام الهواتف والعناوين. من الممكن على مستوى المنظمات لتقليل التعرض لهذا النوع من الهجمات، استخدام قواميس مماثلة لعدم السماح للمستخدمين باستخدام كلمات المرور الموجودة في هذه القواميس أثناء عملية إعادة التعيين وبالتالي الحماية من كلمات المرور التي يسهل تخمينها. بالإضافة إلى ذلك، فإن القواعد التي تشترط أرقامًا وحروفاً خاصة في كلمات المرور تجعل هجوم القاموس أقل فعالية.

- الهندسة الاجتماعية Social engineering attack:

يتم ذلك من خلال قيام المهاجمون بتجميع بيانات عن الشخص المراد اختراق حسابه ومحاولة استخدامها ككلمة مرور، ويتم تجميع تلك المعلومات عن طريق الشبكات الاجتماعية مثلًا (سيتم التطرق لموضوع الهندسة الاجتماعية بالتفصيل لاحقا في هذه الحقيبة).

ولكن من الممكن تقليل التعرض لهذه الهجمات من خلال تقوية كلمات المرور وذلك باتباع النقاط التالية:

- يجب الاعتماد على كلمات مرور طويلة بحيث لا تقل كلمة المرور عن ١٠خانات.
- يجب الاعتماد على كلمات مرور مقعدة بحيث يتم الاعتماد على استخدام الحروف باختلاف حالتها الكبيرة والصغيرة) والأرقام والرموز، ويجب الابتعاد عن كلمات المرور المتسلسلة مثل ١٢٣٤٥٦ أو abcdefg.
- يجب الاعتماد على كلمات مرور يصعب تخمينها بحيث لا يتم استخدام البيانات الشخصية مثل تاريخ الميلاد أو اسم العائلة.
- يجب ألا يتم استخدام نفس كلمة المرور لأكثر من حساب.
- يجب تغيير كلمة المرور بشكل دوري، كل شهرين مثلا.
- يجب عدم استخدام كلمات مرور دارجة ويكثر استخدامها مثل استخدام كلمة password ككلمة مرور.
- يجب عدم إعادة استخدام كلمة مرور قديمة سبق استخدامها.
- يجب عدم كتابة كلمات المرور في مكان ما للتذكير مثل كتابتها في ورقة خارجية أو مذكرة الهاتف.
- يجب عدم ضبط الأجهزة للدخول على الحسابات تلقائياً، مثل تفعيل خاصية (تذكر كلمة المرور).
- عدم إدخال كلمات المرور حينما يكون الاتصال غير آمن بالشبكة أو إدخالها في أجهزة عامة أو غير محمية.

تطبيق عملي (٣)

الهدف: أن يتعرف المتدرب على هجوم القاموس لكسر كلمات المرور. **الزمن:** ١٥ دقيقة

يعمل المتدربون على تطبيق هجوم القاموس dictionary attack لمحاولة كسر كلمات المرور مختلفة القوة وذلك باستخدام online password cracker.

الإرشادات:

١. يستخدم المتدربون متصفح الويب الخاص بك للذهاب إلى www.fileformat.info/tool/hash.htm
٢. ضمن جزء String hash، أدخل كلمة المرور البسيطة abcd١٢٣٤ في مربع النص.
٣. انقر فوق الزر Hash.
٤. قم بالتمرير والنزول لأسفل الصفحة وانسخ قيمة MD٥ لكلمة المرور بعد تشفيرها. عن طريق تحديد النص والنقر بزر الماوس الأيمن واختيار نسخ.
٥. افتح علامة تبويب جديدة في متصفح الويب الخاص بك.
٦. اذهب إلى https://crackstation.net/.
٧. الصق النص المنسوخ والذي يمثل القيمة المشفرة لكلمة المرور abcd١٢٣٤ في مربع النص.
٨. قم باختيار I'm not robot، ومن ثم اضغط على الزر Crack Hashes.
٩. هل ظهرت لك كلمة المرور التي تم إدخالها قبل التشفير؟
١٠. قم بتحديث روابط المواقع السابقة وذلك بالضغط على زر refresh في المتصفح.
١١. قم بإعادة الخطوات السابقة على كلمة المرور D٥٨#sec٩٦m.
١٢. هل استطاع موقع crackstation من كسر كلمة المرور هذه المرة؟

(ماذا لديك؟):

الآلية الثانية من آليات المصادقة تعتمد على عنصر يكون بحوزة المستخدم، العناصر الأكثر استخداما للمصادقة بهذا النوع هي جهاز الشفرة الرقمية (token) والبطاقات الذكية والهواتف المحمولة. غالبًا ما يتم استخدام هذه العناصر جنبًا إلى جنب مع كلمات المرور. نظرًا لأن المستخدم يستخدم أكثر من نوع من آليات المصادقة -ما يعرفه المستخدم (ككلمة المرور) وما يمتلكه المستخدم (كالهاتف المحمول) -يُسمى هذا النوع من بالمصادقة المتعددة، حيث يُطلق على استخدام نوع واحد فقط من آليات المصادقة بالمصادقة الأحادية.

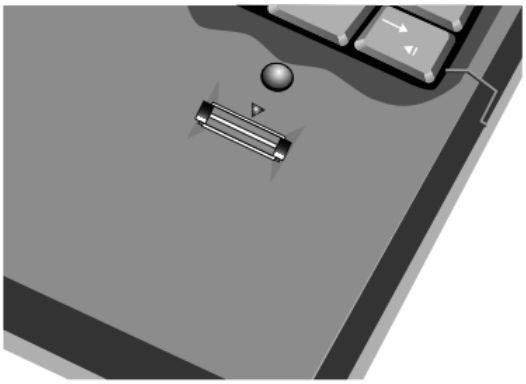
جهاز الشفرة الرقمية (token) عبارة عن جهاز صغير مع نافذة للعرض، متزامن مع خادم المصادقة. ويتم إنشاء شفرته من خوارزمية معينة يحددها خادم المصادقة وتتغير الشفرة كل ٣٠ إلى ٦٠ ثانية. أما البطاقة الذكية فهي بطاقة تتضمن شريحة تحتوي على خط ممغنط وهو بدوره يحوي معلومات المستخدم التي تقوم بتعريفه.

مؤخراً، حلت الهواتف المحمولة مكان جهاز الشفرة الرقمية (token) والبطاقات الذكية بشكل كبير. يمكن إرسال رمز إلى الهاتف المحمول الخاص بالمستخدم من خلال تطبيق رمز أمان برمجي على الجهاز أو كرسالة نصية عند استخدام خوارزمية إنشاء كلمات المرور المستخدمة لمرة واحدة ومحصورة بعمر زمني Time-based One-Time Password (TOTP).

(ماذا تملك؟):

الآلية الثالثة من آليات المصادقة تعتمد على مميزات وخصائص المستخدم التي تتضمن القياسات الحيوية القياسية المميزة للفرد مثل التعرف على وجه الشخص أو بصمات أصابعه أو بصمة صوته أو عينيه للتحقق من هويته، وهو ما يتطلب وجود ماسحات ضوئية بيو مترية متخصصة في أجهزة إدخال تقنية للتعرف على هذه القياسات، مثل استخدام جهاز مسح بصمات الأصابع الموضح في شكل (١٦): *جهاز مسح بصمات الأصابع*.

.



شكل (١٦): *جهاز مسح بصمات الأصابع*.

ولكن تتمثل عيوب هذه الآلية في أن الأجهزة القارئة للقياسات البيو مترية غالباً ما تكون باهظة الثمن، وفي بعض الأحيان تكون قراءاتها غير دقيقة.

(ماذا تفعل؟)

يعتمد هذا النوع من المصادقة على الإجراءات أو السلوكيات التي يؤديها المستخدم بشكل فريد، هذا يسمى أحيانًا القياسات الحيوية السلوكية. أحد أنواع القياسات الحيوية السلوكية هو طريقة النقر على لوحة المفاتيح (ديناميكية النسخ)، والتي تحاول التعرف على إيقاع الكتابة الفريد للمستخدم، حيث اتضح أن كل مستخدم يكتب بوتيرة مختلفة عن الآخر على لوحة المفاتيح.

خلصت دراسة مولها المكتب الوطني الأمريكي للمعايير إلى أن ديناميكيات ضغط المفاتيح لإدخال اسم مستخدم وكلمة مرور يمكن أن توفر دقة تصل إلى ٩٨ بالمائة. تستخدم ديناميكيات ضغط المفاتيح متغيرين فريدين للكتابة. يُعرف الأول باسم وقت الاستقرار، وهو الوقت الذي يستغرقه الضغط على المفتاح ثم تحريره. السمة الثانية هي زمن الانتقال، أو الوقت بين ضغطات المفاتيح (يتم قياس كل من "لأسفل" عند الضغط على المفتاح و "لأعلى" عند تحرير المفتاح). يتم جمع عينات متعددة لتكوين نموذج كتابة للمستخدم، ثم يتم إرسالها مع نموذج الكتابة الفردي للمستخدم الذي تم الحصول عليه عن طريق إدخال اسم المستخدم وكلمة المرور إلى خادم المصادقة. إذا تطابق كل من كلمة المرور وعينة الكتابة مع تلك المخزنة على خادم المصادقة فإنه يتم مصادقة المستخدم؛ إذا كان قالب الكتابة لا يتطابق بالرغم من أن كلمة المرور متطابقة، فلن تتم مصادقة المستخدم. تتمتع ديناميكيات ضغط المفاتيح بقدر كبير من القبول نظرًا لأنه لا تتطلب أجهزة متخصصة ولأن المستخدم لا يضطر إلى اتخاذ أي خطوات إضافية بخلاف إدخال اسم المستخدم وكلمة المرور، يتوقع بعض الخبراء هذه الآلية ستنتشر على نطاق واسع في المستقبل القريب.

(أين أنت؟)

يعتمد هذا النوع من المصادقة على مكان وجود المستخدم، يُعرف أيضًا باسم تحديد الموقع الجغرافي، وهو تحديد موقع شخص أو كائن باستخدام الخرائط الجغرافية التقنية. ومع ذلك، غالبًا ما يستخدم هذا النوع من المصادقة لرفض المحتالين بدلاً من قبول المستخدمين المصرح لهم. بمعنى آخر، على الرغم من أن الموقع الجغرافي قد لا يحدد المستخدم بشكل فريد، إلا أنه يمكن أن يشير إلى ما إذا كان منتحل الهوية يحاول تنفيذ إجراء من موقع مختلف عن الموقع الطبيعي للمستخدم.

تم استخدام تحديد الموقع الجغرافي لأجهزة الكمبيوتر المحمولة والمكتبية لعدة سنوات، خاصة من قبل المؤسسات المالية. على سبيل المثال، عادةً ما يدخل المستخدم إلى موقع الويب الخاص بالبنك الذي يتعامل معه من جهاز الكمبيوتر المنزلي الخاص به، ولذلك يمكن استخدام هذه المعلومات لإنشاء نمط تحديد الموقع الجغرافي استنادًا إلى عنوان بروتوكول الإنترنت (IP) لجهاز كمبيوتر المستخدم. وبالتالي إذا تم بشكل مفاجئ محاولة الوصول إلى حساب المستخدم في البنك من دولة أخرى، فقد يكون هذا مؤشرًا على وجود مهاجم بدلاً من المستخدم الحقيقي، وقد يطلب موقع الويب الخاص بالبنك نوعًا ثانيًا من المصادقة، مثل رمز يتم إرساله كرسالة نصية إلى رقم الهاتف المحمول الخاص بالمستخدم والمُسجل لديهم، قبل التمكن من مصادقة المستخدم.

تطبيق عملي (٤)

الهدف: أن يتعرف المتدرب على مدى قوة كلمات المرور الخاصة بهم. **الزمن:** ١٠ دقائق

يعمل المتدربون على فحص كلمات المرور الخاصة بهم وقياس مدى قوتها من خلال مواقع الويب المخصصة لذلك والتي يمكن الوصول إليها من خلال البحث في قوقل عن Password Checker، والتي تعمل على تحديد مدى إمكانية تعرض كلمة المرور للهجمات المُستهدفة لها.

الإرشادات:

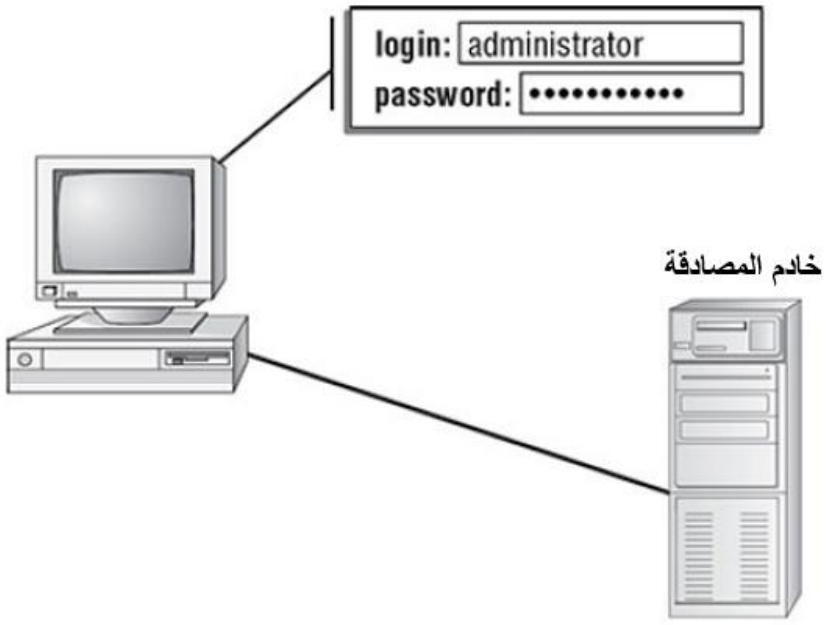
١. يقوم المتدربون بالدخول على الرابط التالي https://password.kaspersky.com/
٢. يقوم المتدربون بفحص كلمات المرور الخاصة بهم.
٣. يقوم المدرب بمناقشة النتائج مع المتدربين.

أنواع المصادقة:

تقوم الأنظمة بمصادقة بعضها البعض باستخدام طرق مماثلة، حيث تمرر الأنظمة المعلومات الخاصة بها بين بعضها البعض لإثبات الهوية. بمجرد حدوث المصادقة، يمكن لنظامين الاتصال بالطريقة الصحيحة حسب الامتيازات والصلاحيات المحددة لكل منهما. يتم استخدام العديد من الطرق الشائعة للمصادقة، وهي تقع تحت نطاق نوعين أساسيين: المصادقة الأحادية Single factor authentication والمصادقة المتعددة Multifactor authentication. حيث يقدم كلا النوعين مستوى معين من التعقيد وبالتالي تحديد مستوى الأمان المطلوب. (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- المصادقة الأحادية Single factor authentication:

تُعد المصادقة الأحادية على أنها الشكل الأساسي للمصادقة ويتم من خلالها التأكد من هوية المستخدم من خلال مطابقة آلية واحدة فقط من آليات المصادقة التي تطرقنا لها سابقاً، والتي غالباً ما تتم من خلال استخدام الآلية الأكثر شيوعاً والتي تتم من خلال فحص كل من اسم المستخدم وكلمة المرور ومطابقتهما مع المخزن مسبقاً في خادم المصادقة. حيث يعتبر اسم المستخدم وكلمة المرور معرّفات فريدة لعملية تسجيل دخول المستخدم. وبناءً على ذلك، فإن خطوات المصادقة الأحادية تتم من خلال طلب العنصر المراد تسجيل الدخول إليه (نظام – موقع ويب – جهاز كمبيوتر -شبكة) من المستخدم أن يُدخل اسم المستخدم الخاص به وكلمة المرور حتى يتم التحقق من الهوية. بعد ذلك، يتم إرسال قيم المعرفات عبر الاتصال الشبكي إلى خادم المصادقة كنص عادي أو مُشفر لزيادة مستوى الأمان كما هو موضح في شكل (١٧): *عملية تسجيل الدخول باستخدام اسم المستخدم وكلمة المرور*. وأخيراً، يقوم خادم المصادقة بمطابقة هذه القيم مع بالمعلومات المخزنة لديه مسبقاً، وبناءً على عملية المطابقة، يتم قبول محاولة تسجيل الدخول أو رفضها. كما يتم تحديد امتيازات أو أذونات المستخدم User Permissions بناءً على البيانات المخزنة حول معرف المستخدم المحدد.



شكل (١٧): *عملية تسجيل الدخول باستخدام اسم المستخدم وكلمة المرور.*

- المصادقة المتعددة Multifactor authentication:

تعتمد المصادقة المتعددة على تضمين آليتين أو أكثر من آليات التحقق من الهوية في عملية المصادقة الواحدة، وبالتالي فهي تعتبر أقوى أمنياً. كأن يتم الاعتماد في عملية المصادقة على إدخال اسم المستخدم وكلمة المرور (ماذا تعرف؟) كخطوة أولى على أن تليها خطوة تالية لإدخال كلمة مرور مؤقتة ترسل على الهاتف المحمول للمستخدم (ماذا لديك؟) أو التحقق من بصمة إصبعه (ماذا تملك؟). ولرفع مستوى الأمان، من المهم الإشارة إلى ألا تكون الآليات المستخدمة في عملية المصادقة من نفس الفئة.

التفويض أو الترخيص :Authorization

بعد أن تتم مصادقة المستخدم والتأكد من هويته، ننتقل إلى المرحلة الثانية من مراحل التحكم في الوصول وهي مرحلة التفويض أو الترخيص، والتي يتم من خلالها التأكد من أن المستخدم لديه الصلاحيات والأذونات التي تخوله من استخدام الموارد وتنفيذ العمليات بشكل صحيح ووفق المعايير المُنظمة لذلك والموضحة فيما يلي: (القحطاني، ٢٠١٥)

- منح الصلاحيات بناءً على دور المستخدم والمهام التي من المفترض أن يقوم بها، مثل تحديد صلاحيات المستخدم - بناءً على دوره-في الاطلاع على البيانات وقراءتها فقط، أم يتم رفع مستوى الصلاحيات بحيث يتم السماح له بالتعديل والحذف أيضاً.
- منح الصلاحيات بناءً على موقع المستخدم، حيث يمكن التحكم في الوصول إلى المورد من خلال عدم السماح بتسجيل الدخول إليه عن بعد، ويتم إلزام المستخدم بالتواجد في نفس المكان الذي يوجد في المورد الذي يرغب بالوصول إليه، مثل أن تقوم بعض المنظمات بإلزام موظفيها على الحضور إلى مقر العمل للدخول على الخوادم الرئيسية ومراكز البيانات، وذلك من أجل ضمان السيطرة المركزية على كافة العمليات التي تتم على المورد.
- منح الصلاحيات بناءً على أوقات محددة، حيث يمكن السماح للمستخدمين بتسجيل الدخول في أوقات أو تواريخ معينة، كأن يتم – على سبيل المثال-السماح بالدخول على نظام معين خلال أوقات الدوام الرسمي فقط.
- منح الصلاحيات بناءً على الإجراء أو العملية، بحيث يمكن التحكم في الوصول بناءً على العملية المراد القيام بها على البيانات، كأن يتم السماح بتعديل بعض البيانات دون غيرها أو التحكم في إظهار وإخفاء بعض حقول البيانات.

تجدر الإشارة بأن عملية التفويض أو الترخيص تعد من العمليات الحساسة التي يجب أن يتم تنفيذها بعناية، لأن تقييد الصلاحيات أو الأذونات بمعايير معقدة قد ينتج عنه عدم القدرة على الوصل للموارد أو المعلومات المطلوبة وفي الأوقات المناسبة وهذا مما يخل بعنصر التوافر (Availability) الذي يعد كأحد ركائز أمن المعلومات CIA. وفي المقابل، فإن ترك الموارد مفتوحة لأي مستخدم قد ينتج عنه ثغرات أمنية وبما يخل بعنصري السرية (Confidentiality) والنزاهة (Integrity). (القحطاني، ٢٠١٥)

المحاسبة أو المتابعة :Accounting

تهدف هذه العملية إلى متابعة دخول وعمليات المستخدمين على الأنظمة والموارد، وتسجيلها من أجل مراجعتها ومتابعتها لمعرفة في حال وجود أي خلل أو تجاوز للصلاحيات الممنوحة لكل مستخدم وذلك لاتخاذ الإجراءات المناسبة، مثل أن يتم حجب مستخدم بشكل نهائي أو حجب مورد معين عن جميع المستخدمين. (القحطاني، ٢٠١٥)

العنصر الثاني: إدارة التحكم بالوصول:

تحدد سياسة التحكم في الوصول أنواع الوصول المسموح بها وتحت أي ظروف ومن قبل المستخدمين من خلال إدارتها بطريقة معيارية وممنهجة. حيث إن هناك أربعة نماذج أساسية في إدارة التحكم في الوصول موضحة فيما يلي:

نماذج التحكم في الوصول:

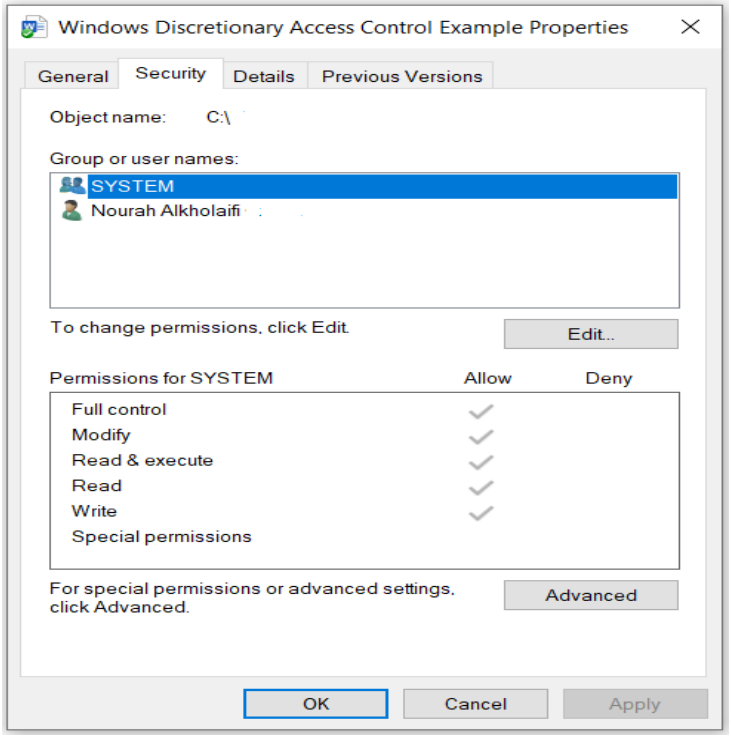
- التحكم في الوصول التقديري Discretionary access control (DAC):

يعتمد هذا النموذج على التحكم في الوصول استنادًا إلى هوية المستخدم وعلى قواعد الوصول (الصلاحيات أو الأذونات) التي توضح ما يُسمح وما لا يُسمح للمستخدمين القيام به.(Stallings, ٢٠١٩)

يُعد نموذج التحكم في الوصول التقديري (DAC) هو الأقل تقييدًا وذلك لاعتماده على ضوابط تقديرية، بمعنى أن الشخص الذي لديه إذن وصول معين قادر على تمرير هذا الإذن (ربما بشكل غير مباشر) إلى أي مورد آخر. باستخدام سياسة DAC، يكون لمنشئ المورد أو الملف (المالك Owner) السيطرة الكاملة على هذا المورد، وبالتالي يكون لمالك المورد السلطة التقديرية وحق الاختيار فيما يتعلق بمن يمكنه الوصول إلى موارده وملفاته. فعلياً، يتم استخدام DAC في العديد من أنظمة التشغيل مثل نظام ويندوز كما هو موضح في شكل (١٨): *التحكم في الوصول التقديري في نظام ويندوز*

حيث يمكن لمالك الملف منح الصلاحيات لغيره من المستخدمين.

على الرغم من أن DAC يوفر درجة عالية من الحرية، إلا أنه ينطوي على نقطتي ضعف هامتين. أولاً، أنه يعتمد على قرارات المستخدم في تحديد مستوى الأمان المناسب مما يشكل خطراً أمنياً حيث قد يتم منح أذونات بطريقة غير صحيحة. ثانياً، هي أن الصلاحيات والأذونات الممنوحة بهذا النموذج تكون موروثة بواسطة أي برامج يستخدم هذه المورد أو الملف.(Ciampa, ٢٠١٨)



شكل (١٨): *التحكم في الوصول التقديري في نظام ويندوز*

- التحكم في الوصول الإلزامي(Mandatory access control (MAC) :

يُعد نموذج التحكم في الوصول الإلزامي (MAC) هو الأكثر تقييدًا والتزاماً – على النقيض من DAC – حيث يعتمد MAC على تعيين ضوابط وصول المستخدمين بشكل صارم وفقًا لرغبات مسؤول النظام Administrator. وبالتالي، لا يكون للمستخدم الحرية في تعيين أي عناصر تحكم أو توزيع الوصول إلى الموارد والملفات الأخرى. يوجد هذا النموذج عادةً في الإعدادات العسكرية حيث يكون للأمن أهمية قصوى. (Ciampa, ٢٠١٨)

- التحكم في الوصول المبني على الأدوار (Role-based access control (RBAC:

يتم من خلال هذا النموذج التحكم في الوصول استنادًا إلى دور المستخدم، أي من خلال تحديد مجموعة صلاحيات الوصول التي يتلقاها المستخدم بناءً على تأديته لدور معين، حيث يمكن أن ينطبق دور معين على مستخدم واحد أو عدة مستخدمين. (Stallings, ٢٠١٩).

يعتبر نموذج RBAC من أكثر نماذج التحكم بالوصول القريبة من الواقع الفعلي للمنظمات، حيث يتم بموجب RBAC منح الصلاحيات بناءً على وظيفة عمل المستخدم الفعلية داخل المنظمة. وبناءً على ذلك بدلاً من تعيين أذونات لكل مستخدم، يقوم نموذج RBAC بتعيين الأذونات لأدوار معينة في المنظمة، ثم يقوم بتعيين المستخدمين لهذه الأدوار. كأن يتم على سبيل المثال تحديد صلاحيات (المدير Manager) ويتم بعد ذلك ربط جميع المدراء بنفس مستوى الأذونات. (Ciampa, ٢٠١٨)

- التحكم في الوصول المبني على القواعد (Rule-based access control (RB-RBAC:

يعتمد نموذج التحكم في الوصول المبني على القواعد -ويسمى أيضاً Control (RB- Rule-Based Role-Based Access RBAC) -على تعيين الأدوار ديناميكيًا للموارد بناءً على مجموعة من القواعد التي يحددها مسؤول النظام Administrator. حيث يحتوي كل مورد أو ملف على مجموعة من القواعد التي تحدد خصائص الوصول. فعندما يحاول المستخدم الوصول إلى هذا المورد، يتحقق النظام من القواعد الموجودة في هذا المورد لتحديد ما إذا كان الوصول مسموحًا به أم لا. غالبًا ما يتم استخدام هذا النموذج لإدارة وصول المستخدم إلى نظام واحد أو أكثر، حيث قد تؤدي التغييرات في الأعمال والإجراءات إلى تطبيق القواعد التي تحدد التغييرات المحتملة في إمكانية الوصول. على سبيل المثال، يريد مستخدم ما متصل من خلال الشبكة "أ" الوصول إلى الموارد الموجودة على الشبكة "ب "والمرتبطة على الطرف الآخر من الموجه Router. يحتوي الموجه هذا على مجموعة من قواعد التحكم في الوصول وبالتالي يمكنه تعيين دور معين للمستخدم، بناءً على عنوان الشبكة IP أو البروتوكول الخاص به، والذي سيحدد بناءً على ذلك ما إذا كان سيتم منحه حق الوصول أم لا. على غرارMAC ، لا يمكن للمستخدمين تغيير التحكم في الوصول المستند إلى القواعد. يتم التحكم في جميع أذونات الوصول بناءً على القواعد التي وضعها مسؤول النظام. (Ciampa, ٢٠١٨)

تطبيق عملي (٥)

الهدف: أن يطبق المتدرب نموذج التحكم في الوصول التقديري DAC. **الزمن:** ١٥ دقيقة

يعمل المتدربون على تطبيق نموذج التحكم في الوصول التقديري Discretionary Access Control (DAC) لتعديل صلاحيات ملفات المشاركة في نظام ويندوز.

الإرشادات:

١. يتم الدخول من خلال مستخدم Administrator على الويندوز.
٢. يقوم المتدربون بإنشاء ملف نصي باسم DAC.txt باستخدام برنامج Notepad.
٣. لاستعراض الأذونات Permissions الحالية للملف، ينقر بالزر الأيمن على الملف، ومن ثم اختيار Properties ومن ثم الذهاب إلى تبويب Security.
٤. يتم استعراض قائمة المستخدمين Users المنشأين مسبقاً على الكمبيوتر وفحص صلاحيات كل منهم.
٥. يتم الضغط على زر Edit، ومن ثم اختيار أحد المستخدمين وتعديل صلاحياته، من خلال منعه من قراءة الملف بواسط اختيار Deny لصلاحية القراءة Read.
٦. يتم الضغط على زر Apply واختيار Yes من خيارات الرسالة التنبيهية.
٧. يتم إغلاق نافذة التعديل بالضغط على OK واغلاق نافذة الخصائص بالضغط على Ok أيضاً.
٨. يتم تسجيل الخروج من مستخدم Administrator، وإعادة تسجيل الدخول على الويندوز من خلال حساب المستخدم الذي تم تعديل صلاحياته.
٩. يتم محاولة فتح الملف DAC.txt وملاحظة النتيجة.
١٠. يقوم المدرب بمناقشة النتائج مع المتدربين.

اليوم التدريبي الثالث

الموضوع الخامس: أمن الشبكات اللاسلكية

الموضوع السادس: الحوسبة السحابية

المخطط التدريبي لليوم الثالث

الجلسة الأولى

- (٨:٠٠:٩:٣٠)
- أمن الشبكات اللاسلكية.

استراحة (٩:٣٠:١٠:٠٠)

الجلسة الثانية

- (١٠:٠٠:١١:٣٠)
- الحوسبة السحابية(١).

استراحة (١١:٣٠:١٢:٣٠)

الجلسة الثالثة

- (١٢:٣٠:٢:٠٠)
- الحوسبة السحابية (٢).

الموضوع الخامس: أمن الشبكات اللاسلكية

تعتبر الشبكات والاتصالات اللاسلكية من أكثر التقنيات الحديثة تأثيراً على حياتنا في السنوات الأخيرة الماضية، نظرًا لأنه لم يعد من الضروري ارتباط أجهزتنا بالشبكات بواسطة الأسلاك. بفضل انتشار الشبكات اللاسلكية أصبح بإمكان المستخدمين تصفح مواقع الويب أو التحقق من البريد الإلكتروني أو تنزيل الملفات ومشاهدة مقاطع الفيديو من أي مكان تقريبًا وفي أي وقت، حيث أصبح الاتصال اللاسلكي بالإنترنت متوفر في أغلب الأماكن العامة على مستوى العالم، كالمدارس والجامعات والمطارات والفنادق والمطاعم. أما في بيئات العمل، فيمكن للموظفين الوصول إلى بياناتهم وخدماتهم عن بُعد أثناء الاجتماعات أو المؤتمرات، وبالتالي زيادة إنتاجيتهم بشكل أكبر. كما حفزت الشبكات اللاسلكية نمو العديد من التقنيات الجديدة الأخرى، مثل انتشار الأجهزة اللوحية المحمولة. (Ciampa, ٢٠١٨)

تؤكد الإحصائيات زيادة انتشار تقنية الشبكات اللاسلكية على مدى السنوات الأخيرة، حيث إنه قد تم تقدير عدد الأجهزة المتصلة بالشبكات اللاسلكية على مستوى العالم في عام ٢٠١٦ بحوالي ٨,٣٦ مليار جهاز، ولكن هذا العدد قد زاد بحوالي ثلاثة أضعاف في عام ٢٠٢١، حيث تم تقدير حوالي ٢٢,٢ مليار جهاز متصل بالشبكات اللاسلكية عالمياً. (https://www.statista.com/, ٢٠٢١)

ونظراً لهذا الانتشار، نما المعدل الشهري لحركة نقل البيانات من الأجهزة والهواتف المحمولة في عام ٢٠٢١ بمقدار سبعة أضعاف عما كان عليه في عام ٢٠١٦، حيث تجاوز حجم نقل البينات في الشبكات اللاسلكية عالمياً في عام ٢٠٢١ ما مقداره ٤٩ اكسابايت كل شهر (واحد اكسابايت يعادل مليار جيجابايت)، بينما كان المعدل الشهري في عام ٢٠١٦ يعادل ٧ اكسابايت فقط. (Cisco, ٢٠١٧)

الشبكات اللاسلكية Wireless Local Area Network(WLAN) عرضة لجميع الهجمات التي تتعرض لها الشبكات السلكية، بل إنها أضعف من الناحية الأمنية نتيجة اعتماد الشبكات اللاسلكية على الموجات الكهرومغناطيسية في نقل البيانات، حيث إنه يمكن اعتراض هذا النوع من الموجات بسهولة. بشكل عام، لا يتطلب اعتراض موجات الشبكات اللاسلكية -والتي تعتمد على بروتوكول IEEE ٨٠٢,١١ -إلا على جهاز كمبيوتر مثبت عليه كرت شبكة يدعم الاتصال اللاسلكي حتى يكون قادراً على التقاط الترددات المطلوبة. تعمل الشبكات اللاسلكية على الإعلان عن وجودها للمستخدمين من خلال بث اسمها بانتظام (المعروف باسم Service Set Identifier SSID Broadcasting)، ونتيجة لذلك يمكن للبرامج البسيطة الموجودة على جهاز الكمبيوتر التقاط حركة مرور الارتباط في نقطة الوصول اللاسلكية access point ثم معالجة هذه البيانات من أجل فك تشفير معلومات الحساب وكلمة المرور.(Emmett Dulaney and Chuck Easttom, ٢٠١٨)

ومع ذلك، هناك تطورات كبيرة في مجال أمن الشبكات اللاسلكية، لدرجة أن تكنولوجيا ومعايير الأمان اللاسلكي توفر اليوم للمستخدمين أمانًا يضاهي ما تتمتع به الشبكات اللاسلكية.

العنصر الأول: الهجمات المهددة للشبكات اللاسلكية:

تختلف الشبكات اللاسلكية WLAN اختلافاً جوهريا عن الشبكات السلكية LAN في كون الأولى غير مقيدة بحدود فيزيائية واضحة ونتيجة لذلك فهي تحتوي على نقاط دخول غير محددة، حيث إنه يكفي لجهاز المستخدم أن يكون في مجال التقاط الموجات الكهرومغناطيسية لإنشاء اتصال لاسلكي مع نقطة الوصول اللاسلكية access point والتي تعتبر مدخل المستخدم إلى الشبكة. في الشبكات اللاسلكية WLAN، تُنشِئ إشارات التردد اللاسلكي من نقاط الوصول عدة نقاط إدخال للبيانات إلى الشبكة، ويمكن من خلالها للمهاجمين تنفيذ الهجمات أو سرقة البيانات. بالإضافة إلى ذلك، نظرًا لأن إشارات التردد اللاسلكي تمتد إلى خارج حدود المبنى، فلا يمكن اعتبار الجدران بمثابة حاجز مادي لمنع المهاجمين من الوصول للشبكة. لا يزال بإمكان المهاجم -المتواجد خارج محيط للمبنى-بسهولة التقاط الإشارة اللاسلكية للتنصت على عمليات إرسال البيانات أو حقن البرامج الضارة، ويمكن لأي نقطة وصولaccess point لم يتم تعيين إعدادات الأمان الخاصة بها بشكل غير صحيح أن تسمح للمهاجمين بالوصول إلى الشبكة. وفيما يلي أهم أنواع الهجمات المهددة للشبكات اللاسلكية: (Ciampa, ٢٠١٨)

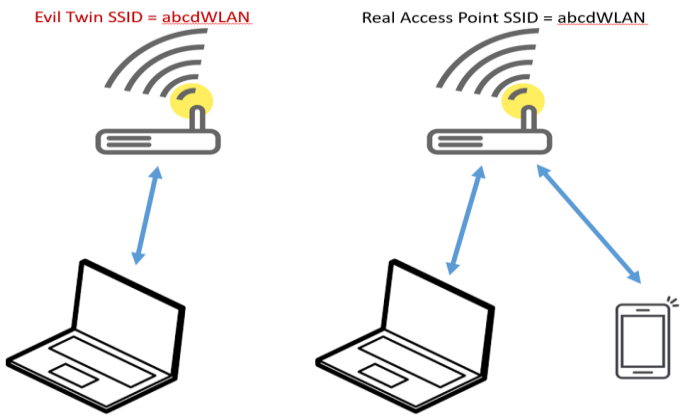
- نقطة وصول ضارة: Rogue Access Point:

يعتمد هذا الهجوم على وجود نقطة وصول غير مصرح بها في الشبكة غالباً ما يتم استحداثها من قبل المستخدمين الفعليين للشبكة بهدف توسيع نطاقها دون إعدادها بشكل جيد أمنياً مما يجعلها تتحول إلى ثغرة ممكن استغلالها، بحيث تسمح للمهاجمين بتجاوز العديد من الإعدادات الأمنية الخاصة بالشبكة، مما يتسبب وجودها في تعرض الشبكة ومستخدميها للهجمات.

لا يجب أن تكون نقاط الوصول الضارة عبارة عن أجهزة شبكة حقيقة، حيث إنه من الممكن إنشائها بشكل افتراضي. على سبيل المثال، يتيح نظام مايكروسوفت ويندوز خدمة الشبكة المضيفة اللاسلكية The wireless Hosted Network والتي تعمل على محاكاة البطاقة الشبكة اللاسلكية الفعلية (wireless NIC) إلى عدة بطاقات لاسلكية افتراضية (مما ينتج عنه شبكة Wi-Fi افتراضية) يمكن الوصول إليها عن طريق نقطة وصول لاسلكية برمجية (SoftAP) software-based wireless AP يتم انشائها. هذا يعني أنه يمكن بسهولة تحويل أي جهاز كمبيوتر إلى نقطة وصول ضارة. وتسمح بعض التطبيقات أيضاً بتحويل الهواتف الذكية إلى نقاط وصول.

- هجوم التوأم الشرير Evil Twin:

بينما يتم إعداد نقطة الوصول الضارة من قبل مستخدم داخلي، فإن التوأم الشرير هو عبارة عن نقطة وصول تم إعداده بواسطة مهاجم. بحيث يتم تصميم نقطة الوصول هذه لتقليد نقطة وصول سليمة ومعتمدة، لذا فإن جهاز المستخدم المحمول مثل الكمبيوتر المحمول أو الجهاز اللوحي سيتصل دون قصد بهذا التوأم الشرير كما هو موضح في شكل (١٩)، وبالتالي يتمكن المهاجم من التقاط البيانات المرسلة من المستخدمين.



شكل (١٩): التوأم الشرير

- هجوم إعادة الإرسال Reply Attack:

يحدث هذا النوع من الهجمات عندما يتمكن المهاجم من التقاط المعلومات عبر الشبكة اللاسلكية ثم يعمل على إعادة استخدامها بشكل خبيث لغرض آخر غير المقصود. كمثال على ذلك، عندما يتم إرسال معلومات تسجيل الدخول وكلمة المرور بين المستخدم وخادم المصادقة في أحد الأنظمة أو مواقع الويب. يمكن للمهاجم التقاط المعلومات وإعادة استخدامها لاحقًا. (Emmett Dulaney and Chuck Easttom, ٢٠١٨).

- حجب الخدمة في الشبكة اللاسلكية Wireless Denial of Service Attack:

نظرًا لأن الأجهزة اللاسلكية تعمل باستخدام الترددات الكهرومغناطيسية، فهناك احتمال وارد للتداخل والتشويش مع الترددات الأخرى. قد يكون الجهاز اللاسلكي نفسه في الشبكة مصدر تداخل للأجهزة الأخرى، ويمكن للإشارات الواردة من الأجهزة الأخرى أن تعطل الإرسال اللاسلكي في شبكة ما. ترسل عدة أنواع من الأجهزة موجات لاسلكية يمكن أن تسبب تداخلًا عرضيًا مع الشبكة اللاسلكية WLAN تشمل هذه أجهزة الميكروويف ومحركات المصاعد وآلات التصوير وأنواع من أنظمة الإضاءة الخارجية أو غرف التصوير الإشعاعي. كل ذلك قد يتسبب في حدوث أخطاء في الاتصال أو يمنعه تمامًا بين جهاز المستخدم اللاسلكي ونقطة الوصول.

يمكن للمهاجمين أيضًا استخدام تداخل الترددات للموجات اللاسلكية لإغراق طيف التردد اللاسلكي –أو تشويشه-بشكل متعمد وكافي لمنع الأجهزة من الاتصال بشكل فعال مع نقطة الوصول، وبالتالي يتسبب هذا الهجوم في وقف ارسال البيانات بين الأجهزة في الشبكة.

- هجمات الشبكات اللاسلكية المنزلية:

تعتبر الهجمات ضد الشبكات اللاسلكية المنزلية سهلة إلى حدٍ ما، وذلك لأن العديد من المستخدمين لا يقومون بضبط إعدادات الأمان بشكل صحيح على شبكاتهم اللاسلكية المنزلية. يواجه المستخدمون العديد من المخاطر والهجمات على شبكاتهم اللاسلكية غير الآمنة. حيث يمكن للمهاجمين القيام بما يلي: (Ciampa, ٢٠١٨).

- سرقة البيانات من على جهاز كمبيوتر متصل بشبكة لاسلكية منزلية.
- التقاط البث اللاسلكي للشبكة، حيث يمكن للمهاجم التقاط أسماء المستخدمين وكلمات المرور وأرقام بطاقات الائتمان والمعلومات الأخرى المرسلة عبر الشبكة اللاسلكية.
- زرع البرمجيات الخبيثة، حيث إنه في حال تمكن المهاجمين من اختراق جدار الحماية، فإنه يمكنهم حقن الفيروسات والبرامج الضارة الأخرى على الكمبيوتر.
- استغلال اتصال الشبكة بتنزيل محتوى مخالف للقوانين. في العديد من الحالات، تمكن المهاجمون من الوصول إلى جهاز كمبيوتر منزلي من خلال شبكة لاسلكية غير مؤمنه وقاموا بتنزيل ملفات غير قانونية على الكمبيوتر، ثم قاموا بتحويل هذا الكمبيوتر إلى خادم ملفات لنشر المحتوى.

نقاط الضعف الأمنية في الشبكات اللاسلكية:

يتضمن بروتوكول IEEE٨٠٢,١١ العدد من المعايير والتنظيمات الخاصة بالشبكات اللاسلكية، ولكنه لا يخلو أيضاً من بعض الثغرات التي من الممكن استغلالها للهجوم على الشبكة اللاسلكية، تتضمن هذه الثغرات ما يلي: (Ciampa, ٢٠١٨)

- بروتوكول الحماية Wired Equivalent Privacy (WEP):

وهو بروتوكول أمني في معايير IEEE٨٠٢,١١، تم تصميمه لضمان أن الأطراف المصرح لها فقط هي التي يمكنها عرض المعلومات المنقولة في الشبكة اللاسلكية وبطريقة مكافئة لمستوى الخصوصية المعتمد في الشبكات السلكية. يحقق WEP هذه السرية عن طريق تشفير المرسلة، بحيث يعتمد WEP على مفتاح سري مشترك لا يعرفه إلا الجهاز اللاسلكي ونقطة الوصول. يجب إدخال نفس المفتاح السري على نفطة الوصول وعلى جميع الأجهزة قبل حدوث أي عمليات إرسال، لأنه سيُستخدم لتشفير أي بيانات سيتم إرسالها وكذلك فك تشفير البيانات التي سيتم تلقيها.

بشكل عام يُعتبر بروتوكول WEP ضعيف من الناحية الأمنية. حيث أن المفتاح السري الذي يعتمد عليه في عملية التشفير يتراوح طوله بين ٦٤ بت أو ١٢٨ بت فقط، والذي يعتبر قصير نسبيا وبالتالي يسهل كسره.

- بروتوكول الحماية Wi-Fi Protected Access (WPA):

نظراً لضعف برتوكول الحماية WEP، ظهرت الحاجة إلى تطوير بروتوكول حماية أقوى أمنياً. لذلك ظهر بروتوكول الحماية Wi-Fi Protected Access (WPA) والذي كان أحد أهداف تصميمه هو التوافق مع بروتوكول WEP السابق دون الحاجة إلى استبدال شامل للأجهزة أو ترقيتها.

يتميز بروتوكولWPA بتوفيره مستوى أعلى من الحماية للشبكة اللاسلكية وذلك من خلال تنفيذه لعمليات المصادقة والتشفير باستخدام بروتوكول واحد وهو بروتوكول Temporal Key Integrity Protocol (TKIP)، والذي يعتمد في عملياته على مفتاح تشفير بطول ١٢٨ بت ويكون مختلف لكل حزمة من البيانات، مما يعني أنه ينشئ بشكل ديناميكي مفتاحًا جديدًا لكل حزمة. مما يجعل بروتوكول WPAأصعب اختراقاً من بروتوكول WEP. (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

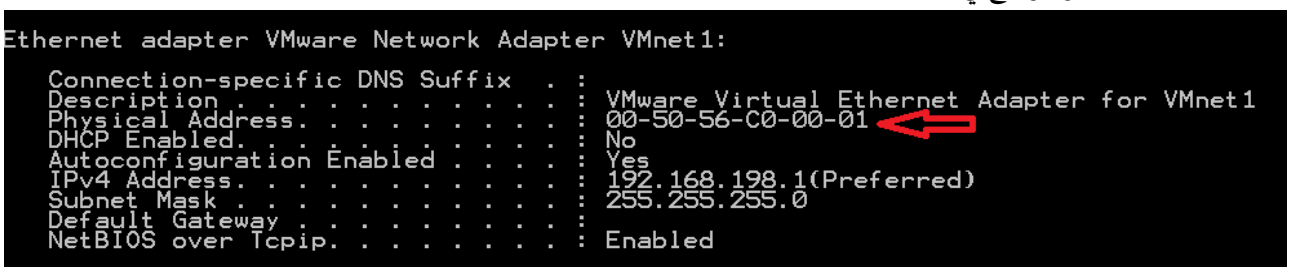
لم يكن WPA هو تصميم البروتوكول اللاسلكي الأكثر أمانًا. تم إجراء بعض التنازلات في تصميم الأمان للسماح بالتوافق مع مكونات الشبكة اللاسلكية الحالية. البروتوكولات لتحل محل TKIP قيد التطوير حاليا

ولكن لم يحقق بروتوكول WPAمستوى الأمان المطلوب في الشبكات اللاسلكية، نظراً للتركيز في تصميه على التوافق مع البرتوكولات السابق، لذلك تم تطوير بروتوكول WPA٢ كبديل أقوى من الناحية الأمنية لبروتوكول WPA. تم التركيز في تصميم WPA٢ على تطوير العديد من نقاط الضعف الموجودة WPA، وأبرزها الاعتماد على بروتوكول التشفير Advanced Encryption Standard (AES) block cipher بدلا عن بروتوكولTKIP . حالياً، أصبح بروتوكول WPA٢ – والإصدارات الأحدث منه -إلزاميًا لجميع أجهزة Wi-Fi الجديدة، كما أنه متوافق مع الإصدارات السابقة مع WPA، على الرغم من أن بعض بطاقات الشبكة القديمة تواجه صعوبة في استخدامه. (Michael E. Whitman, Herbert J. Mattord, ٢٠١٨)

- التصفية باستخدام العناوين الفيزيائية للأجهزة MAC Address Filtering:

تتمثل إحدى وسائل حماية الشبكات اللاسلكية WLAN في التحكم في الأجهزة المسموح لها بالاتصال بالشبكة. يهدف التحكم في الوصول اللاسلكي إلى تقييد دخول المستخدمين إلى الشبكة من خلال نقطة الوصول، بحيث يمكن فقط للأجهزة المصرح لهم الاتصال بنقطة الوصول وبالتالي يصبحون جزءًا من الشبكة المحلية اللاسلكية.

النوع الأكثر شيوعًا للتحكم في الوصول في الشبكات اللاسلكية هو التصفية باستخدام العناوين الفيزيائية للأجهزة MAC address، حيث يشكل العنوان الفيزيائي MAC address رمز فريد لبطاقات الشبكة NIC الموجودة على أجهزة المستخدمين (يمكنك معرفة العنوان الفيزيائي الخاص بجهاز الكمبيوتر من خلال الدخول على Command Prompt وتنفيذ الأمر ipconfig/all كما هو موضح في شكل (٢٠).



شكل (٢٠): العنوان الفيزيائي

يتم تصفية عنوان MAC كوسيلة للتحكم في الدخول للشبكة من خلال إعداد نقاط الوصول بعناوين MACالتي يُسمح لها – أو لا يُسمح لها-الاتصال بالشبكة. التصفية حسب عنوان MAC لديها العديد من نقاط الضعف. أولاً، في بداية الاتصال يتم تبادل عناوين MAC بين الأجهزة اللاسلكية ونقطة الوصول بإرسال غير مشفر. يمكن للمهاجم الذي يراقب الموجات اللاسلكية أن يرى بسهولة عنوان MAC الخاص بجهاز معين ثم يقوم بانتحاله بشكل متعمد على جهازه الخاص. ثانياً، أن إدارة عدة عناوين MAC يمكن أن تشكل تحدياً أمام مسؤول الشبكة نظرا لصعوبة إدارتها –نظراً لطبيعة هيكلتها – خاصة في ظل تزايد أعداد المستخدمين. كما أن عملية إضافة مستخدمين جدد إلى الشبكة أو حظر مستخدمين سابقين، يتطلب تتبع دقيق لعناوين MAC وبشكل دائم تقريبًا. لهذا السبب، لا تكون تصفية عناوين MAC عملية دائمًا في شبكة لاسلكية كبيرة وحيوية.

- إيقاف الإعلان عن الشبكة اللاسلكية SSID Broadcasting:

هناك وسيلة أخرى للتحكم في الوصول إلى شبكة لاسلكية من خلال تقييد الإعلان الدوري عن الشبكة. يعتبر SSID كاسم للشبكة يوفرها المستخدم لشبكة لاسلكية ويمكن عمومًا أن يكون أي سلسلة أبجدية رقمية تصل إلى ٣٢ حرفًا. على الرغم من أنه عادةً ما يتم بثSSID بشكل دوري بحيث يمكن لأي جهاز رؤيته، إلا أنه يمكن تقييد هذا البث. عندئذٍ لن يُسمح إلا للمستخدمين الذين يعرفون مسبقاً "SSIDالسري" بالوصول إلى الشبكة، بحيث يُطلب من المستخدم إدخال SSID بشكل يدوي على جهازه اللاسلكي. على الرغم من أن هذا قد يبدو آمناً بسبب عدم الإعلان المطلق عنSSID ، إلا أنه يوفر درجة ضعيفة من الحماية ولديه العديد من القيود:

- يمكن اكتشاف SSID بسهولة في حالة إرساله في حزم غير محمية من قبل نقطة الوصول.
- قد يؤدي إيقاف تشغيل بث SSID إلى منع المستخدمين من القدرة على التجول بحرية في منطقة تغطية نقطة وصول إلى أخرى.
- ليس من الممكن أو المناسب دائمًا إيقاف تشغيل إشارات SSID. إن إشارات SSID هي الوضع الافتراضي في كل نقاط الوصول تقريبًا، ولا تسمح جميع نقاط الوصول بإيقاف تشغيل بث SSID.

العنصر الثاني: الاحتياطات الأمنية للشبكات اللاسلكية:

لرفع مستوى أمان الشبكات اللاسلكية وللتقليل من تعرضها للهجمات التي تهددها، هناك مجموعة من الاحتياطات الأمنية التي من الواجب اتباعها كما يلي:

- التأكد من تغيير إعدادات اسم المستخدم وكلمة المرور الافتراضية على جميع الأجهزة اللاسلكية، حيث تقوم معظم الشركات المصنعة لأجهزة الشبكات بتعيين بيانات اسم المستخدم وكلمة المرور بشكل افتراضي لأجهزتها، وهذا مما يُمكن أن يُستغل من قبل المهاجم إذا تمّكن من معرفة نوع الجهاز مالم يتم تغييره من قبل المستخدم.
- إعداد الشبكة من خلال الاعتماد على بروتوكول الحماية WPA٢ (Wi-Fi Protected Access version ٢ or newer) والذي يوفر مستوى أكثر أمانا للبيانات، والذي يعتمد بدوره على معيار التشفير Advanced Encryption Standard (AES).
- الحرص على تحديث أجهزة الشبكات اللاسلكية وترقيتها بشكل مستمر.

أما على صعيد المستخدم فمن الأفضل قدر المستطاع تجنب الاتصال بشبكة لاسلكية مفتوحة والمتوفرة غالباً في الأماكن العامة. أما في حالا الاضطرار للاتصال بها، فيجب تجنب إجراء عمليات تسجيل أو دخول من خلالها على أحد مواقع الويب أو تنفيذ عمليات مالية إلكترونية.

تطبيق عملي (٦)

الهدف: أن يطبق المتدرب إعداد نقطة وصول Access Point لشبكة لاسلكية. **الزمن:** ١٥ دقيقة

يعمل المتدربون على تنفيذ إجراءات إعداد نقطة وصول Access Point لشبكة لاسلكية من خلال استخدام واجهة محاكاة متوفرة على الإنترنت من TRENDnet، لأن إعداد نقطة وصول بشكل صحيح تعتبر من المهارات المهمة لأي متخصص في الشبكات اللاسلكية وكذلك للمستخدمين.

الإرشادات:

١. يقوم المتدربون بالدخول على الرابط التالي والذي يوفر واجهة محاكاة Trendnet Emulators لإجراء الإعدادات الخاصة بنقاط الوصول في الشبكات اللاسلكية.
http://www.trendnet.com/emulators/TEW-٨١٨DRU_v١/login.htm
٢. ستظهر شاشة تسجيل الدخول على Trendnet Emulator. انقر فوق Login دون إدخال اسم المستخدم أو كلمة المرور. يتم عرض شاشة إعداد تحاكي ما قد يراه المستخدم عند إعداد نقطة وصول فعلية.
٣. تأكد من تحديد علامة التبويب "Basic" في الجزء الأيسر من الشاشة. استعرض معلومات الشبكة الحالية والظاهرة على الشاشة.
٤. انقر فوق "Wireless" في الجزء الأيسر من الشاشة واستعرض الإعدادات الموجودة.
٥. ضمن حقل Broadcast Network Name (SSID)، ما هو الخيار الافتراضي؟ ماهي الخيارات الأخرى الممكنة؟
٦. يوجد ضمن إعدادات "Security Policy" حقل واحد فقط وهو "Security Mode". ما هو الاختيار الافتراضي؟ هل يوفر حماية مناسبة؟
٧. ضمن إعدادات "WPA"، ما هو خيار التشفير الموجود في "WPA Encryption"؟ وما هي الخيارات الأخرى المتاحة؟
٨. ما هي كلمة المرور الافتراضية والمُتضمنة في حقل "WPA passphrase"؟ قيم مدى قوة كلمة المرور المحددة؟
٩. في الجزء الأيسر من الشاشة، انقر فوق "Guest Network". تتيح لك هذا الجزة من الواجهة إعداد شبكة إضافية مفتوحة للمستخدمين المؤقتين فقط والتي لا تؤثر على الشبكة اللاسلكية الرئيسية. ما مزايا وعيوب هذا النوع من الشبكات؟
١٠. لاحظ الخيار الموجود ضمن "Internet Access Only". ماهي ميزة تحديد هذا الخيار؟
١١. في الجزء الأيسر من الشاشة، انقر فوق "Advanced."، ثم انقر فوق "Security".
١٢. ضمن خيارات "Access Control"، ما هي وظيفة "LAN Client Filter Function" بناءً على الإعدادات المعروضة على الشاشة؟
١٣. يقوم المدرب بمناقشة النتائج مع المتدربين.

العنصر الثالث: الشبكات الافتراضية الخاصة VPN:

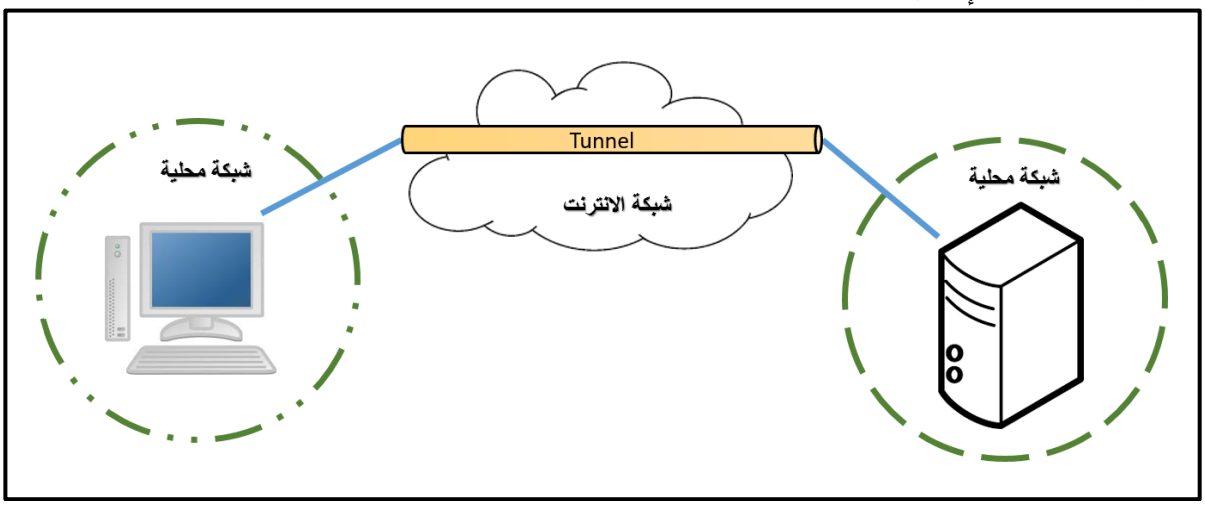
مع انتشار استخدام شبكة الإنترنت، زادت الحاجة إلى النظر في إمكانية استخدامها لنقل البيانات الحساسة والسرية من خلالها مع كونها شبكة عامة وغير آمنة، حيث يحتاج المستخدمين من أي مكان في العالم إلى الاتصال بالشبكات المحلية في جهات عملهم، كما تحتاج المنظمات إلى ربط شبكات فروعها المنتشرة حول العالم ببعضها البعض، فكان الحل من خلال إنشاء خطوط اتصال خاصة وآمنه بين طرفين باستخدام الشبكة العامة للإنترنت، وهو ما يعرف بالشبكة الافتراضية الخاصة VPN.

الشبكات الافتراضية الخاصة (VPN) :Virtual Private Network

تعرف الشبكة الافتراضية الخاصة Virtual Private Network (VPN) على أنها شبكة خاصة لنقل البيانات ولكنها تستخدم البنية التحتية لشبكة عامة –مثل الانترنت-وذلك بهدف إنشاء وسيلة اتصال خاصة عبر استخدام بروتوكول نقل نفقي Tunneling Protocol مُدعم بإجراءات أمنية. (Michael E. Whitman, Herbert J. Mattord, ٢٠١٨).

وبالتالي تعتبر VPN كتقنية تمكن المستخدمين المصرح لهم من استخدام شبكة عامة غير آمنة، مثل الإنترنت، كما لو كانت شبكة خاصة آمنة. ويتم ذلك عن طريق تشفير جميع البيانات التي يتم إرسالها بين طرفي الاتصال. حيث يقوم أساس عمل الشبكة الافتراضية الخاصة VPN على بناء نفق افتراضي خاص "VPN Tunnel" بين طرفي الاتصال كما هو موضح في شكل (٢١)، ويتم تبادل البيانات من خلال هذا النفق، حيث يُعَبِر النفق عن آلية لتغليف البيانات وإرسالها في مسار محدد على شبكة الإنترنت بحيث تكون غير مرئية من قبل الأطراف غير المصرح لها بالاطلاع عليها. (القحطاني، ٢٠١٥)

طرفي الاتصال هما عبارة عن طرفي النفق في أجهزة VPN، حيث يمكن أن يكون أحد الأطراف عبارة عن برنامج على جهاز كمبيوتر محلي، أو جهاز قائم بحد ذاته مخصص لتجميع مئات أو آلاف من اتصالات VPN مثل جهاز VPN concentrator، أو مدمج في جهاز شبكة آخر مثل جدار الحماية، وبالتالي تعمل هذه الأطراف باختلاف أنواعها على التعامل مع جميع إعدادات VPN من تغليف البينات وتشفيرها وإرسالها. (Ciampa, ٢٠١٨)



شكل (٢١): *الشبكة الافتراضية الخاصة VPN*

للشبكات الخاصة الافتراضية مجموعة من المزايا تتلخص فيما يلي: (القحطاني، ٢٠١٥)

- سهولة توسع الشبكة مستقبلا Network Scalability.
- سهولة إضافة مستخدمين وحذفهم، كما تتمتع بسهولة إضافة الفروع وحذفها.
- غير مكلفة.
- تحقيق حد مقبول من أمن المعلومات، من خلال توفير الخصوصية لخطوط الاتصال، مقارنة بمستوى الأمان المتدني في الإنترنت.

ولكن على النقيض، تحتوي الشبكات الخاصة الافتراضية على مجموعة من العيوب كما يلي: (القحطاني، ٢٠١٥)

- تحتاج إلى تطبيق معايير أمنية أكثر صرامة.
- يتأثر أداؤها بكفاءة أداء شبكة الإنترنت، والذي لا يمكن التنبؤ به.

أمن الشبكات الافتراضية الخاصة VPN:

نظرا لأن شبكة الإنترنت هو الناقل الحقيقي للشبكات الافتراضية الخاصة، والتي تعتبر بيئة غير أمنة لنقل البيانات، فيجب توفير الحماية اللازمة عند إعداد شبكات VPN بحيث نضمن تحقيق عناصر أمن المعلومات الثلاثة CIA، وذلك من خلال ما يلي: (القحطاني، ٢٠١٥).

- التحقق من هوية الأطراف المرسلة والمستقبلة بأحد آليات التحقق من الهوية المناسبة لذلك.
- تحقيق السرية أو الخصوصية من خلال تشفير البيانات بما يضمن أن يتم تبادل المعلومات بشكل سري ولا يطلع عليها إلا الأشخاص المصرح لهم بذلك.
- سلامة البيانات وتكاملها من خلال تطبيق البصمة الرقمية والتي تضمن عدم التغيير في البيانات أثناء نقلها في شبكة VPN.
- استخدام التوقيع الرقمي لضمان عدم إنكار طرفي الاتصال علاقتهم بالبيانات المرسلة.

الموضوع السادس: الحوسبة السحابية

في الحوسبة السحابيةCloud computing ، يتم تخزين البيانات والبرامج ومشاركتها والوصول إليها عبر شبكة الإنترنت من أي مكان وفي أي وقت باستخدام أي جهاز إلكتروني ممكن، وبسعات تخزينية لا محدودة وسرعة وصول عالية جداً. وتمثل بديلاً أحدث للطرق التقليدية التي تعتمد على الأجهزة وخوادم والشبكات المحلية والتي تعتبر محدودة بسرعات وسعات تخزينية معينة، ومقيدة بآلية وصول محددة. (حيان، ٢٠١٩).

العنصر الأول: تعريف الحوسبة السحابية:

ويعرّف المعهد الوطني للمعايير والتقنية (NIST) الحوسبة السحابية بأنها "عبارة عن نموذج يهدف إلى تمكين الوصول إلى الشبكة الحاسوبية، بناءً على طلب المستفيد، بشكل مريح ومن أي مكان، حيث يوجد تجمُّع مشترك من الموارد الحاسوبية المجهزة (على سبيل المثال لا الحصر: الشبكات، والخوادم، وأماكن التخزين، والتطبيقات، والخدمات الإلكترونية)، التي يمكن توفيرها ونشرها بأقل جهد إداري ممكن، وبدون تدخُّل من مزود الخدمة" (حيان، ٢٠١٩)

لذلك، يتم استخدام مصطلح السحابة عادةً ليشير مجازاً إلى استخدام الإنترنت؛ كون الإنترنت تمثل مرتكزاً أساسياً لعمل السحابة. فعندما نقوم بتخزين البيانات أو تشغيل أحد البرامج من على القرص الصلب الموجود في جهاز الكمبيوتر، فإن ذلك يُسمَّى تخزيناً وحوسبة محلية. بينما ليتم اعتبار هاتين العمليتين نمطين من أنماط الحوسبة السحابية، نحتاج إلى الوصول للبيانات وتشغيل البرامج عبر الإنترنت. وعلى الرغم من أن النتيجة النهائية هي نفسها في كلتا الحالتين، إلا أن الاتصال عبر الإنترنت أو السحابة يسهم بشكل مباشر في إنجاز الأعمال في أي وقت، ومن أي مكان، وباستخدام أي جهاز إلكتروني مناسب. (حيان، ٢٠١٩)

من الممكن وصف الحوسبة السحابية على أنها عبارة عن "تجمُّع ضخم من الموارد الحاسوبية الافتراضية والقابلة للاستخدام والوصول السهل (كالتجهيزات المادية، والمنصات التطويرية، والخدمات الإلكترونية). ويمكن أن يتم تجهيز هذه الموارد وإعادة تخصيصها لتتكيف مع احتياجات أو أحمال تقنية متغيرة؛ الأمر الذي يسمح بالانتفاع بشكل أمثل –وأكثر كفاءة-من هذه الموارد. ويتم الاستفادة من هذا التجمُّع من الموارد الحاسوبية ليعمل بمبدأ الدفع حسب الاستخدام pay-as-per-use، والذي يوفّر ضمانات بأن يقوم مزود خدمة الحوسبة السحابية على تقديم اتفاقيات مستوى خدمة (SLAs) تتناسب وحاجة المستفيد."

يتطلب عمل الحوسبة السحابية، أن يجهز مزودو الخدمة السحابية بنيةً تحتيةً تشمل مختلف الموارد الحاسوبية التي يحتاجها المستفيدون من الخدمة لإنجاز أعمالهم؛ كأنظمة التشغيل، والشبكات الحاسوبية، وخوادم التخزين، والبرمجيات والتطبيقات، وآليات الوصول الآمنة والمرنة، بحيث تصبح الخدمات السحابية جاهزة للاستخدام المباشر عبر الإنترنت في أي وقت ومن أي مكان من خلال أي جهاز إلكتروني متصل بالإنترنت. (حيان، ٢٠١٩)

أنواع السحابات في الحوسبة السحابية:

هناك أربعة أنواع من السحابات المقدمة لتقديم خدمات الحوسبة السحابية، هي: السحابة الخاصة، والسحابة العامة، والسحابة المجتمعية، والسحابة الهجينة، ومن الممكن توضيح كل منها كما يلي: (حيان، ٢٠١٩).

- السحابة الخاصة Private Cloud:

من خلال السحابة الخاصة، يكون استخدام موارد السحابة حكراً على منظمة واحدة فقط، والتي يكون لها في الغالب عدة وحدات إدارية متفرقة في عدة مواقع جغرافية. وتتصل جميع هذه الوحدات الإدارية ببعضها البعض عن طريق شبكة حاسوبية مناسبة (كالإنترنت)، ويتم الوصول للموارد الحاسوبية بشكل مرن وآمن يسهل معه مشاركة البيانات والتطبيقات الخاصة بالمنظمة. ويمكن أن يتم امتلاك وإدارة وتشغيل البنية التحتية للموارد الحاسوبية بواسطة المنظمة نفسها أو بواسطة طرف ثالث، ومن الممكن أن يتم امتلاك الموارد من قبل مزود الخدمة على أن يكون التحكم والإدارة من خلال المنظمة. أمّا فيما يتعلق بموقع الموارد الحاسوبية للسحابة الخاصة، فيمكن أن يكون متواجد داخل المنظمة في مركز البيانات الخاص بها، أو موجود خارجها وتكون الموارد مملوكة لطرف ثالث، على الرغم من أن هذا النوع يوفر أعلى مستوى من الأمان والتحكم، إلا أنه يعتبر مكلف إلى حد ما.

- السحابة العامة Public Cloud :

في السحابة العامة، يتم فتح استخدام موارد السحابة من قبل مستخدمين مختلفين، بحيث يتم مشاركة هذه الموارد بناءً على طلب المستخدم واحتياجه. ويمكن أن تعود ملكية هذه الموارد ومسؤولية إداراتها وتشغيلها إلى منظمات خاصة أو حكومية أو أكاديمية. أما فيما يتعلق بموقع الموارد المُشَكلة للبنية التحتية للسحابة العامة، فإنها تكون لدى مزود خدمة الحوسبة السحابية.

- السحابة المجتمعية Community Cloud :

بالنسبة للسحابة المجتمعية، يكون استخدام موارد السحابة محصوراً على عدة منظمات أو أفراد يتشاركون في نفس الاهتمام أو الأهداف (كتوفُّر متطلبات أمنية معينة، أو أداء مهام محددة، أو تطبيق سياسات معينة). ويمكن أن يتم امتلاك وإدارة وتشغيل الموارد الحاسوبية للبنية التحتية للسحابة بواسطة هذه المنظمات أو بواسطة طرف ثالث. أما فيما يتعلق بموقع هذه الموارد، فيمكن أن يكون موجوداً داخل المنظمات ذات العلاقة أو متواجداً خارجها بحيث تتبع لطرف ثالث. وأفضل مثال على هذا النوع من الحوسبة السحابية، هو السحابة الحكومية في المملكة العربية السعودية (ديم) والتي توفر مجموعة واسعة من الموارد الحاسوبية التي تكون مخصّصة فقط للأجهزة والجهات والهيئات الحكومية، حيث تمثل هذه السحابة إحدى مبادرات برنامج التعاملات الحكومية "يسّر" لإنشاء سحابة حكومية مقتصر استخدامها على الأجهزة الحكومية في المملكة.

- السحابة الهجينة Hybrid Cloud:

يتكون هذا النوع من أنواع الحوسبة السحابية من اثنين أو أكثر من أنواع السحابات السابق ذكرها، بحيث تكون البنية التحتية لكل نوع مستقلة عن النوع الآخر، لكن ترتبط مع بعضها البعض عبر قناة اتصال مشفرة تسمح بنقل وتبادل البيانات وتشغيل التطبيقات والخدمات الإلكترونية فيما بينها. كما أنّ استقلالية كل نوع من السحابات المرتبطة يسمح للمستخدم أن يقوم بتخزين بياناته الخاصة على السحابة الخاصة، وفي الوقت نفسه يستغل الخدمات التي يتم توفيرها في السحابة العامة كتشغيل تطبيقات أو خدمات إلكترونية والاستفادة منها بمقابل مادي مقبول.

العنصر الثاني: نماذج خدمات الحوسبة السحابية:

يتيح مزودو الحوسبة السحابية خدماتهم بناءً على نماذج مختلفة، ولكن يعد أشهر هذه النماذج هو النموذج المعياري الذي يقدّمه المعهد الوطني للمعايير والتقنية National Institute of Standards and Technology (NIST)، يتكون هذا النموذج من ثلاث طبقات رأسية على النحو التالي: طبقة البرمجيات كخدمة(SaaS –Software as a Service) ، وطبقة المنصة كخدمة (PaaS – Platform as a Service)، وطبقة البنية التحتية كخدمة(IaaS – Infrastructure as a Service) .

وفيما يلي يتمُّ إعطاء بعض التفاصيل عن كل واحد من هذه النماذج الثلاثة. وسيتم توضيح كل منها كما يلي: (حيان، ٢٠١٩).

- طبقة البرمجيات كخدمة Software as a Service- SaaS:

يتيح هذا النموذج للمستخدم إمكانية الوصول إلى التطبيقات البرمجية واستخدامها، والتي يملك هذه التطبيقات هو مزود الخدمة، بحيث يتم تشغيل هذه التطبيقات على بنية تحتية سحابية تخصُّ مزود الخدمة ويقوم على إدارتها، وتشتمل البينة التحتية في هذه الحالة على الشبكة الحاسوبية، والخوادم، وأنظمة التشغيل، والتخزين. كما يمكن في هذا النموذج أن يتم الوصول إلى الخدمات المتاحة عبر أجهزة إلكترونية متعددة من خلال واجهة بسيطة للمستخدم مثل تشمل مستعرضَ الويب أو عبر واجهة برنامج معين. ولا يمكن للمستخدم في هذا النموذج الإدارة أو التحكم في موارد البنية التحتية للسحابة، ومن الأمثلة على تطبيقات البرمجيات كخدمة: خدمة Dropbox أو استخدام تطبيقات إدارة علاقات المستفيدين (Customer relationship management) عبر الإنترنت أو تطبيقات ذكاء الأعمال.

- طبقة المنصة كخدمة Platform as a Service- PaaS:

يتيح هذا النموذج للمستخدم إمكانية تهيئة وتطوير ونشر برمجياته الخاصة به من خلال السحابة، بحيث تعمل على منصة محوسبة يمتلكها ويستضيفها مزود الخدمة، وتشمل – على سبيل المثال – أنظمة التشغيل(OSs) ، وبيئات تطوير وتنفيذ التطبيقات البرمجية وأنظمة قواعد البيانات. ويتم من خلال هذه الطبقة تخصيص هذه الموارد أو جزء منها بناءً على طلب المستخدم وحسب احتياجاته، حيث يتم تشغيلها عبر الإنترنت دون الحاجة لأن يقوم المستخدم بتنزيل وتثبيت هذه الأنظمة على أجهزة الكمبيوتر المحلية الخاصة به. في هذا النموذج، تعود مسؤولية التحكم وإدارة البنية التحتية السحابية ومواردها إلى مزود الخدمة وليس المستخدم، لكن يمكن المستخدم أن يتحكم في تطبيقاته البرمجية التي يقوم بنشرها، وفي الإعدادات الخاصة بالبيئة التطويرية لهذه التطبيقات.

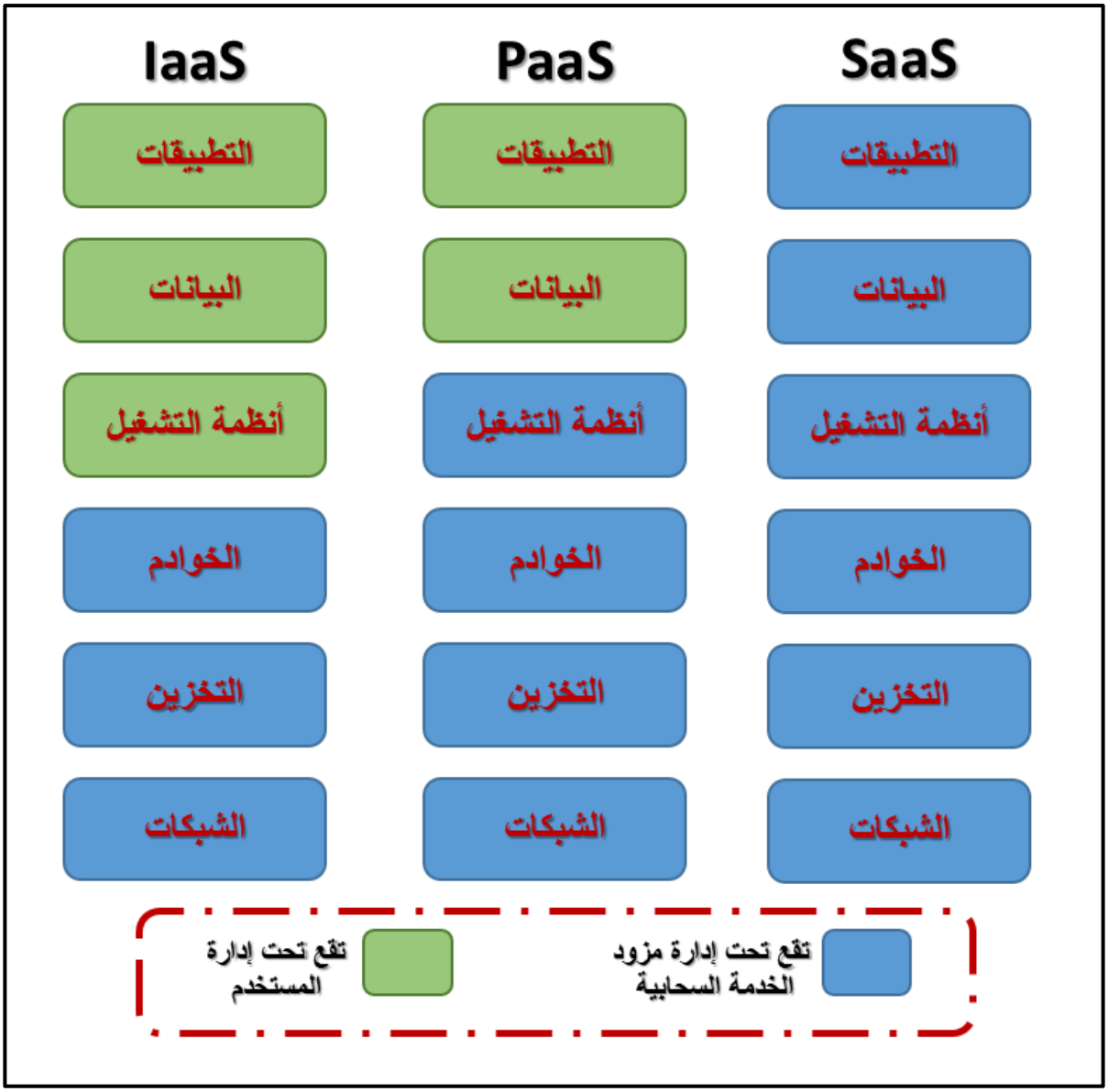
ومن الامثلة على هذا النموذج، خدمة محرك تطبيقات قوقل (Google App Engine)، وهو عبارة عن منصة حوسبة سحابية يتم استخدامه لتطوير واستضافة تطبيقات الويب في مراكز البيانات الخاصة بقوقل والمنتشرة في أماكن متفرقة من العالم. كما ان ويندوز أزور (Windows Azure) هو مثال آخر على المنصة كخدمة (PaaS)، والتي تعمل بشكل مشابه لمحرك تطبيقات قوقل كما إنها تقوم بعرض خدمة إضافية متمثلة في البنية التحتية كخدمة حسب حاجة العميل.

- طبقة البنية التحتية كخدمة Infrastructure as a Service- IaaS:

يتيح هذا النموذج للمستخدم إمكانية الاستفادة من العمليات الحاسوبية الأساسية، سواء اكانت مادية أم افتراضية، كالمعالجة والتخزين، وكذلك الاستفادة من البنية التحتية كالشبكات والخوادم، من قِبل مزود الخدمة، كما يتيح هذا النموذج للمستخدم مستوى أعلى من الإدارة والتحكم في البنية التحتية التي يتيحها مزود الخدمة مقارنة بالنموذجين السابقين، ويشمل ذلك التحكم في أنظمة التشغيل التي يريدها ويخصصها المستخدم، والتحكم في خوادم التخزين والتطبيقات البرمجية التي تعمل عليها، ولكنه يتيح مستوى أقل في التحكم في مكونات الشبكة (كالجدران النارية). كما يمكن للمستخدم التوسُّع في مستويات وكميات هذه

المكونات بالزيادة أو التخفيض بناءً على متطلباته. ويبقى أمر الإشراف والاستضافة والصيانة والترقية لكل هذه الموارد من مسؤولية مزود الخدمة؛ مما يتيح للمستخدم التركيز على إنجاز مهامه فقط. ومن الأمثلة على خدمات البنية التحتية كخدمة (IaaS): خدمة أمازون السحابية (Amazon Web Services – AWS) وخدمة سيسكو ميتابود (Cisco Metapod)، وخدمة مايكروسوفت أزور (Microsoft Azure)، وخدمة محرك الحوسبة من قوقل (Google Computer Engine – GCE).

ويمكن تلخيص الفروقات بين الطبقات الثلاثة في شكل (٢٢) من ناحية المسؤولية الأمنية الواقعة على المستخدم ومزود الخدمة السحابية.



شكل (٢٢): *الفروقات بين نماذج الخدمات السحابية.*

أسئلة ونقاش (٢)

الهدف: أن يميز المتدرب بين نماذج خدمات الحوسبة السحابية. **الزمن:** ١٠ دقائق

بناءً على نماذج خدمات الحوسبة السحابية المذكورة سابقاً، تعمل العديد من الشبكات العالمية بإطلاق العديد من الخدمات في مجال الحوسبة السحابية على اختلاف أنواعها وطبقاتها. وعلة المستخدم أن يبحث عن الخدمة المناسبة له.

الإرشادات:

١. يقوم المتدربون بشكل فردي باستخدام الإنترنت للبحث عن أنواع الخدمات السحابية الموجودة في الجدول وتصنيفها إلى SaaS –PaaS - IaaS.

٢. يقوم المدرب بمناقشة النتائج مع المتدربين.

جدول (٨): تصنيف *أنواع الخدمات السحابية*.

الخدمة	تصنيفها
خدمة iCloud من شركة Apple	
خدمة WebEx من شركة Cisco	
خدمة Google Compute Engine من شركة Google	
خدمة Google App Engine من شركة Google	
خدمة Gmail من شركة Google	
خدمة Microsoft Hyper-V من شركة Microsoft	
خدمة Office ٣٦٥ من شركة Microsoft	

العنصر الثالث: البيئات الافتراضيةVirtualization Environments :

من الصعوبة أن نتطرق لموضوع الحوسبة السحابية دون الحديث عن البيئات الافتراضية والتي تعتبر من المفاهيم المكملة لتقنية الحوسبة السحابية. أحد أسباب انتشار المحاكاة الافتراضية هو أنه من أجل الحصول على خدمات الحوسبة السحابية، يجب أن يكون لدى المستخدم محاكاة افتراضية، حيث أن الأساس الذي تُبنى عليه الحوسبة السحابية هو تجريد وتحرير العتاد Hardware في الكمبيوتر وإتاحته للأجهزة الافتراضية والذي يتم تحقيقه من خلال استخدام برامج مراقبة الأجهزة الافتراضية Hypervisor. (Emmett Dulaney and Chuck Easttom, ٢٠١٨).

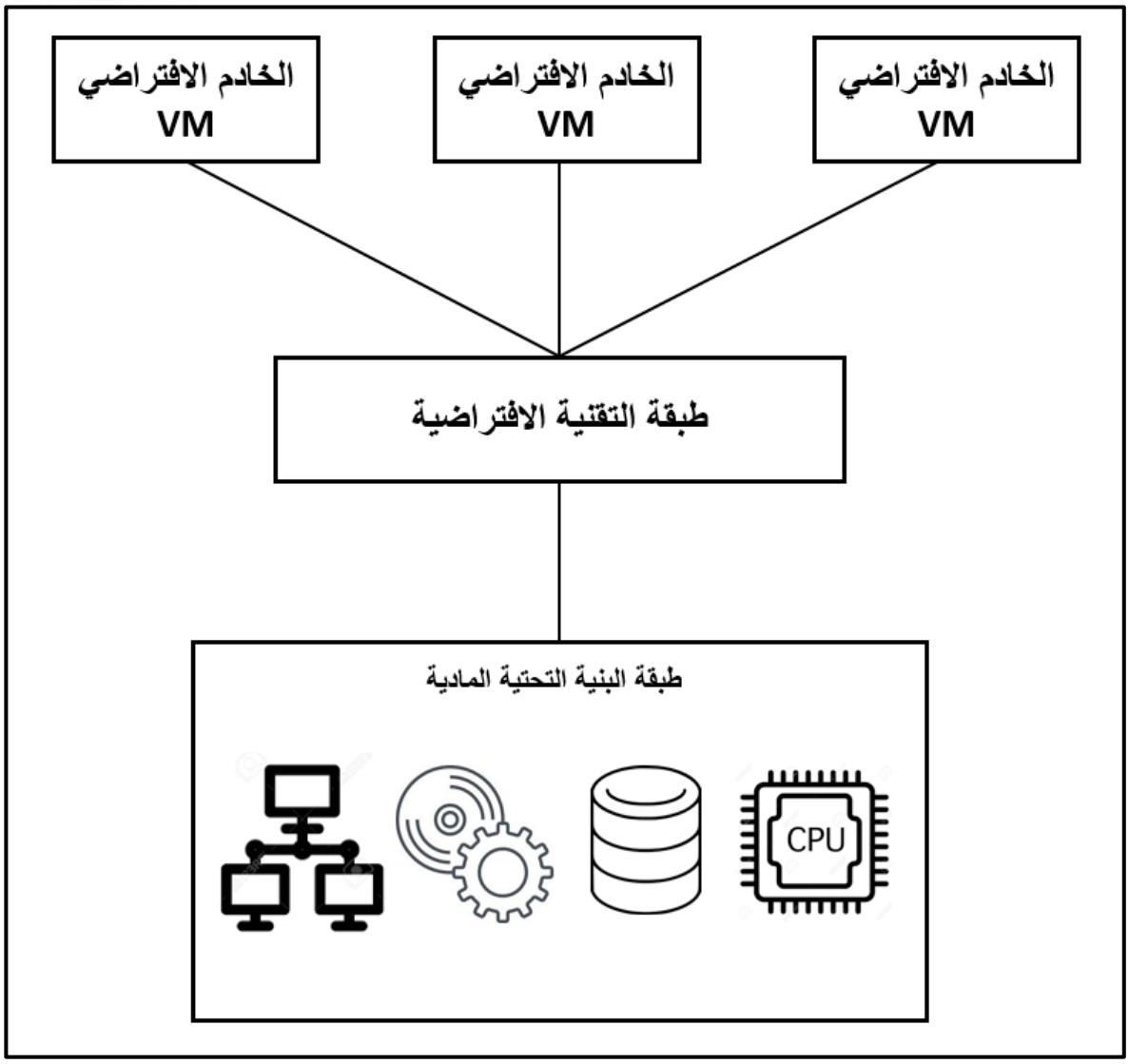
التقنية الافتراضية:

تُعرف التقنية الافتراضية على أنها تقنية برمجية تخفي تفاصيل الموارد التقنية المادية المتاحة من تجهيزات مادية Hardware وبرمجيات Software، فتظهر للمستخدم وكأن المورد المادي الواحد كالخادم ووسيط التخزين عبارة عن عدة موارد تقنية منطقية، كما تُظهِر مجموعة موارد تقنية مادية وكأنها مورد تقني منطقي وحيد. وتهدف التقنية الافتراضية على زيادة الانتفاع من القدرات الموارد التقنية غير المستغلّة، وتسمح بمشاركة نفس المورد التقني بين العديد من المستخدمين، ومن ثمّ توفير استهلاك الطاقة وزيادة العائد الاستثماري بالنسبة لمزود الخدمة، إضافة إلى تسهيل إدارة الموارد المخصصة للمستخدمين. ويمكن تطبيق التقنية الافتراضية على موارد تقنية متعددة، مثل: المعالجات، والذاكرة الرئيسية، ووسائط التخزين، والشبكات، والبيانات، والتطبيقات. (حيان، ٢٠١٩).

أنواع الموارد الافتراضية:

تعتبر التقنية الافتراضية إحدى الوسائل الأساسية لتفعيل الخصائص الأساسية للحوسبة السحابية من خلال قدرتها على تحويل الموارد التقنية الفعلية إلى موارد افتراضية. ولكن تحتاج التقنية الافتراضية إلى بيئة معينة للعمل من خلالها، حيث تتكون هذه البيئة –كما هو مبين في(٢٣) من ثلاث طبقات رئيسية: (حيان، ٢٠١٩)

- بنية تحتية تقنية، تشتمل على جميع الموارد المادية الفعلية التي يمكن تطبيق التقنية الافتراضية عليها، مثل: المعالجات، والذاكرة الرئيسية، ووسائط التخزين، والشبكات الحاسوبية، وبرمجيات التطبيقات، وأسطح المكتب.
- برمجية التقنية الافتراضية، والتي تسمى غالباً Hypervisor. يتم تنصيب هذه البرمجية على خادم فعلي يسمى بالمستضيف؛ مما يمكّنها من الوصول مباشرةً إلى طبقة البنية التحتية الفعلية. تتمثل المهمة الرئيسية لهذه البرمجيّة في إدارة الخوادم الافتراضية بشكل عام. يتم ربط Hypervisor غالباً بخادم فعلي، لكن يمكنه إنشاء عدة نسخ من الخوادم الافتراضية تكون مرتبطة بنفس الخادم الفعلي، ولكنها تكون مستقلة عن بعضها البعض افتراضياً. يستطيع Hypervisor تخصيص عدة موارد افتراضية لكل خادم افتراضي يقوم بإنشائه. كما يستطيع Hypervisor التحكم في زيادة وتخفيض مستوى الموارد الممنوحة لكل خادم افتراضي، أو إيقافه وتشغيله.
- خوادم افتراضية Virtual Machines (VM) يتم انشائها من خلال برمجية التقنية الافتراضية. حيث يُحاكي كل خادم افتراضي الخادم المادي الفعلي في طريقة عمله إلا أنه فعلياً عبارة عن ملف برمجي يمكن إنشاؤه ونسخه ونقله ومسحه عند الحاجة. لذلك يستطيع أن يستضيف في محتواه العديد من الموارد التقنية الافتراضية، والخدمات السحابية، والعديد من الميزات والقدرات السحابية الأخرى.



شكل (٢٣): طبقات البيئة الافتراضية.

برمجيات التقنية الافتراضية:

تعتمد البيئات الافتراضية في عملها على برمجية تسمى hypervisor يتم تنصيبها على خادم فعلي يسمى بالمستضيف، مما يمكنها من الوصول مباشرة إلى طبقة البنية التحتية الفعلية. حيث يعمل hypervisor على تحقيق ثلاث مزايا مهمة تساعد في تفعيل الخصائص الرئيسية للحوسبة السحابية، وهي: استقلالية التجهيزات الفعلية، ومشاركة الموارد التقنية، وتكرار الموارد التقنية المشغلة. (حيان، ٢٠١٩).

فيما يخص استقلالية التجهيزات الفعلية، فإن التقنية الافتراضية عموماً هي عملية تقوم بمحاكاة جهاز فعلي واحد (كالخادم) وتحويله افتراضياً إلى نسخة برمجية افتراضية، الأمر الذي يحقق استقلالية من خلال hypervisor الذي يعمل كوسيط لإدارة عملية التواصل بين الجهاز المادي والنسخ الافتراضية المنشأة منه. من خلال هذه الاستقلالية يسهل نقل الخادم الافتراضي من مستضيف إلى آخر دون مواجهة أي مشاكل تذكر بسبب عدم التوافق بين البرمجيات والتجهيزات المادية. ونتيجةً لذلك، تصبح عملية استنساخ المورد التقني الافتراضي أسهل واقل كلفة من تكرار المورد التقني الفعلي.

أما فيما يخص مشاركة الموارد التقنية، فإن hypervisor يتيح إمكانية إنشاء عدة خوادم افتراضية من نفس المورد التقني الفعلي الواحد. تزيد هذه الخاصية من مستوى الانتفاع من قدرات الجهاز الفعلي الواحد مع إمكانية توزيع تنفيذ طلبات المعالجة الواردة

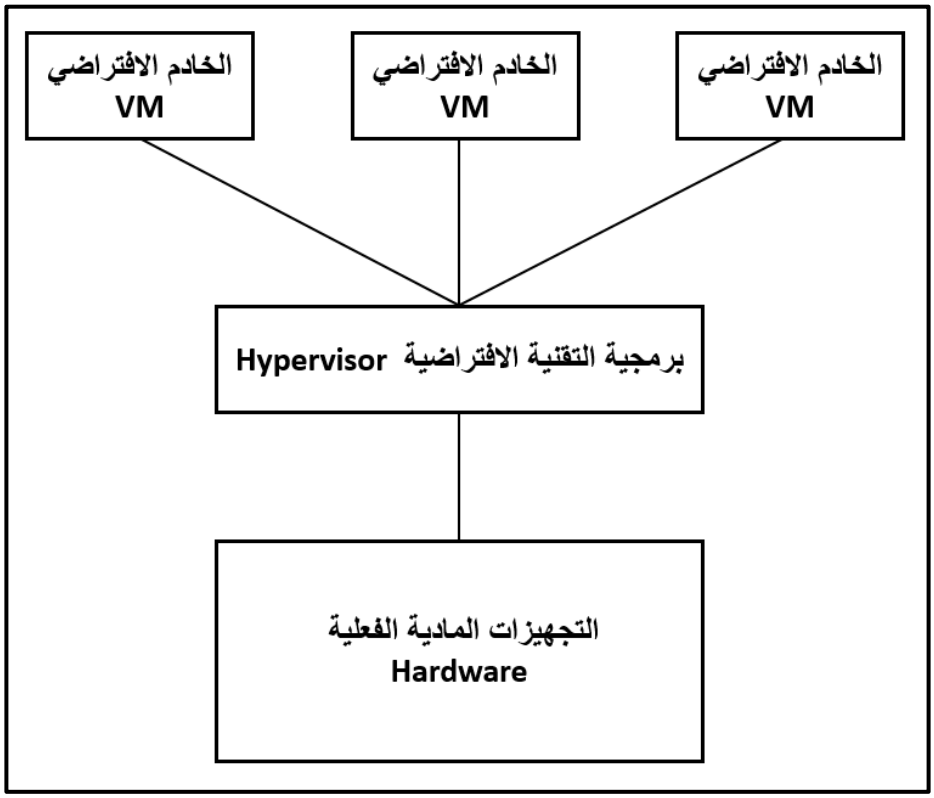
بشكل متوازن بين الخوادم الافتراضية. وتبرز المرونة العالية في التعامل مع مورد فعلي واحد في إمكانية أن تشغّل عدة خوادم افتراضية أنظمة تشغيل مختلفة للمستخدم على نفس المورد الفعلي.

إنّ التمثيل الفعلي للخادم الافتراضي على هيئة ملف برمجي يمكّننا ذلك من عمليات نقله ونسخه ولصقه، وبالتالي إنشاء عدة نسخ منه، ولذلك يسهل كثيراً عمليات متابعة وإدارة الموارد مثل القيام بعمليات النسخ الاحتياطي، أو تنفيذ خطط الاستعادة من الكوارث.

يتم تصنيف برمجية التقنية الافتراضية (hypervisor) إلى نوعين رئيسيين، حسب علاقته مع التجهيزات المادية: (حيان، ٢٠١٩).

- برمجية التقنية الافتراضية المبنية على التجهيزات المادية:

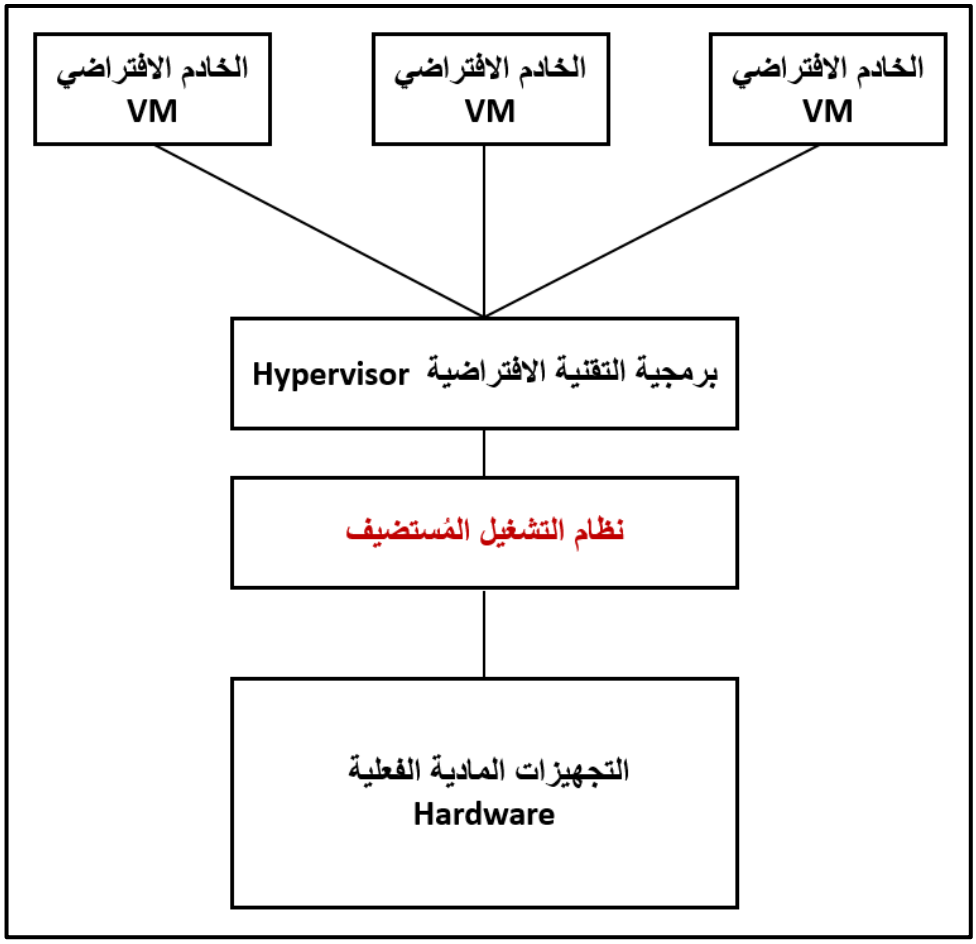
حيث يتم تثبيت برمجية التقنية الافتراضية hypervisor مباشرةً على التجهيزات المادية الفعلية المستضيفة دون الحاجة لوجود نظام تشغيل مستضيف كما هو موضح في شكل (٢٤)، وبالتالي يمكن للخوادم الافتراضية الوصول إلى الموارد الفعلية وتشغيلها مباشرةً دون حاجة لمساعدة نظام تشغيل المستضيف. يُسهم ذلك في التخلص من الأعباء التي تنشأ من التواصل بنظام تشغيل المستضيف كوسيط؛ الأمر الذي يرفع من كفاءة الأداء مقارنةً بالنوع الثاني. يناسب هذا النوع من hypervisor الخوادم التي تواجه أعباءً كبيرة وطلبات مُستخدم مستمرة، وتلك الخوادم التي تتطلب مستوى عاليًا من الأمان. ومن الأدوات البرمجية التي تستخدم هذا النوع من الهايبرفايزر VMWare ESXi ، وخادم Oracle VM، و Microsoft Hyper-V، و Linux KVM.



شكل (٢٤): *برمجية التقنية الافتراضية المبنية على التجهيزات المادية*

- برمجية التقنية الافتراضية المبنية على البرمجيات:

حيث يتم تثبيت برمجية التقنية الافتراضية hypervisor على نظام تشغيل موجود مسبقاً، وبالتالي يُسمى نظام التشغيل المستضيف كما هو موضح في(٢٥). وبالتالي يمكن للمستخدم إنشاء وإدارة الخوادم الافتراضية باستخدام hypervisor. فبينما يستطيع نظام التشغيل المستضيف التعامل والوصول المباشر إلى التجهيزات الفعلية، يحتاج الهايبرفايزر إلى مساعدة نظام التشغيل المستضيف كطبقة وسيطة للوصول والتعامل مع التجهيزات الفعلية. ويتمثل العيب الرئيسي لذلك في احتمالية فشل وتعطل نظام تشغيل المستضيف؛ الأمر الذي يؤدي إلى تعطُّل الخوادم الافتراضية. لذا يُنصح بتجنب استخدام النوع الثاني من الهايبرفايزر في الحالات التي تكون فيها استمرارية عمل تطبيقات المستخدم ذات أهمية قصوى. ومن الأدوات البرمجية التي تستخدم هذا النوع من الهايبرفايزر: Oracle VirtualBox، و VMare Workstation Player، و Linux-Vserver.



شكل (٢٥): *برمجية التقنية الافتراضية المبنية على البرمجيات*

التهديدات الأمنية المرتبطة بالبيئات الافتراضية:

يتم إنشاء البيئة الافتراضية في مراكز البيانات عموماً باستخدام برمجية التقنية الافتراضية hypervisor. وبالتالي، فإن أسهل طريقة للاختراق الأمني لها والوصول إلى موارد البنية التحتية التقنية الفعلية والتحكم فيها يكون من خلال اختراق hypervisor. قد يتم ذلك من خلال تعطيل الخادم المستضيف أو تسريب البيانات المخزنة فيه وذلك عن طريق مهاجمته ببعض الشفرات البرمجية وتشغيلها عليه.

بشكل عام، تعتبر برمجية التقنية الافتراضية المبنية على البرمجيات أكثر قابليةً للتعرض للهجمات الإلكترونية من برمجية التقنية الافتراضية المبنية على التجهيزات المادية، حيث تتم عملية الاختراق عبر نظام تشغيل المستخدم أو نظام تشغيل المستضيف. لذا ينبغي على المزود والمستخدم اتخاذ أعلى مستوى من الاحتياطات في تأمين مواردهما التقنية الافتراضية بنفس الطريقة التي يتم بها تامين الموارد التقنية الفعلية. ويمكن أن يتم ذلك بإيجاد واعتماد وتنفيذ سياسات أمنية صارمة، وتكون مفصّلة بوجود إجراءات واضحة لحماية الموارد التقنية؛ كوجود جدران حماية، والحرص على تحديث hypervisor ونظام تشغيل المستضيف بشكل دوري، واستخدام أدوات برمجية لمراقبة أداء الهايبرفايزر واكتشاف ومنع الأنشطة المريبة، وتبني إجراءات واضحة للتحكم في الوصول إلى الموارد. (حيان، ٢٠١٩)

العنصر الرابع: أمن الحوسبة السحابية:

في الحوسبة السحابية، تكون المسؤولية مشتركة بين مزود الخدمة والمستخدم لتوفير الأمن المعلوماتي واتخاذ التدابير والاحتياطات اللازمة لحماية كل من البنى التحتية والبيانات والتطبيقات. وبناءً على طبيعة عمل السحابة التي تستلزم انتقال معظم مسؤوليات التحكم في الموارد التقنية من تطبيقات وبيانات من موقع المستخدم إلى موقع مزود الخدمة، فمن الطبيعي حدوث تحول لدى كلٍّ من المزود والمستخدم فيما يتعلق بدرجة الاهتمام بالنواحي الأمنية لضمان سلامة التطبيقات والبيانات. بشكل عام، يمكن تصنيف المخاطر الأمنية المتعلقة بالحوسبة السحابية إلى نوعين أساسيين: (حيان، ٢٠١٩).

- المخاطر الأمنية التي تواجه مزودي الخدمات السحابية؛ كتلك المرتبطة بخدمات البنية التحتية كخدمة (IaaS)، أو خدمات البرمجيات كخدمة(SaaS) ، أو خدمات المنصة كخدمة.(PaaS) لذلك، يجب على مزودي الخدمة التأكد من أن بنيتهم التقنية التحتية آمنة، وأن بيانات وتطبيقات عملائهم محميّة من أي تهديدات إلكترونية.
- المخاطر التي تواجه المستخدمين أثناء استخدام الخدمات السحابية. لهذا ينبغي على المستخدم التعرف على حقوقه وواجباته ومسؤولياته بدقة، وأخذ التدابير اللازمة لحماية الوصول إلى تطبيقاته وبياناته من خلال استخدام ممارسات آمنة.

التهديدات الأمنية المهددة للحوسبة السحابية:

إن أكبر تحدي يواجه أمان الحوسبة السحابية هو اعتمادها الكلي على الاتصال بالإنترنت، فعندما نفقد الاتصال نكون قد فقدنا الاتصال بالسحابة تماماً، وبالتالي يتعذر وصولنا إلى البيانات والتطبيقات الإلكترونية. هذه النقطة لا تمثل مخاطرة فقط لمستخدم الحوسبة السحابية، إنما أيضاً تشكل تهديداً لمزود الخدمة كونها تعيق إيصال خدماته للعملاء. كما إن نقل البيانات والتطبيقات الخاصة بالمستخدم ليتم تخزينها وتشغيلها على السحابة العائدة ملكيتها إلى مزود الخدمة، يعني ذلك أن المسؤولية الأمنية تصبح مشتركة بين مزود السحابة والمستخدم كما ذكرنا سابقاً. لذلك يتطلب استخدام السحابة والتعامل معها من خلال الانترنت أن يزيد المستخدم من حدود ثقته، لتشمل التعامل مع موارد السحابة الخارجية. قد يكون من الصعب تأسيس نموذج أمني يوفر هذه الثقة دون تقديم بعض التنازلات مقابل الفوائد المتوقعة من قبل المستخدم. لذلك، نستعرض فيما يلي أبرز التهديدات الأمنية التي قد تواجه الحوسبة السحابية: (حيان، ٢٠١٩).

- <u>التنصت على حركة البيانات:</u>

قد يحدث تنصت على البيانات عن انتقالها بين المستخدم ومزود الخدمة، وقد يتم ذلك من خلال أحد البرمجيات الخبيثة بغرض جمع معلومات معينة وكشفها لتحقيق أهداف قد تخدم المهاجم.

- <u>الوسيط الخبيث:</u>

قد يحدث هذا التهديد عند قيام برمجية خبيثة باعتراض الرسائل على السحابة ثم التعديل عليها، الأمر الذي يؤثر سرية ونزاهة البيانات. كما قد يتم إدراج بيانات أو برمجيات خبيصة ضمن محتويات الرسالة قبل إعادة توجيهها إلى المُستقبل.

- <u>الحرمان من الخدمة:</u>

ينتج ذلك عندما يتم إغراق أحد الموارد السحابية مثل الخادم بكمّ هائل من الطلبات والرسائل الوهمية التي تتسبب في توقفه عن العمل، وبالتالي حرمان المستفيدين من جميع الخدمات السحابية التي يشغّلها ذلك المورد، وبالتالي يؤثر على توافر الخدمة للمستفيد.

- الصلاحية غير الشرعية:

يتم ذلك عندما يتمكن مهاجم من الحصول على صلاحية الوصول إلى أحد الموارد السحابية عن طريق الصدفة أو بطريقة غير نظامية، الأمر الذي ينتج عنه وصول المهاجم إلى موارد عادةً ما تكون محمية. وقد يقع ذلك أيضاً بسبب تأمين الوصول إلى المورد السحابي باستخدام كلمات مرور ضعيفة أو بحسابات مشتركة. قد يؤدي هذا النوع من التهديدات إلى نتائج خطيرة بناءً على نطاق الوصول الذي اكتسبه المهاجم، كأن يتمكن من الوصول إلى قواعد بيانات محمية.

- الهجوم الافتراضي:

تتيح التقنية الافتراضية إمكانية وصول عدة مستفيدين إلى الموارد التقنية الافتراضية (كالخوادم الافتراضية) التي قد تشترك في نفس التجهيزات التقنية الفعلية (كالخوادم الفعلية) إلا أنَّ الموارد التقنية الافتراضية تكون منفصلة عن بعضها البعض بشكل منطقي وليس فعلي. ولكن قد يؤدي ذلك إلى حدوث انتهاك أمني نتيجة تمَّكن أحد المستخدمين من إساءة استخدام صلاحية الوصول الممنوحة له والهجوم على التجهيزات التقنية الفعلية. ينتج عن هذا التهديد إفشاء معلومات سرية لمستخدمين آخرين، أو إجراء عمليات غير نظامية على البيانات.

- تفاوت الإجراءات الأمينة:

عند قيام المستخدم بوضع تطبيقاته وبياناته على سحابة عامة، فمن المحتمل أن تكون السياسات والإجراءات الأمنية التي يتبعها غير متطابقة مع تلك المتبعة من قبل مزود الخدمة، حينئذٍ عليه القبول بما هو متاح على السحابة. يحتاج المستفيد القيام بتقييم التطابق في مستويات الأمان بينه وبين مزود الخدمة، والتأكد من أن البيانات والتطبيقات المنتقلة إلى السحابة العامة تكون حسب البنود المتفق عليها في وضع محمي من أي تهديد أمني.

- قصور في فهم اتفاقية مستوى الخدمة:

من الضروري قيام المستخدم بمراجعة وتدقيق بنود اتفاقية مستوى الخدمة(Service-level agreement SLA) ، والتي غالباً ما يحددها مزود الخدمة، وذلك للتأكد من أن السياسات الأمنية متوافقة وبمستوى مقبول احتياجات المستخدم. وأي قصور في فهم تلك البنود قد يؤدي إلى دخول المستخدم في إشكاليات تقنية أو قانونية بعد بدء تشغيل الخدمة السحابية. كلما زادت المسؤولية المكتوبة في اتفاقية مستوى الخدمة على مزود الخدمة، انخفضت المخاطر على المستخدم.

- قصور في إدارة المخاطر:

كجزء من استراتيجية إدارة المخاطر، ينبغي على المستخدم القيام بتقييم جاد للمخاطر، يشمل تحديد التهديدات والمخاطر المحتملة وآلية للتخفيف من آثارها ومعالجتها عند حدوثها. أي قصور في أداء الخطوات الأساسية لإدارة المخاطر قد يؤدي إلى وقوع المستفيد في مشاكل تشغيلية أو تقنية أو قانونية.

الاحتياطات الأمنية للحوسبة السحابية:

تتمركز الاحتياطات الأمنية والتدابير الإجرائية لحماية السحابات في ثلاثة جوانب أساسية كما يلي: (حيان، ٢٠١٩):

- أمن البيانات على السحابة:

تعتبر البيانات من أهم الأصول التي يسعى المستخدم إلى حمايتها وتأمينها. لذلك، يجب تنفيذ سياسات أمنية صارمة تكون مفصَّلة بإجراءات واضحة لحماية البيانات، وفرض ضوابط أمنية بتشفير البيانات الحساسة في أماكن تخزينها على قواعد البيانات وأثناء انتقالها على بين السحابة والمستخدم، وتطبيق مستوى عالٍ من الإجراءات الأمنية لضبط الوصول إلى البيانات. كما يجب تحديد الصلاحيات في استخدام البيانات، كالقراءة أو التعديل أو الكتابة أو المسح. ويتم تحديد هذه الصلاحيات إلكترونياً ومنحها للمستخدم استناداً إلى سياسات الاستخدام المحددة مسبقاً لمنح هذه الصلاحيات. من المهم الإشارة إلى ضرورة وجود سياسات وإجراءات واضحة لعمل نسخ احتياطية ومكررة للبيانات الحساسة على السحابة.

- أمن الشبكة السحابية:

تتيح طبقة الشبكة السحابية للمستخدمين الاتصال مباشرةً بالسحابة. وتشكل العصب الأساسي لتشغيل وإيصال خدمات الحوسبة السحابية والاستفادة منها لكل من المزود والمستخدم، حيث تعتمد البنية التحتية للسحابة بشكل كامل على هذا الاتصال الشبكي الذي يتم من خلاله تقديم الخدمات للمستخدمين.

ينبغي أيضاً مراعاة أن يكون هناك مرونة في إضافة تجهيزات وبرمجيات جديدة في مراكز البيانات الخاصة بالمستخدم الذي قد يحتاج إلى إضافة جدران الحماية، وأنظمة مكافحة البرمجيات الخبيثة. ينبغي أن يتم توظيف هذه البرمجيات والتجهيزات للعمل بسلاسة جنباً على جنب مع غيرها من البرمجيات والتجهيزات السحابية الموجودة مسبقاً لرفع مستوى الأمن.

- أمن التقنية الافتراضية:

تستهدف التقنية الافتراضية الاستغلال الأمثل للموارد التقنية، وتسمح بمشاركة نفس المورد التقني بين العديد من المستخدمين، كما تسمح بدمج قدرات عدة موارد تقنية من نفس النوع، فتظهر للمستفيد وكأنها مورد واحد. لذلك فهي بشكل أساسي على ثلاثة محاور أساسية: الشبكات الافتراضية، والتخزين الافتراضي، والخوادم الافتراضية.

فيما يخص الشبكات الافتراضية فإن دخول طبقة وسيطة، وهي طبقة التقنية الافتراضية، بين البنية التحتية الفعلية ونظام التشغيل تحتم ضرورة فهم طريقة عملها، وإلا نتج عن تطبيقها قابلية عالية لوجود ثغرات أمنية وزيادة في أعباء العمليات السحابية، الأمر الذي يؤثر بالتأكيد سلباً على أدائها بشكل عام. لذا فإن اختراق هذه الطبقة الوسيطة hypervisor يعني سهولة الوصول إلى موارد البنية التحتية الفعلية والتحكم فيها. إلا أنه بفهم طبيعة عمل هذه الطبقة يمكن من تخفيف الآثار السلبية المحتملة وذلك من خلال تطبيق الفصل المنطقي للموارد الشبكية، واستخدام أدوات برمجية لمراقبة أداء hypervisor واكتشاف الأنشطة المريبة لمنع حدوثها، وتبنّي إجراءات واضحة للتحكم في الوصول إلى الموارد.

أما في التخزين الافتراضي، فيتم عند تخصيص أو تحرير الموارد السحابية الافتراضية. على سبيل المثال، خلال تشغيل الخدام الافتراضي وتخصيص موارد افتراضية متعددة له، يقوم بعلمه الاعتيادي بالقراءة والكتابة من وعلى الذاكرة الثانوية الفعلية من خلال الذاكرة الثانوية الافتراضية. إذا لم يتم مسح المحتوى على الذاكرة الفعلية قبل تحرير الجزء المخصص لهذا الخادم الافتراضي وتخصيصه لخادم افتراضي آخر، قد يصبح المحتوى على الذاكرة الثانوية الفعلية منكشفاً للخادم الافتراضي الآخر؛ لذا فإنه ينصح كممارسة جيدة القيام بالتأكد من مسح المحتوى لكل الموارد السحابية المحررة قبل تخصيصها للاستخدام الذي يليه.

بالنسبة للخوادم الافتراضية، فقد يكون هناك اختراق شبكي داخلي يحدث بين بينها وهي التي تعمل على خادم فعلي واحد. من الصعب اكتشاف هذه الاختراق الداخلي ما لم يكن هناك خدمة رقابية تقوم على مراقبة الحركة من وإلى كل خادم افتراضي يتم إنشاؤه من hypervisor. وللحد من تدفق الحركة بين الخوادم الافتراضية المختلفة. وكممارسة جيدة في هذا الشأن، يتم استخدام شبكة محلية افتراضية (vLAN) لعزل الخادم الافتراضي الخاص بمستخدم ما عن الخادم الافتراضي الخاص بمستخدم آخر، حيث تعتبر (vLAN) على أنها شبكة منطقية غير فعلية تم تقسيمها من شبكة فعلية محمية أكبر حجماً. ويتطلب تطبيق هذه الآلية الافتراضية تعزيز الدعم للشبكة المحلية الافتراضية من خلال توظيف وتهيئة المحولات الشبكية والخوادم الفعلية لتطبيق العزل الآمن.

أسئلة ونقاش (٣)

الهدف: أن يميز المتدرب بين خدمات الحوسبة السحابية المختلفة. **الزمن:** ١٠ دقائق.

مع انتشار مزودي خدمات الحوسبة السحابية، تزداد المنافسة فيما بينهم لتقديم مزايا وإضافات بشكل مستمر للمستخدمين. لذلك، يقوم المتدربون بالمقارنة بين Microsoft Azure مع Amazon Web Services (AWS). كمزودي خدمات سحابية

الإرشادات:

١. يقوم المتدربون بشكل فردي باستخدام الإنترنت للبحث عن مزودي الخدمة المذكورين في التمرين.
٢. استخدام الجدول التالي لاستعراض خمسة مزايا لكل مزود خدمة.
٣. يقوم المتدرب بمناقشة النتائج مع المتدربين.

جدول (٩): *مزايا مزودين خدمة.*

Microsoft Azure	Amazon Web Services (AWS)

اليوم التدريبي الرابع

الموضوع السابع: الضوابط الأمنية لحماية البرمجيات والتطبيقات.

الموضوع الثامن: أمن المعلومات في الأجهزة المحمولة.

الموضوع التاسع: التشفير.

المخطط التدريبي لليوم الرابع

الجلسة الأولى

- (٨:٠٠-٩:٣٠)
- الضوابط الأمنية لحماية البرمجيات والتطبيقات.

استراحة (٩:٣٠-١٠:٠٠)

الجلسة الثانية

- (١٠:٠٠-١١:٣٠)
- أمن المعلومات في الأجهزة المحمولة.

استراحة (١١:٣٠-١٢:٣٠)

الجلسة الثالثة

- (١٢:٣٠-٢:٠٠)
- التشفير.

الموضوع السابع: الضوابط الأمنية لحماية البرمجيات والتطبيقات

إن أحد الأهداف الأساسية لأمن المعلومات هو حماية بيانات المستخدم، والذي يتم تحقيقه بشكل كبير في حال رفع مستوى الحماية الأمنية لكل من الأجهزة وأنظمة التشغيل والشبكات. ولكن، من المهم أيضًا ألا نغفل عن مستوى أمان التطبيقات التي يتم تشغيلها على أجهزة المستخدمين. حيث أنه يمكن للتطبيق غير الآمن أن يفتح الباب للمهاجمين لاستغلال التطبيق والبيانات التي يستخدمها وحتى نظام التشغيل الأساسي للجهاز.

العنصر الأول: الثغرات الأمنية المهددة للبرمجيات والتطبيقات:

الكثير من نقاط ضعف البرمجيات والتطبيقات وحتى الثغرات الأمنية المهددة لها ترجع إلى عيوب تصميم التطبيق أو برمجته، حيث توفر هذه العيوب طريق للمهاجم لاستغلال التطبيق أو الوصول من خلاله لنظام التشغيل. من الممكن حصر الثغرات الأمنية في البرمجيات والتطبيقات التي يجب على المطورين أخذها في الاعتبار في نوعين أساسيين: ثغرات المدخلات Input Vulnerabilities، ونقاط ضعف الذاكرة Memory Vulnerabilities. وفيما يلي إيضاح لكل نوع على حدة. (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- ثغرات المدخلات Input Vulnerabilities:

تعمل معظم التطبيقات والبرمجيات على أساس تنفيذ عمليات معالجة على مدخلات من المستخدم ذات أنواع وصيغ معينة كالقيم النصية والرقمية وما إلى ذلك. في بعض الأحيان، من الممكن أن يتسبب إدخال قيم غير متوقعة في تعطل التطبيق، والذي قد يُمَّكن المستخدم من الحصول على صلاحيات أعلى أو الوصول إلى قيم لا ينبغي له الوصول اليها. لذلك، قد يتسبب عدم تحقق التطبيق بشكل صحيح من مدخلات المستخدم Inputs في حدوث عدد من الهجمات، مثل هجوم حقن SQL (SQL Injection). يحدث هجوم حقن SQL عندما لا يقوم التطبيق بالتحقق من المدخلات بشكل سليم، مما ينتج عنه استغلال ذلك من خلال إدراج عبارات SQL للاستعلام من قواعد البيانات المرتبطة بالتطبيق. حيث تستخدم لغة الاستعلام الهيكلية Structured Query Language (SQL) بشكل عام لعرض ومعالجة البيانات المخزنة في قواعد البيانات. وبالتالي، يستهدف هجوم حقن SQL خوادم قواعد البيانات من خلال إدخال أوامر ضارة فيها بواسطة التطبيقات. (Ciampa, ٢٠١٨)

لذلك، يجب على التطبيق التحقق من صحة جميع المدخلات Input Validation قبل معالجتها أو ارسالها. هذا يعني أنه عندما يقوم المستخدم بإدخال البيانات في حقل نصي مثل الاسم أو العنوان، فأنه يجب على التطبيق أن يقوم بفحصها من واجهة العميل Client Side للتأكد من أنها من نوع وحجم البيانات المطلوب. كما يمكن أن يتم أيضًا إجراء فحوصات أخرى، مثل البحث عن رموز حقن SQL الشائعة. كما يجب أن يتم فحص البيانات مرة أخرى أيضاً عندما يتم نقلها من نظام إلى آخر، أي عندما تنتقل البيانات من العميل إلى الخادم، حيث يجب أن يتم التحقق من صحة البيانات من جانب الخادمServer Side . لذلك يمكن تلخيص القول بأن التحقق من صحة جميع البيانات من جانب العميل ومن جانب الخادم، يوفر مستوى حماية مقبول ضد الهجمات المستغلة لأخطاء المدخلات.

- نقاط ضعف الذاكرة: Memory Vulnerabilities:

أحد أهم نقاط الضعف في التطبيقات والتي يتم غالباً ما يتم استغلالها، هو وجود أخطاء في البرمجة قد تتسبب في وجود ثغرات ذاكرة الكمبيوتر أو الذاكرة المؤقتة Buffer memory. لذلك، سيتم توضيح الثغرات فيما يلي:

تسرب الذاكرة Memory Leak: ويحدث ذلك عندما يقوم التطبيق بتخصيص أو حجز جزء من الذاكرة ولكنه لا يحررها بعد الانتهاء من استخدامها ديناميكيًا. لا تسمح العديد من لغات البرمجة الحديثة مثل Java وC# للمبرمج بتخصيص الذاكرة وتحريرها مباشرةً. لذلك، فإن لغات البرمجة هذه ليست عرضة لتسريب الذاكرة. ومع ذلك، فإن بعض لغات البرمجة، وأبرزها C و C+ تمنح المبرمج قدرًا كبيرًا من التحكم في إدارة الذاكرة، والذي قد يتسبب في وجود هذه الثغرة بسبب الفشل في تحرير الذاكرة التي تم تخصيصها. يمكن للمهاجم الاستفادة من سلوك البرنامج غير المتوقع الناتج عن حالة انخفاض مساحة الذاكرة بسبب تسربها.

- استنفاذ الذاكرة Memory Exhaustion: يحدث ذلك عندما يقوم أحد التطبيقات بتخصيص مساحات إضافية من الذاكرة باستمرار، يتم في النهاية استنفاد الذاكرة المحدودة لجهاز المستخدم، مما يؤدي إلى توقف النظام أو تعطله. يمكن أن يكون هذا شكلاً من أشكال هجوم رفض الخدمة Denial of Service attack عندما يتم تنفيذه عن قصد.
- فيضان الذاكرة المؤقتة Buffer Overflow: ويحدث عندما يحاول التطبيق تخزين البيانات في ذاكرة الوصول العشوائيRAM بحجم يفوق مساحة الذاكرة المؤقتة. يمكن للمهاجم إغراق الذاكرة المؤقتة برموز تشير إلى برمجيات ضارة أو قد تعمل على تشغيل هذه البرمجيات.

العنصر الثاني: معايير التطوير الآمن للبرمجيات والتطبيقات:

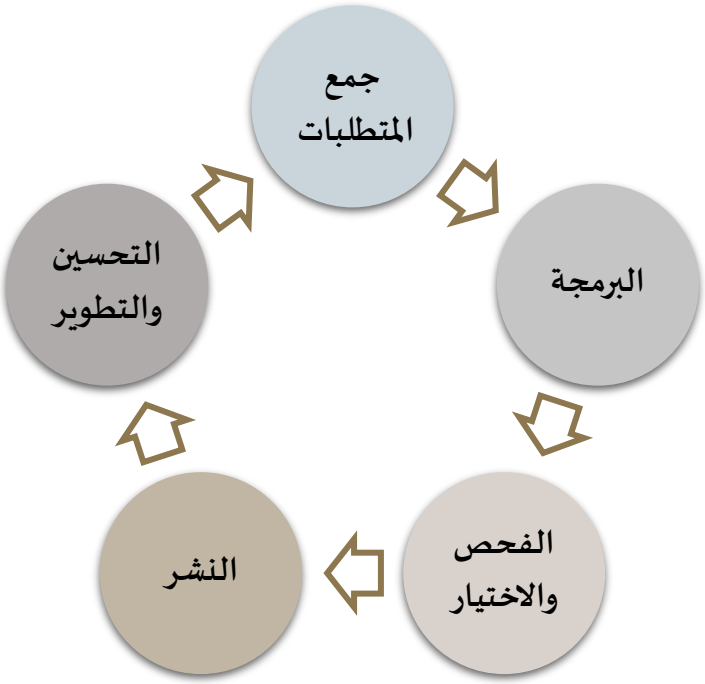
تتضمن معايير التطوير الآمن للبرمجيات والتطبيقات على الإلمام بمفاهيم تطوير التطبيقات، وتقنيات البرمجة الآمنة، وفحص التعليمات البرمجية. وفيما يلي سيتم استعراض كل عنصر بشكل منفصل. (Ciampa, ٢٠١٨)

- مفاهيم تطوير البرمجيات والتطبيقات:

يتطلب تطوير التطبيقات المرور بعدة مراحل مختلفة. تشمل هذه المراحل:

- التطويرDevelopment : يتم في هذه المرحلة تحديد متطلبات المستخدم والتأكد من أن التطبيق يلبي احتياجات العمل المقصودة قبل أن نبدأ بمرحلة البرمجة الفعلية للتطبيق.
- الفحص Testing: تختبر هذه المرحلة التطبيق بدقة بحثًا عن أي أخطاء قد تؤدي إلى وجود ثغرات أمنية.
- الإطلاق Staging: يتم في هذه المرحلة اختبار "ضمان الجودة" للتحقق من أن الكود البرمجي يعمل على النحو المطلوب.
- الإنتاج Production: يتم في هذه المرحلة إطلاق التطبيق لاستخدامه في البيئة الفعلي.

لذلك، يعتبر نموذج دورة حياة تطوير التطبيقات Application Development Lifecycle على أنه نموذج مفاهيمي يصف المراحل المختلفة التي ينطوي عليها إنشاء التطبيق، والموضحة في شكل (٢٦).



شكل (٢٦): *دورة حياة تطوير البرمجيات والتطبيقات*

- تقنيات البرمجة الآمنة:

هناك العديد من تقنيات البرمجة التي يجب اتباعها لتطوير تطبيقات آمنة تساهم في الحد من تعرض البيانات للانتهاك أو كشفها للمهاجمين. وتتضمن هذه التقنيات التي تساهم على رفع مستوى أمان التطبيق ما يلي: (Ciampa, ٢٠١٨)

- اعتماد خوارزمية تشفير مناسبة لجميع البيانات التي يتم نقلها أو تخزينها من خلال البرمجية أو التطبيق.
- معالجة الأخطاء البرمجية بشكل مناسب، للتقليل من احتمالية توقف التطبيق بشكل مفاجئ والذي قد يستغل من قبل المهاجمين.
- التحقق المناسب من صحة مدخلات المستخدم من جانب العميل والخادم، لمنع أي مدخلات قد تتسبب بالضرر للتطبيق أو نظام التشغيل.
- التأكد من دقة قواعد البيانات من خلال تنفيذ عمليات Normalization والتي تتحقق من عدم وجود تكرار في البيانات لتقليل احتمالية حدوث الأخطاء.
- مصادقة الأكواد البرمجية من خلال التوقيع الرقمي من مالك التطبيق لضمان عدم تعرض الأكواد للتعديل أو الإتلاف.

- فحص التعليمات البرمجية:

هناك عدة أدوات واختبارات مختلفة يمكن تطبيقها لفحص جودة التعليمات البرمجية (الكود) الخاصة بالتطبيق. بشكل عام، لابد من اجراء اختبار التحقق من النموذج التطبيق المعد model verification في كل مرحلة من مراحل تطوير التطبيق للتأكد من أنه يفي بجميع متطلبات المستخدم. إضافة إلى ذلك، هناك أنواع مختلفة من الاختبارات التي من المهم إجراءها على التطبيقات لضمان جودتها ولتقليل معدل الأخطاء الذي قد يؤدي إلى اختراقات أمنية، ومن هذه الاختبارات والفحوصات ما هو موضح في جدول (١٠). (Emmett Dulaney and Chuck Easttom, ٢٠١٨).

جدول (١٠): *أنواع اختبارات البرمجيات والتطبيقات.*

نوع الاختبار	الوصف
تحليل الكود الجامد Static code analyzers	هي أدوات تقرأ ببساطة الكود البرمجي وتعمل على تحليله بدون تشغيل التطبيق في محاولة لتوثيق الثغرات الأمنية. يمكن أن يتم نتيجة هذا الفحص معالجة الأخطاء البرمجية المكتشفة ومعالجة مشاكل إدارة الذاكرة وتخصيصها.
الفحص الحيوي (العشوائي) Dynamic testing (fuzzing)	هو أسلوب اختبار برمجي يقوم بفحص التطبيق من خلال تعمد إدخال بيانات عشوائية أو غير صحيحة أو متوقعة، ثم يتم مراقبة البرنامج للتأكد من أن جميع الأخطاء تم التعامل معها برمجياً بشكل صحيح. يشاع استخدام هذا النوع لاختبار مشاكل الأمان في البرامج والتطبيقات أو أنظمة الكمبيوتر.
اختبار صلابة التطبيق Stress testing	وهو اختبار يضع التطبيق تحت أحمال تشغيلية أعلى من المعتاد والتي تتطلب عمليات معالجة عالية لتحديد ما إذا كان البرنامج قويًا ومستقراً بما يكفي بحيث يمكنه تنفيذ جميع عمليات معالجة الأخطاء بشكل صحيح.
اختبار الوحدات البرمجية Unit testing	وهو اختبار يتم بشكل منفصل على كل عملية أو وحدة برمجية في التطبيق للتأكد من سلامتها بمعزل عن بقية العمليات الأخرى. عادة ما يتم ذلك بواسطة المبرمجين، ويمكن أن يكون الاختبار ديناميكيًا أو ثابتًا أو كليهما.
اختبار التكامل Integration testing	وهو اختبار يتم ربط وحدتين أو أكثر من الوحدات أو العمليات البرمجية في التطبيق، حيث يجب اختبارهما للتأكد من أنهما يعملان معًا بشكل صحيح وبدون أي تعارض. يتم هذا الاختبار بواسطة المبرمجين. وعادة ما يكون اختبارًا ديناميكيًا.
اختبار النظام بشكل كامل System testing	وهو اختبار يتم اجراءه من قبل فريق محايد عن مبرمجين التطبيق، ويهدف إلى اختبار التطبيق أو النظام بشكل عام للتأكد بأنه يعمل بشكل صحيح. عادة ما يكون هذا الاختبار اختبارًا ديناميكيًا.
اختبار موافقة المستخدم User acceptance testing	وهو اختبار يتم من خلال منح مجموعة من المستخدمين حق الوصول إلى التطبيق لاختباره، لمعرفة ما إذا كان النظام يلبي احتياجاتهم.

العنصر الثالث: ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي:

تعرف شبكات التواصل الاجتماعي على أنها مواقع الويب التي تسهل ربط الأفراد بغيرهم ممن يقاسمونهم الاهتمامات المشتركة مثل الهوايات أو المواضيع الدينية والسياسة والاجتماعية أو يشاركونهم مراحل وخبرات سابقة مثل كونهم زملاء دراسة أو خريجي نفس الجامعة، حيث تعمل مواقع التواصل الاجتماعي على انشاء وإدارة مجتمعات افتراضية للمستخدمين عبر الإنترنت. حيث إنه يمكن للمستخدم الذي يتم منحه حق الوصول إلى أحد مواقع التواصل الاجتماعي من خلال إنشاء حساب عليها من قراءة صفحات الملفات الشخصية للأعضاء الآخرين والتفاعل معهم وقراءة المعلومات التي ينشرها الآخرون ومشاركتهم المستندات والصور ومقاطع الفيديو. (Ciampa, ٢٠١٨).

يوماً بعد يوم تزداد شعبية مواقع التواصل الاجتماعي عبر الإنترنت، ويتمثل ذلك في زيادة عدد المستخدمين والمشتركين فيها. حيث وصل عدد مستخدمي شبكات التواصل الاجتماعي في عام ٢٠٢١ إلى ٣,٧٨ مليار مستخدم، ومن المتوقع زيادة هذا العدد إلى ٤,٤١ مليار في عام ٢٠٢٥. (https://www.statista.com/, ٢٠٢١)

لذلك نظراً لهذا التزايد في أعداد المستخدمين، توجهت الكثير في الجهات في القطاعين العام والخاص إلى استخدام شبكات التواصل الاجتماعي كونها إحدى الوسائل الممكنة للتواصل السريع والفعّال مع المستفيدين مما يسهم في سرعة الاستجابة وتحسن وتسهيل تجربة المستفيدين. ومع ازدياد استخدام شبكات التواصل الاجتماعي بشكل رسمي من قبل الجهات داخل المملكة للتواصل مع المستفيدين، ازداد خطر جرائم سرقة حسابات التواصل الرسمية أو سوء استغلالها أو انتحال شخصيتها، مما يستوجب وضع متطلبات الأمن السيبراني للحد من هذه المخاطر. (Organizations' Social Media Accounts Cybersecurity Controls, ٢٠٢١)

التهديدات الأمنية لشبكات التواصل الاجتماعي:

على صعيد الأفراد، تتضمن شبكات التواصل الاجتماعي مجموعة من المخاطر. حيث تشمل ما يلي:

- إمكانية استغلال بيانات المستخدمين الشخصية والمنشورة في وسائل التواصل الاجتماعي بشكل ضار. حيث ينشر المستخدمون معلوماتهم الشخصية على حساباتهم وصفحاتهم ليشاركوها الآخرين، مثل تواريخ الميلاد وعنوان السكن وخططهم لعطلة نهاية الأسبوع وغيرها من المعلومات. لذلك، يمكن للمهاجمين استغلال هذه المعلومات لمجموعة من المقاصد الخبيثة. على سبيل المثال، معرفة أن شخصًا ما في إجازة يمكن أن يسمح لصوص باقتحام منزله في حال كان قد قام بنشر عنوانه ومخطط قضاء إجازته. كما يمكن استخدام الكثير من المعلومات الشخصية في انتحال الهوية. وبالتالي هناك الكثير من المعلومات التي يمكن للمهاجمين جمعها عن أهدافهم من الأشخاص.
- زيادة مستوى ثقة المستخدمين في متابعيهم أو أصدقائهم في بيئات التواصل الاجتماعي الافتراضية. غالبًا ما ينضم المهاجمون إلى أحد مواقع التواصل الاجتماعي ويتظاهرون بأنهم جزء من شبكة المستخدمين. بعد مدة زمنية، يبدأ المستخدمون في الشعور بأنهم قد كونوا علاقة صداقة مع المهاجمين وقد يبدؤون في التصريح عن

معلوماتهم الشخصية أو النقر على الروابط المضمنة التي يوفرها المهاجم والتي تحمل برامج ضارة على جهاز كمبيوتر المستخدم.

- التوسع في قبول الأصدقاء والمتابعين في وسائل التواصل الاجتماعي قد يكون عواقب وخيمة وغير متوقعة. حيث يقبل بعض مستخدمي وسائل التواصل الاجتماعي بسهولة أي طلب "صداقة" يتلقونه، حتى لو لم يكونوا على معرفة مسبقة بهذا الشخص. يمكن أن يؤدي هذا إلى حدوث انتهاكات أمنية معلوماتية، لأن أي شخص يتم قبوله كصديق غالباً ما يكون قادرًا على رؤية ليس فقط جميع المعلومات الشخصية لهذا المستخدم، ولكن أيضًا المعلومات الشخصية لأصدقائه.
- يعتبر أمن المعلومات في وسائل التواصل الاجتماعي متساهل إلى حد ما ويدعو للحيرة. نظرًا لأن المقصود من استحداث مواقع الشبكات الاجتماعية هو مشاركة المعلومات، فقد جعلت هذه المواقع من السهل غالبًا على المستخدمين غير المصرح لهم عرض معلومات الأشخاص الآخرين. ولمكافحة ذلك، تقوم العديد من المواقع بتغيير خيارات الأمان الخاصة بها بشكل دائم، مما يجعل من الصعب على المستخدمين مواكبة هذه التغييرات.

أما على صعيد المنظمات، فيمكن أن يشكل استخدام الموظفين لوسائل التواصل الاجتماعي مخاطر معلوماتية أيضًا. لذلك من المهم أن يتم فرض سياسة وسائل التواصل الاجتماعي التي تحدد استخدام الموظف المقبول لوسائل التواصل الاجتماعي. والتي من الممكن أن تشتمل على العناصر التالية: (Ciampa, ٢٠١٨)

- وضع معايير وإرشادات واضحة لاستخدام الموظفين لوسائل التواصل الاجتماعي بما يضمن التمثيل الصحيح لهوية المنظمة.
- تحديد قيود النشر في حسابات المنظمة الرسمية على شبكات التواصل الاجتماعي. حيث إنه في كثير من الأحيان قد لا يُقدر الموظفون ما هو مناسب وغير مناسب لنشره عبر الإنترنت. لذلك يجب التفريق بين الآراء الشخصية للموظفين والتصاريح الرسمية.
- الحرص على حماية سمعة المنظمة. تقلل سياسة التعامل والنشر في وسائل التواصل الاجتماعي للمنظمات من مخاطر المشكلات القانونية وتساعد على حماية المنظمة من خلال تحديد المخاطر المحتملة والخطوات التي يجب اتخاذها للموظفين في حالة اتخاذ إجراء سلبي.
- الحرص على وجود التناسق في كافة حسابات المنظمة في شبكات التواصل الاجتماعي المختلفة. قد تتعارض مشاركة واحدة غير مناسبة على أحد وسائل التواصل الاجتماعي مع توجهات وأهداف المنظمة. يمكن أن تساعد سياسة النشر في الشبكات الاجتماعية في خلق الاتساق عبر قنوات التواصل الاجتماعي المختلفة.

الضوابط الأمنية لحسابات التواصل الاجتماعي في المنظمات:

للإسهام في تقليل المخاطر المهددة لحسابات التواصل الاجتماعي الرسمية وتعزيز حمايتها في المملكة، قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكن الجهات من استخدام شبكات التواصل الاجتماعي بطريقة آمنة. حيث تم تحديد الضوابط كما يلي: (Social Media Accounts Cybersecurity Controls ’Organizations، ٢٠٢١)

- تقييم مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي في الجهات، مرة واحدة سنوياً على الأقل، وتوثيقها ومتابعتها بشكل مستمر.
- يجب تحديد وحصر حسابات التواصل الاجتماعي والأصول المعلوماتية والتقنية المتعلقة بها، وتحديثها مرة واحدة، كل سنة على الأقل.
- التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي داخل المنظمة.
- الاستخدام الآمن للأجهزة المخصصة لحسابات التواصل الاجتماعي والمحافظة عليها وحمايتها. وعدم احتوائها على بيانات مصنفة أو استخدامها لأغراض شخصية.
- التعامل الآمن مع هويات الدخول وكلمات المرور والأسئلة الأمنية.
- تحديد خطة استعادة حسابات التواصل الاجتماعي والتعامل مع الهجمات التي قد تتعرض لها.
- عدم استخدام حسابات التواصل الاجتماعي الرسمية لأغراض شخصية مثل التصفح.
- تجنب الدخول لحسابات التواصل الاجتماعي الرسمية باستخدام أجهزة أو شبكات عامة غير موثوقة.
- التسجيل في الحسابات الرسمية للجهات باستخدام معلومات رسمية (بريد إلكتروني رسمي خاص لوسائل التواصل الاجتماعي ورقم جوال رسمي)، وعدم استخدام معلومات شخصية.
- توثيق حسابات التواصل الاجتماعي الرسمية والمحافظة على هوية متسقة في جميع حسابات التواصل الاجتماعي المستخدمة؛ لتسهيل معرفة الحسابات الرسمية، واكتشاف حسابات الاحتيال.
- استخدام كلمة مرور آمنة وخاصة لكل حسابات التواصل الاجتماعي الرسمية. وتغير كلمة المرور بشكل دوري، وعدم إعادة استخدام كلمة مرور تم استخدامها من قبل.
- اعتماد استخدام المصادقة المتعددة لعمليات الدخول لحسابات التواصل الاجتماعي الرسمية.
- إدارة صلاحيات المستخدمين لحسابات التواصل الاجتماعي بناءً على احتياجات العمل، مع مراعاة حساسية الحسابات ومستوى الصلاحيات، ونوعية الأجهزة والأنظمة المستخدمة.
- الحرص على تطبيق حزم التحديثات والإصلاحات الأمنية لتطبيقات التواصل الاجتماعي، مرة واحدة شهرياً على الأقل.
- مراجعة إعدادات الحماية والتحصن لحسابات التواصل الاجتماعي للجهة والأصول التقنية الخاصة بها مرة واحدة كل سنة على الأقل.
- تفعيل جميع الإشعارات وتنبيهات الأمن السيبراني الخاصة بحسابات التواصل الاجتماعي وسجلات الأحداث Event Logs الخاصة بالأمن السيبراني على الأصول التقنية الخاصة بحسابات التواصل الاجتماعي.
- متابعة حسابات التواصل الاجتماعي ومراقبتها للتأكد من عدم نشر أي محتوى غير مصرح، أو تسجيل أي دخول غير مصرح.
- متابعة شبكات التواصل الاجتماعي ومراقبتها للتأكد من عدم انتحال هوية الجهة من أي طرف آخر.

تطبيق عملي (٧)

الهدف: أن يطبق المتدرب خاصية رفع مستوى الحماية في تطبيق Twitter.

الزمن: ١٠ دقائق

يعمل المتدربون على رفع مستوى الأمان في حساباتهم على شبكة التواصل الاجتماعي Twitter، وذلك لحماية بياناتهم ومحادثاتهم عن طريق تفعيل خاصية تسجيل الدخول بخطوتين (التحقق الثنائي).

الإرشادات:

١. يعمل المتدربون على الدخول على تطبيق Twitter في هواتفهم الذكية.
٢. الذهاب إلى الملف الشخصي > الإعدادات والخصوصية > الحساب > الأمان
٣. الضغط على خاصية تسجيل الدخول بخطوتين > اختر أحد الخيارات المتاحة (رسالة نصية) > أدخل رقم هاتفك وستصلك رسالة نصية فيها رمز مؤقت للتحقق > أدخل رمز التحقق > سيظهر لك في الشاشة رمزاً للاسترداد والذي يعتبر حلاً بديلاً يمكّنك من دخول حسابك في حال عدم إمكانية الوصول إلى رقم هاتفك.
٤. تأكّد من تعطيل خاصية السماح لتطبيق Twitter بالوصول إلى الموقع: من خلال الملف الشخصي > الإعدادات والخصوصية > الخصوصية والأمان
٥. اذهب إلى الموقع الجغرافي وقم بتعطيل الخاصية.

الموضوع الثامن: أمن المعلومات في الأجهزة المحمولة

بشكل عام، قد تتعرض الأجهزة المحمولة، مثل أجهزة الكمبيوتر المحمولة Laptops والأجهزة اللوحية Tablets والهواتف الذكية Smartphones، لتحديات أمنية أعلى من تلك التي تواجهها أجهزة الكمبيوتر المكتبية والخوادم، نتيجة لسهولة نقل الأجهزة المحمولة وحملها، حيث تزداد على سبيل المثال احتمالية تعرضها للسرقة كأحد أنواع الهجمات. لذلك لا بد من التركيز على الأمن المعلوماتي في الأجهزة المحمولة خاصة في ظل تزايد استخدامها الملحوظ. حيث إنه في عام ٢٠٢١ وصل عدد مستخدمي الإنترنت في جميع أنحاء العالم إلى ٤,٦٦ مليار مستخدم، منهم حوالي ٤,٣٢ مليار مستخدم يصلون إلى الإنترنت من خلال أجهزتهم المحمولة، وهذا ما يشكل ٩٢,٦% من إجمالي مستخدمي الإنترنت. (https://www.statista.com/, ٢٠٢١)

العنصر الأول: التهديدات الأمنية للأجهزة المحمولة:

تتعرض الأجهزة المحمولة للكثير من التهديدات الأمنية أهمها ما يلي: (Ciampa, ٢٠١٨)

- فقدان الجهاز:

أحد أهم مزايا الأجهزة المحمولة هو قابليتها للنقل مع المستخدم في أي مكان، ولكن هذه الميزة قد تشكل أحد أكبر نقاط الضعف فيها والتي يمكن استغلالها من خلالها. حيث إنه يمكن بسهولة فقدان هذه الأجهزة بسبب الضياع أو السرقة (تهديد الأمن المادي)، وبالتالي يمكن للشخص الذي تمكن من الحصول عليها استرداد أي بيانات غير محمية على الجهاز.

إضافة إلى الضياع أو السرقة، فإن مجرد استخدام الجهاز المحمول في مكان عام قد يشكل خطرًا في حال محاولة الأشخاص الآخرين استراق النظر إلى الجهاز خلال إدخال المستخدم لبيانات حساسة، مثل رقم بطاقة الائتمان أو كلمة المرور. لذلك يجب على المستخدمين التحقق من المنطقة المحيطة بهم قبل إدخال أي معلومات سرية في الأماكن العامة.

- ضعف التحديثات الأمنية لأنظمة التشغيل للأجهزة المحمولة:

حاليًا يوجد نظامي تشغيل الأكثر شيوعاً للاستخدام على الأجهزة المحمولة، نظام iOS من شركة Apple والذي يستخدم حكراً على أجهزتها، ونظام Android من شركة Google، وتُعد أولى الفروقات الأساسية بين النظامين أن Apple تعمل على تطوير النظام والأجهزة المشغلة معاً، أما Google فتعمل على دعم تطوير النظام فقط.

أما الفرق الثاني، أن نظام التشغيل iOS يعتبر نظام ذا بنية مغلقة ومملوكة closed and proprietary architecture لشركة Apple. كما أنه يعتمد iOS على متجر التطبيقات الخاص به، وهو جزء من Apple iTunes، كمصدر لتوزيع التطبيقات المعتمدة. لذلك عند الحاجة لتحديث النظام، يمكن لمستخدمي Apple إما التحديث من خلال iTunes أو من خلال over-the-air (OTA) update والتي توزعها Apple من خلال شركات الاتصالات اللاسلكية، وهذا يشبه الطريقة التي يتم بها توزيع التصحيحات patches الروتينية لأنظمةApple macOS و Microsoft Windows. ولكن هذا الأمر مختلف تماماً مع Google Android، وذلك لأن Android -على عكس iOS – يعتبر نظام مفتوح وغير مملوك ويمكن لأي شخص من استخدامه أو حتى تعديله (ومع ذلك، يجب أن تلتزم التعديلات بمعايير Google لتتمكن من الوصول إلى خدمات Google). لذلك، تعمل العديد

من الشركات المصنعة للأجهزة المحمولة في جميع أنحاء العالم على انتاج أجهزة تعتمد في تشغيلها على نظام Android لكونه متاح مجانًا. ثم يتم بيع هذه الهواتف بعد ذلك للمستهلكين من خلال شركات الاتصالات المختلفة.

بناءً على ذلك، ونظرًا لأن Google لا تنتج الأجهزة مثل Apple أو تتحكم في البنية التحتية للاتصالات اللاسلكية، فمن الصعب جدًا الاعتماد على شركات الاتصالات في توزيع تحديثات الأمان على الأجهزة للأسباب التالية:

- يقوم العديد من مصنعي الأجهزة المحمولة على تعديل نظامAndroid ، وبالتالي يكونون مترددين في توزيع التحديثات التي قد تتعارض مع تغييراتهم.
- تحتاج شركات الاتصالات اللاسلكية إلى إجراء اختبارات مكثفة للتأكد من أن التحديثات لا تسبب أي مشكلات في الشبكة، الأمر الذي يعتبر مكلف مادياً إضافة إلى إنه قد يستغرق وقتًا طويلاً.
- يتردد كل من مصنعي الأجهزة المحمولة وشركات الاتصالات اللاسلكية في توزيع تحديثات Google لأنه يحد من قدرتهم على تمييز أنفسهم عن المنافسين إذا بدأت جميع إصدارات Android في الظهور بنفس الشكل من خلال التحديثات.
- نظرًا لأن مصنعي الأجهزة المحمولة وشركات الاتصالات اللاسلكية يرغبون في بيع أكبر عدد ممكن من الأجهزة، فليس لديهم أي حافز مادي لتحديث الأجهزة المحمولة والذي سيجعل المستهلكين يستمرون في استخدامها إلى أجل غير مسمى.

ولكن لابد من الإشارة إلى أن شركة Google تبذل جهودًا مضاعفة لجعل تحديثات أمان Android متاحة بسهولة أكبر. وذلك من خلال رفع مستوى استقلالية نظام Android على الأجهزة عن طريق فصله عن برامج التشغيل والبرامج الثابتة الخاصة بالأجهزة hardware-specific drivers and firmware.

- <u>تتبع موقع الجهاز أو المستخدم:</u>

عادةً ما تكون الأجهزة المحمولة مزودة بنظام تحديد المواقع العالمي (GPS) والتي تعمل على تحديد الموقع الجغرافي للجهاز. حيث يتيح تحديد موقع المستخدم أو موقع عنوان يرغب الشخص في الوصول إليه. كما تُستخدم خدمات تحديد الموقع على نطاق واسع بواسطة وسائل التواصل الاجتماعي وأنظمة الملاحة وأنظمة الطقس والتطبيقات الأخرى في الجهاز المحمول.

ولكن هذه الخاصية قد تساعد للمهاجم في تحديد موقع المستخدم والجهاز الهدف، وقد يتم استخدام هذه المعلومات لمتابعة المستخدم لسرقة جهازه المحمول أو إلحاق الضرر به. بالإضافة إلى ذلك، يمكن للمهاجمين أن يجمعوا بمرور الوقت قائمة بالأشخاص الذين يرتبط بهم المستخدم وأنواع الأنشطة التي يؤدونها في مواقع معينة من أجل شن هجمات. من المخاطر ذات الصلة وضع معلومات GPS (وتسمى أيضًا العلامات الجغرافية)، والتي تضيف بيانات التعريف الجغرافي إلى الوسائط مثل الصور الرقمية التي تم التقاطها على جهاز محمول. وقد يقوم المستخدم بنشر صورة على أحد مواقع التواصل الاجتماعية، بتحديد موقع خاص دون قصد لأي شخص يمكنه الوصول إلى الصورة.

- التسجيل الصوتي أو المرئي غير المصرح به:

لطالما كانت الكاميرات والميكروفونات الموجودة على الأجهزة المحمولة هدفًا متكررًا للمهاجمين. من خلال استهداف جهاز من خلال البرمجيات الخبيثة، يمكن للمهاجم التجسس سراً على الضحية وتسجيل المحادثات أو مقاطع الفيديو. لذلك تتضمن بعض الاحتياطات الأساسية ضد التسجيل غير المصرح به ما يلي:

- لا تستخدم كاميرا الويب في أي برنامج محادثة غير موثوق فيه.
- لا تسمح بإذن الوصول إلى الكاميرا أو الميكروفون إلا للتطبيقات التي تتطلب هذا الاستخدام.
- يجب مراجعة أذونات التطبيقات بشكل دوري على الجهاز وإيقاف أي أذونات غير الضرورية.

- ثغرات الاتصالات:

من الممكن للمهاجمين استغلال الثغرات الأمنية للأجهزة المحمولة من خلال الاتصالات، حيث يمكن أن يتم ذلك في قيام المستخدم بالاتصال بالإنترنت من خلال الشبكات العامة والتي غالباً ما تكون مفتوحة وغير مؤمنة، وبالتاي تكون هدف للمهاجمين في التنصت على البيانات المرسلة من خلالها، أو من الممكن أن يتعرض الجهاز للهجمات من خلال مشاركة اتصال الانترنت مع جهاز آخر غير محمي، كأن يتم مشاركة الاتصال من خلال البلوتوث أو Wi-Fi.

- الوصول إلى محتوى غير آمن:

بشكل عام، تعتبر احتمالية الوصول إلى محتويات غير موثوق بها بواسطة الأجهزة المحمولة أعلى من أجهزة الكمبيوتر الأخرى. أحد أسباب ذلك هو انتشار استخدام رموز الاستجابة السريعة QR codes كالموضحة في شكل (٢٧)، والتي يمكن قراءتها بواسطة كاميرا الجهاز المحمول.

شكل (٢٧): *رمز الاستجابة السريعة QR code*

أصبحت رموز QR شائعة الاستخدام نظرًا لسرعة قراءتها وكبر سعتها التخزينية مقارنةً بالباركود التقليدي. يمكن لأكواد QR تخزين عناوين URL لمواقع الويب أو النص العادي أو أرقام الهواتف أو عناوين البريد الإلكتروني أو بيانات نصية أو رقمية بسعات تصل إلى ٤٢٩٦ حرفًا.

لذلك يمكن للمهاجم تصميم إعلان مفبرك منسوب إلى موقع ويب معروف، مثل انتحال صفة موقع أحد البنوك، ولكن يتضمن هذا الإعلان على رمز QR code الذي يحتوي على رابط ويب ذا محتوى ضار أو غير آمن. فبمجرد أن يلتقط المستخدم صورة لرمز الاستجابة السريعة QR code باستخدام كاميرا جهازه المحمول، يوجه الرمز متصفح الويب على الجهاز إلى موقع الويب المحتال للمهاجم أو إلى موقع يقوم بتنزيل البرامج الضارة على الفور. عادةً لا يمكن للمستخدمين تنزيل التطبيقات غير المعتمدة وتثبيتها على جهاز iOS أو Android. هذا لأنه يجب على المستخدمين الوصول إلى متجر تطبيقات Apple أو متجر Google Play لتنزيل تطبيق لتثبيته على الجهاز. ولكن في الواقع، يمكن للمستخدمين التحايل على القيود المضمنة المثبتة على هواتفهم الذكية من خلال عملية كسر الحماية jailbreaking على أجهزة Apple iOS أو rooting على أجهزة Android وذلك بهدف تحميل التطبيقات من غير المتاجر الرسمية والتي تحتوي على تطبيقات لم يتم فحصها والتأكد من خلوها من الثغرات الأمنية، لذلك قد تستجيب الأجهزة في هذه الحالة لطلبات تثبيت البرامج من خلال التحويل من QR codes.

إضافة إلى ذلك هناك وسيلة أخرى يمكن من خلالها أن يغزو المحتوى غير الموثوق به الأجهزة المحمولة وهي خدمة الرسائل القصيرة (SMS) رسائل الوسائط المتعددة (MMS) حيث يمكن لمهاجمين إرسال رسائل تحتوي على روابط لمحتوى غير موثوق به معد خصيصًا لإدخال برامج ضارة إلى الجهاز.

تطبيق عملي (٨)

الهدف: أن يحلل المتدرب أذونات التطبيقات في الهواتف الذكية.

الزمن: ١٥ دقيقة

يعمل المتدربون على استعراض التطبيقات المثبتة على أجهزتهم الذكية ومراجعة الأذونات المتاحة لها وتقييمها وإغلاق غير المستخدم منها.

الإرشادات:

١. يعمل المتدربون على الدخول على هواتفهم الذكية.
٢. الذهاب إلى الإعدادات Settings
٣. اختيار التطبيقات Application
٤. يعمل المتدرب على تحليل الأذونات Permissions للتطبيقات الحالية، والعمل على إغلاق غير المستخدم منها.
٥. يقوم المدرب بمناقشة النتائج مع المتدربين.

العنصر الثاني: الضوابط الأمنية لحماية الأجهزة المحمولة:

لرفع مستوى الأمن في الأجهزة المحمولة، يجب بحد أدنى تطبيق الإجراءات الأمنية التالية: (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- قفل الشاشة Screen lock:

يجب إعداد شاشة الجهاز ليتم إقفالها آلياً أذا لم يتم استخدامها لفترة زمنية قصيرة. بحيث يتوجب على المستخدم في حالة رغبته الوصول إلى نظام التشغيل من تسجيل الدخول من جديد (من خلال كلمة المرور أو غيرها من آليات المصادقة) بعد محاولات محدود.

- كلمة سر قوية:

تعد كلمات المرور القوية مهمة دائمًا، ولكن تبرز أهميتها بشكل أكبر في الأجهزة المحمولة نظراً لكون احتمالية ضياعها أو سرقتها أكبر، مما يتيح للشخص الذي تصل إلى يديه ان تكون لديه فرصة أكبر في محاولة كسر كلمة المرور والوصول إلى البيانات. يمكن أيضًا رفع مستوى الحماية عن طريق المصادقة باستخدام القياسات الحيوية، حيث يعد اليوم استخدام بصمة الإصبع أو حتى التعرف على الوجه أمرًا شائعًا جدًا في الهواتف الذكية.

- تشفير الجهاز:

يجب الحرص على تشفير البيانات الموجودة على الجهاز بحيث إذا وقعت في يد شخص غير المستخدم الفعلي، فلا يمكن الوصول إليها بشكل قابل للاستخدام (أو مفهوم) بدون كلمات المرور الصحيحة. وهناك العديد من البرامج والتطبيقات التي يمكن استخدامها لهذا الغرض.

- استخدام خاصية مسح البيانات عن بعد Remote Wipe:

هناك العديد من البرامج والتطبيقات التي تقوم بإرسال أمر إلى جهاز محمول بهدف بمسح البيانات الموجودة على هذا الجهاز عن بُعد. وهي مخصصة للاستخدام في حالة سرقة الجهاز أو لإعادة تخصيصه لمستخدم آخر.

- تتبع نظام تحديد المواقع GPS:

في حالة سرقة الجهاز، يمكن استخدام نظام تحديد المواقع العالمي (GPS) لتحديد موقع الجهاز والسماح للجهات المختصة من العثور عليه.

- استخدام خاصية Geofencing:

يعتمد Geofencing على تتبع GPS، ولكنه يصل إلى أبعد من تتبع الجغرافي للجهاز. حيث تعتمد هذه الخاصية على استخدام المحيط (السياج) الجغرافي الذي يجعل الجهاز لا يعمل إلا إذا كان ضمن مواقع جغرافية معينة. لذلك، تعمل بعض المنظمات على

ضبط هذه الخاصية على أجهزة المنظمة المحمولة، بحيث إذا تمت سرقة الجهاز فإنه لن يعمل هذا الجهاز خارج محيط المنظمة المُحدد له سابقاً.

- التحكم في أذونات التطبيقات Application Permissions:

يهتم التحكم في أذونات التطبيقات المثبتة على الجهاز المحمول من خلال متابعة التطبيقات والحرص على تعطيل الخدمات غير المستخدمة أو التي من المفترض ألا يحتاجها التطبيق.

إضافة إلى ما سبق، يوصي المركز الوطني الإرشادي للأمن السيبراني على اتباع الإجراءات الأمنية الموضحة في جدول (١١) للتعامل مع الأجهزة المحمولة.

جدول (١١): *توصيات المركز الوطني الإرشادي للأمن السيبراني في ا لتعامل مع الأجهزة المحمولة.*

عند التخلص من الجهاز المحمول	عند سرقة أو ضياع الجهاز المحمول
• الحرص على إتلاف شرائح تخزين البيانات وحذف الملفات • الحرص على حذف المعلومات والتطبيقات البنكية • إعادة الجهاز إلى الإعدادات المصنعية	• تفعيل خاصية العثور عن الجهاز عن طريق android.com/findأوicloud.com/#find • اتباع تعليمات الشركة المصنعة لإقفال الأجهزة عن بعد وحذف البيانات • لكل جهاز رقم هوية (IMSI) تجده في صندوقه الأصلي، يمكن استخدامه لإبلاغ مقدّمي خدمات الاتصالات بالمملكة لحجبه

تطبيق عملي (٩)

الهدف: أن يطبق المتدرب خاصية رفع مستوى الحماية في تطبيق WhatsApp.

الزمن: ١٠ دقائق

يعمل المتدربون على رفع مستوى الأمان على حساباتهم في تطبيق WhatsApp الشائع الاستخدام، وذلك لحماية بياناتهم ومحادثاتهم عن طريق تفعيل خاصية التحقق بخطوتين.

الإرشادات:

١. يعمل المتدربون على الدخول على تطبيق WhatsApp في هواتفهم الذكية.
٢. الذهاب إلى الإعدادات Settings
٣. اختيار خيار الحساب Account
٤. اختيار التحقق بخطوتين Two-step verification
٥. تفعيل الخاصية
٦. إدخال رقم سري خاص بتطبيق WhatsApp
٧. إدخال البريد الإلكتروني وسيتم تفعيل الخاصية.

الموضوع التاسع: التشفير

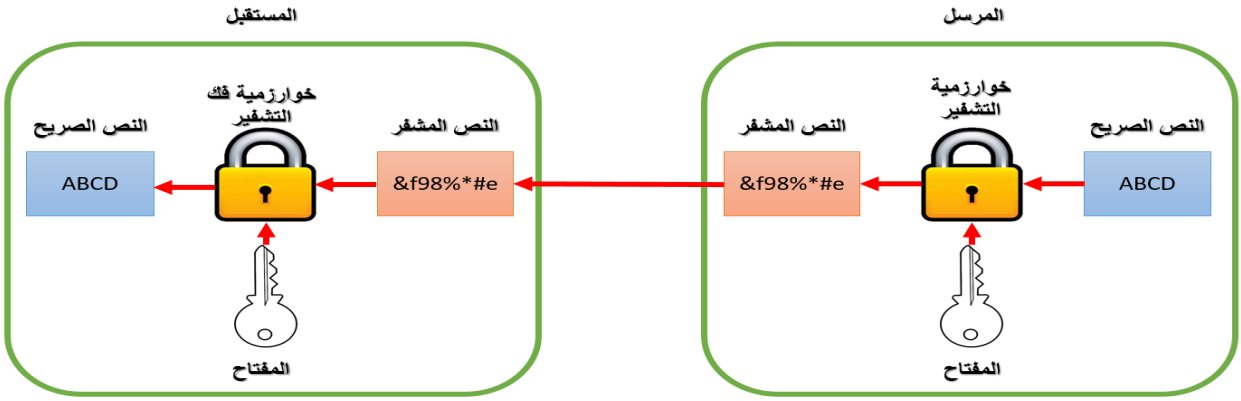
العنصر الأول: مقدمة في التشفير Cryptography:

يُعرف التشفير أو التعمية بأنها: 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 التشفير التالي: "التشفير 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 المصرح لهم فقط، الذين لديهم الأدوات اللازمة لذلك". (القحطاني، ٢٠١٥)

ويتألف التشفير من عمليتين أساسيتين هما: التشفير، وفك التشفير، والذي يتطلب تنفيذهما وجود مفتاح للتشفير. وبحسب نوعية التشفير، فإنه يمكن استخدام مفتاح تشفير أو أكثر لإتمام هاتين العمليتين. وعموماً، فهناك مصطلحات أساسية، وهي:

- النص الصريح Plain Text : وهو الرسالة أو (البيانات) الأصلية قبل إجراء أي عملية عليها.
- النص المشفر Cipher Text : يطق على الرسالة المشفرة بعد أن تشفر.
- التشفير Encryption : تحويل الرسالة من نص صريح إلى نص مشفر.
- فك التشفير Decryption : استرجاع النص الصريح من النص المشفر.
- خوارزمية التشفير Encryption Algorithm : مجموعة الخطوات والعمليات الرياضية التي يتم إتباعها لتحويل النص الصريح إلى نص مشفر.
- خوارزمية فك التشفير Decryption Algorithm : وهي الخوارزمية العكسية لخوارزمية التشفير لاسترجاع النص الصريح من النص المشفر.
- تحليل الشفرة Cryptanalysis : ويطلق عليها أيضاً (كسر الشيفرة): وتعني التقنيات المستخدمة لفك تشفير رسالة بطريقة غير شرعية، أي كسر تشفيرها بواسطة طرف غير مصرح له، ولا يعرف المفاتيح اللازمة لذلك.
- المفتاح السري Key: وهو عبارة عن قيمة غير معتمدة على الرسالة يتم اختيارها من قبل نظام التشفير أو المستخدم.

ويوضح شكل (٢٨) دور عناصر التشفير بعملية التشفير.



شكل (٢٨): عملية التشفير

يمكن أن يوفر التشفير مجموعة من وسائل الحماية الأمنية التالية: (Ciampa, ٢٠١٨):

- السرية Confidentiality: يمكن أن يحمي التشفير سرية المعلومات من خلال ضمان أن الأطراف المصرح لهم فقط هم من لديهم القدرة على استعراضها كونهم يملكون مفاتيح التشفير.
- النزاهة Integrity: يمكن أن يحمي التشفير سلامة المعلومات. لكون النزاهة تضمن صحة المعلومات ولم يقم أي شخص غير مصرح له أو برامج ضارة بتغيير تلك البيانات. نظرًا لأن النص المشفر يتطلب استخدام مفتاح معين لفك تشفير البيانات قبل أن يتم تعديلها.
- المصادقة Authentication: يمكن التحقق من هوية المرسل أو المستقبل من خلال التشفير، من خلال إثبات هويتهم من خلال مفاتيح التشفير التي يملكونها.
- عدم التنصل Non-repudiation: يمكن أن يفرض التشفير وسيلة لإثبات عدم التنصل. في تقنية المعلومات، عدم التنصل هو عملية إثبات قيام المستخدم بإجراء ما، مثل إرسال رسالة بريد إلكتروني.
- التعتيم Obfuscation: التعتيم هو انتاج شيء غامض أو غير واضح. يمكن أن يساعد التشفير في ضمان التعتيم عن طريق إخفاء تفاصيل البيانات الأصلية بحيث لا يتمكن للمستخدم غير المصرح له من رؤيتها.
-

أنواع التشفير:

بشكل عام، قوة التشفير تكمن في سرية المفتاح السري وقوته، وليس في إبقاء خوارزمية التشفير سرية. فمن المعروف ألا تبقى الخوارزمية سرية وأن تكون معروفة حتى يمكن تطويرها من حين لآخر. وللحصول على مفاتيح سر قوية فإنه يمكن اتباع التالي:

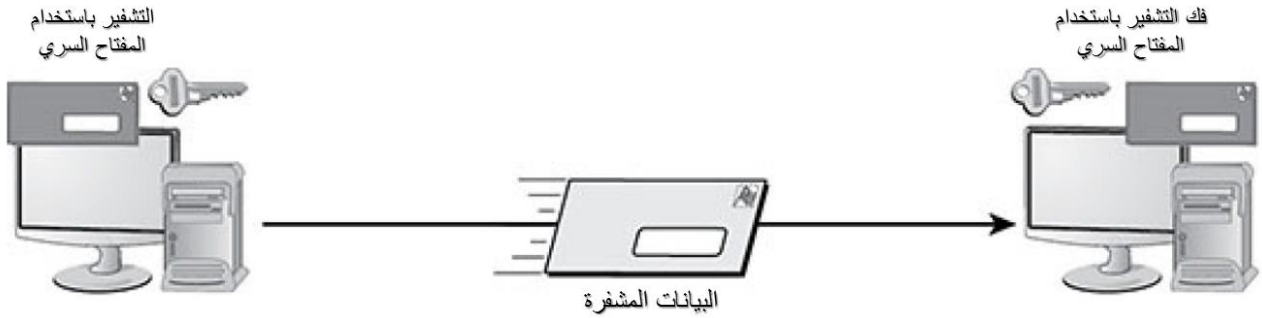
- إنتاج المفاتيح السرية بشكل آلي من قبل النظام، وليس من قبل المستخدم.
- استخدام مفاتيح سرية عشوائية مختلفة لكل عملية إرسال مختلفة.
- استخدام مفاتيح سرية طويلة لا تقل عن ٢٥٦ بت(Bit) .
- استخدام مفاتيح سرية في صيغتها الثنائية (١,٠) فقط وليس في صيغتها المعتادة (الحروف والأرقام المعتادة).

بناءً على ذلك، تنقسم خوارزميات التشفير الحديث إلى ثلاثة أنواع رئيسية: التشفير المتناظر symmetric cryptography، والتشفير غير المتناظر asymmetric cryptography، وخوارزميات التجزئة hashing algorithms. وفيما يلي نستعرض الأنواع الثلاثة، والفروق بينها، والحاجة لكل منها. (Emmett Dulaney and Chuck Easttom, ٢٠١٨).

- <u>التشفير المتناظر Symmetric cryptography:</u>

تتطلب خوارزميات التشفير المتناظر symmetric cryptography أن يقوم كل من المرسل والمستقبل بتشفير وفك شفرة الرسالة باستخدام نفس الخوارزمية ونفس المفتاح. حيث تعتمد خوارزميات التشفير المتناظرة على إنشاء مفتاح سري واحد والذي يجب حمايته. المفتاح المتناظر، الذي يشار إليه أحيانًا بالمفتاح السري secret key، هو عبارة عن مفتاح لا يتم الكشف عنه إلا للأشخاص المصرح لهم باستخدام خوارزمية التشفير. لأن مجرد إن الكشف عن هذا المفتاح السري لأي طرف غير مصرح له يعني انتهاك أمان نظام التشفير. لذلك تتطلب المفاتيح في التشفير المتناظر لمعالجة خاصة لحمايتها. يجب توزيع مفتاح التشفير بين

الأطراف المرسلة والمستقبلة بطريقة آمنة جداً. ويمكن لعملية التوزيع هذه أن تتم بشكل تقليدي (عن طريق قنوات آمنة غير إلكترونية) أو بإنتاج هذه المفاتيح بطريقة آلية آمنة ضمن نظام التشفير، بحيث يتم إنتاج نفس المفتاح عند المرسل والمستقبل. إضافة إلى ذلك، يجب توزيع مفتاح التشفير بين الأطراف المرسلة والمستقبلة بطريقة آمنة جداً. ويمكن لعملية التوزيع هذه أن تتم بشكل تقليدي (عن طريق قنوات آمنة غير إلكترونية) أو بإنتاج هذه المفاتيح بطريقة آلية آمنة ضمن نظام التشفير، بحيث يتم إنتاج نفس المفتاح عند المرسل والمستقبل. يوضح شكل (٢٩): نظام تشفير متناظر، والذي يستخدم نفس المفتاح لكل من عملية التشفير وفك التشفير.



شكل (٢٩): *التشفير المتناظر Symmetric Cryptography*

وللحصول على نظام تشفير متناظر آمن. فإنه يجب تحقيق الشرطين التاليين:

- استخدام خوارزمية تشفير (وفك تشفير) قوية: والخوارزمية القوية هي التي لا يمكن إرجاع النصوص المشفرة المنتجة منها إلى نصوص صريحة، حتى ولو كانت الخوارزمية نفسها معروفة عند من يحاول فك التشفير (المهاجم). وعموماً فإن خوارزمية التشفير القوية هي التي يكون فيها المهاجم غير قادر على فك تشفير النص المشفر أو اكتشاف المفاتيح السرية، حتى ولو توفر لدية عدد من النصوص الصريحة والنصوص المشفرة المقابلة لها.
- يجب توزيع المفتاح على كل من المرسل والمستقبل بشكل آمن: وأن يبقى هذا المفتاح سرياً بينهما. فلو حصل أحد على المفتاح السري فإنه يصبح بإمكانه فك تشفير الرسائل المشفرة باستخدام خوارزمية التشفير التي عادة ما تكون معروفة عند الجميع.

تستخدم العديد من أنظمة التشفير الناجحة الخوارزميات المتناظرة والتي يصعب كسرها لقوتها. فيما يلي بعض المعايير الشائعة التي تستخدم الخوارزميات المتناظرة: (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

❖ Data Encryption Standard (DES) :

تم استخدام هذا المعيار منذ السبعينيات القرن الماضي. حيث كان يعتبر معيار التشفير الأساسي المستخدم في المعلومات الحكومية والصناعية حتى تم استبداله بمعيارAES . يعتمد DES على مفتاح بطول ٥٦ بت، وله العديد من الأوضاع التي توفر السرية والنزاهة. ولكنه يعتبر الآن غير آمن بسبب حجم المفتاح الصغير.

❖ Triple-DES (٣DES):

هذا المعيار –والمستخدم حتى الآن-عبارة عن تطوير للمعيار السابق DES، ولكن يعد كسر ٣ DESأصعب بكثير من العديد من الأنظمة الأخرى، وهو أكثر أمانًا من DES كونه يستخدم مفتاح بطول ١٦٨ بت، أي ٣ أضعاف طول مفتاح DES.

❖ Advanced Encryption Standard (AES):

حل هذا المعيار محل DES كمعيار تشفير يستخدم خوارزميةRijndael ، هو الخيار المفضل حالياً للتطبيقات الحكومية. حيث يدعم أحجام مفاتيح متعددة، مثل ١٢٨، ١٩٢، و٢٥٦ بت، ولكن يعتبر ١٢٨ بت هو الحجم الافتراضي.

بشكل عام، تكمن عيوب خوارزميات التشفير المتناظرة في الوقت المستغرق في عملية التشفير واستهلاكها للطاقة، بالإضافة إلى ضرورة حماية المفتاح السري ومنعه من التسرب إلى الأطراف غير المخول لها بالاطلاع عليه.

- التشفير غير المتناظر Asymmetric cryptography:

تعتمد الخوارزميات غير المتناظرة على استخدام مفتاحين مختلفين لتشفير البيانات وفك تشفيرها. يشار إلى هذه المفاتيح غير المتناظرة بالمفتاح العام Public key والمفتاح الخاص Private Key. حيث يستخدم المرسل المفتاح العام لتشفير رسالة، ويستخدم المُستقبل المفتاح الخاص لفك تشفير الرسالة. كما يشير الاسم، يكون المفتاح العام عامًا حقًا يطلع عليه أي طرف يرغب بالتواصل مع المتلقي، على أن يتم الاحتفاظ بالمفتاح الخاص خاصًا، ولا يعرفه سوى المالك (المتلقي). بناءً على ذلك، إذا أراد شخص ما إرسال رسالة مشفرة إليك، فيمكنه استخدام مفتاحك العام لتشفير الرسالة ثم إرسال الرسالة إليك. من جهتك يمكنك استخدام مفتاحك الخاص لفك تشفير الرسالة. على أن يتم فرض الحماية والسرية على المفتاح الخاص. إذا انكشف كلا المفتاحين لطرف ثالث، يكون بذلك قد تم انتهاك نظام التشفير.

الفكرة الحقيقي لهذه الأنظمة هو أنه لا يمكن استخدام المفتاح العام لفك تشفير رسالة، يمكن فقط للمفتاح الخاص القيام بذلك، كما هو موضح في شكل (٣٠)، لذلك لا يوجد أي حاجة لتبادل المفاتيح بطريقة سرية، كون المفتاح العام مُعلن في الأصل.

شكل (٣٠): *التشفير غير المتناظر Asymmetric cryptography*

حالياً يوجد أربعة أنظمة شائعة الاستخدام للتشفير غير المتناظر، وهي كما يلي: (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

❖ RSA:

تعتمد خوارزمية RSA على استخدام أعدادًا صحيحة كبيرة كأساس لعملية توليد المفاتيح. تم تنفيذ هذه الخوارزمية على نطاق واسع، وأصبحت معيارًا من معايير التشفير. يعمل RSA في كل من التشفير والتوقيعات الرقمية Digital

Signatures، كما تم استخدامه العديد من البيئات، مثل Secure Sockets Layer (SSL)، ويمكن استخدامه في عمليات تبادل المفاتيح.

❖ Diffie-Hellman:

تعتبر من الأنظمة التي أسست مفهوم المفتاح العام والخاص. حيث تُستخدم هذه الخوارزمية بشكل أساسي لتبادل المفاتيح عبر الشبكات العامة.

❖ Elliptic Curve Cryptography (ECC):

عبارة عن نظام يوفر وظائف مماثلة لنظام RSA ولكنه يستخدم أحجام مفاتيح أصغر مع الحصول على نفس مستوى الأمان. من المتوقع أن يتم تنفيذ ECC بشكل شائع في الأجهزة المحمولة في المستقبل القريب.

❖ ElGamal:

تعتبر خوارزمية تشفير غير متناظرة تم إطلاق العديد من الإصدارات منها. تعتمد هذه الخوارزمية على ما يسمى بالمفتاح المؤقت. المفتاح المؤقت هو ببساطة مفتاح تشفير يستخدم لجلسة اتصال واحدة فقط Communication Session، ولا يتم استخدامه مرة أخرى.

- خوارزميات الاختزال Hashing algorithms:

تعتبر من خوارزميات التشفير التي تعمل على انشاء بصمة رقميةHash Value فريدة لكل لمجموعة من البيانات. تسمى هذه العملية بالاختزال، والبصمة الناتجة عبارة عن ملخص لمحتوى البيانات. تستخدم Hashing algorithms في المقام الأول لأغراض المقارنة.

على الرغم من أن الاختزال عبارة عن خوارزمية تشفير أحادية الاتجاه one-way، إلا أن الغرض منها ليس إنشاء نص مشفر يمكن فك تشفيره لاحقًا. بدلاً من ذلك، يُقصد بهذه الخوارزميات هو أنتاج بصمة (أو ملخص) لأي كتلة بيانات، ولكن بطريقة لا يمكن عكسها، بمعنى لا يمكن من خلال معرفة البصمة الرقمية التوصل إلى البيانات الأصلية كون هذه العملية تعمل باتجاه واحد. بناءً على ذلك تعتبر خوارزمية الاختزال آمنة إذا كانت تحتوي على هذه الخصائص: (Ciampa, ٢٠١٨)

- حجم ثابت للبصمة الرقمية: يجب أن يتم انتاج بصمة رقمية (ملخص) ذو حجم موحد بغض النظر عن حجم البيانات الأصلية التي تم استخلاص البصمة منها.
- بصمة رقمية فريدة: لا يمكن لمجموعتين مختلفتين من البيانات إنتاج نفس البصمة. يجب أن ينتج عن تغيير حرف واحد في مجموعة بيانات واحدة بصمة مختلفة تمامًا.
- بصمة مستقلة: لا ينبغي أن يكون من الممكن إنتاج بصمات يتم تحديدها مسبقًا.
- خوارزمية آمنة: لا يمكن عكس الخوارزمية لتحديد النص الأصلي من خلال البصمة.

غالبًا ما يتم استخدام Hashing algorithms في مطابقة كلمات المرور وفي عمليات التحقق من البيانات (النزاهة) وأن المحتويات الأصلية لم يتم التعديل عليها. على سبيل المثال، غالبًا ما يتم استخدام هذه الخوارزميات لإنتاج البصمات الرقمية للملفات التي يمكن تنزيلها من مواقع الويب. بعد تنزيل الملف، يمكن للمستخدم إنشاء بصمة خاص به على الملف ثم مقارنته بقيمة البصمة المنشورة على موقع الويب. يشير التطابق في البصمات إلى عدم وجود تعديل في الملف الأصلي.

أكثر خوارزميات التجزئة شيوعًا هي Message Digest ٥ و Secure Hash Algorithm و RACE Integrity Primitives Assessment Message Digest و Hashed Message Authentication Code.

تطبيق عملي (١٠)

الهدف: أن يطبق المتدرب خاصية إنتاج البصمة الرقمية لبيانات مختلفة.

الزمن: ١٠ دقائق

يعمل المتدربون على انتاج بصمات رقمية Hash Values لبيانات متعددة باستخدام دوال الاختزال Hash Functions المختلفة.

الإرشادات:

١. يعمل المتدربون على الدخول على الرابط https://www.fileformat.info/tool/hash.htm

٢. من جزء String Hash، قم بإدخال أي نص في حقل Text ثم اضغط على زر Hash الموجود أسفل الحقل مباشرة.

٣. قم بالنزول إلى أسفل الصفحة وقارن نتائج البصمات الرقمية Hash Value التي تم انتاجها باستخدام دوال الاختزال المختلفة.

٤. قم بإعادة التمرين باستخدام نصوص مختلفة وقارن النتائج.

٥. يقوم المدرب بمناقشة النتائج مع المتدربين.

العنصر الثاني: الشهادات الرقمية:

كما ذكرنا سابقاً، تعتمد أنظمة التشفير غير المتناظر والتي تعتمد على نوعين من المفاتيح، المفتاح العام (مُعلن) والمفتاح الخاص (سري)، بحيث لو أراد الطرف (أ) ارسال رسالة إلى الطرف (ب)، فعلى (أ) تشفير الرسالة باستخدام المفتاح العام للطرف (ب) والذي يقوم (ب) بالإعلان عنه، وعندما تصل الرسالة إلى (ب) فأنه يجب عليه فك تشفيرها باستخدام المفتاح الخاص الذي يملكه. ولكن مع انتشار أنظمة التشفير غير المتناظر وتطبيقها في مجالات عدة، مع زيادة معدلات الجرائم الالكترونية، يظهر السؤال التالي: ما الذي يثبت للطرف (أ) أن المفتاح العام المعلن عنه على أنه للطرف (ب) هو فعلاً له وليس مفتاح عام لمهاجم ينتحل هوية الطرف (ب) حتى يتمكن من الاطلاع على جميع الرسائل المرسلة إلى (ب) بعد أن يتمكن من فك تشفيرها باستخدام المفتاح الخاص الذي يملكه والمرتبط بالمفتاح العام المفبرك؟ الجواب هو من خلال الشهادات الرقمية التي تعمل على إثبات علاقة المفاتيح العامة بأصحابها بواسطة طرف ثالث موثوق به يملك الصلاحية لإصدارها.

بناءً على السيناريو السابق، تعرف الشهادة الرقمية على أنها تقنية تُستخدم لربط هوية المستخدم بالمفتاح العام الذي يملكه على أن يتم توثيق الشهادة وتوقيعها رقمياً بواسطة طرف ثالث موثوق به، يتحقق من المالك وأن المفتاح العام يخصه. (Ciampa, ٢٠١٨)

يتم إصدار الشهادات الرقمية بناءً على معيار X.٥٠٩ والمعتمد من قبل Telecommunication Standardization Sector (ITU-T).

تطبيق عملي (١١)

الهدف: أن يتعرف المتدرب على الشهادات الرقمية بشكل أعمق.

الزمن: ١٠ دقائق

يعمل المتدربون على استعراض معلومات الشهادة الرقمية باستخدام متصفح الويب Google Chrome.

الإرشادات:

١. يعمل المتدربون على استخدام متصفح الويب Google Chrome للذهاب إلى www.google.com.

٢. ماذا تعني علامة القفل (🔒) الموجودة بجانب العنوان Address bar؟ وهل هو باللون الأخضر أم الأحمر؟ هل هو مفتوح أم مغلق؟

٣. انقر فوق علامة (⋮) الموجودة في أقصى اليمين في شريط العناوين.

٤. انقر على More Tools.

٥. قم باختيار Developer tools.

٦. اختر تبويب Security (إذا لم تظهر علامة التبويب، فانقر فوق الزر >> لعرض المزيد من نوافذ التبويب)، استعرض البيانات الظاهرة؟ ماهي حالة شهادة الموقع Certificate؟ ماهي حالة الاتصال Connection؟

٧. اضغط على الزر View certificate. استعرض البيانات الموجودة في تبويب General، ما هو تاريخ انتهاء شهادة الموقع؟

٨. انتقل إلى التبويب Details واستعرض البيانات الموجودة، ما هو المفتاح العام للموقع؟

٩. انتقل إلى التبويب Certification Path واستعرض البيانات الموجودة، ما هو مسار إصدار شهادة الموقع؟

١٠. يقوم المدرب بمناقشة النتائج مع المتدربين.

العنصر الثالث: إدارة الشهادات الرقمية:

يتم توظيف العديد من الكيانات والتقنيات لإدارة الشهادات الرقمية. وتشمل هذه سلطات تصديق الشهادات الرقمية Certificate Authorities (CA) وأدوات إدارة الشهادات. ومن الممكن توضيح هذه الكيانات والتقنيات فيما يلي: (Ciampa, ٢٠١٨)

- سلطة تصديق الشهادات الرقمية Certificate Authority (CA) :

إذا أراد المستخدم إصدار شهادة رقمية خاصة به، فيجب عليه، بعد توليد المفاتيح العامة والخاصة التي سيستخدمها في اتصالاته، أن يقوم بإكمال نموذج طلب توقيع الشهادة Certificate Signing Request (CSR) ويعمل على توقيعه رقمياً من خلال إلصاق مفتاحه العام ثم إرساله إلى سلطة التصديق (CA). تقوم سلطة التصديق بمعالجة طلب CSR والتحقق من مصداقية المستخدم قبل إصدار الشهادة الرقمية.

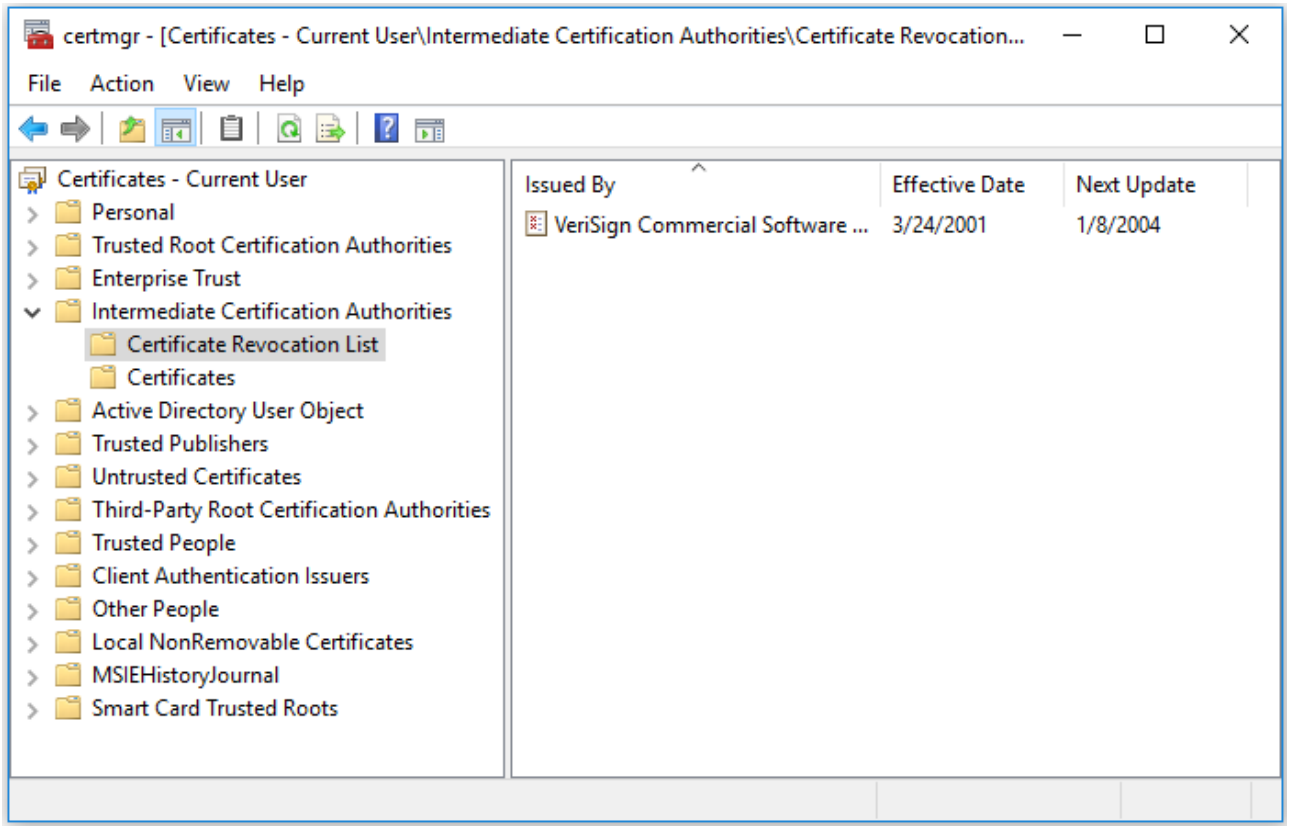
هناك العديد من سلطات التصديق الحكومية مثل المركز الوطني للتصديق الرقمي في المملكة العربية السعودية https://www.ncdc.gov.sa/، أو سلطات التصديق التجارية مثل VeriSign و goDaddy.

- إدارة الشهادات:

هناك العديد من الكيانات التي تُعد كسلطات تصديق الشهادات التي تعتمد على أنظمة قوية لإدارة الشهادات الرقمية. حيث تتضمن هذه الأنظمة ما يلي:

- مستودع الشهادات Certificate Repository (CR) هو دليل مركزي للشهادات الرقمية متاح للعموم يمكن استخدامه لعرض حالة الشهادة الرقمية. يمكن إدارة هذا الدليل محليًا عن طريق إعداده كمنطقة تخزين متصلة بخادم CA.
- إبطال الشهادات، عادةً ما يكون للشهادات الرقمية تاريخ انتهاء صلاحية، مثل سنة واحدة من تاريخ إصدارها. ومع ذلك، هناك ظروف قد تكون سببًا لإلغاء الشهادة قبل انتهاء صلاحيتها. قد تكون بعض الأسباب بسيطة، مثل عدم استخدام الشهادة أو تغيير تفاصيل الشهادة، مثل عنوان المستخدم. قد تكون الظروف الأخرى أكثر خطورة. على سبيل المثال، إذا قام شخص ما بسرقة المفتاح الخاص للمستخدم، فيمكنه انتحال شخصية الضحية من خلال استخدام الشهادات الرقمية دون علم المستخدمين الآخرين بذلك. من المهم أن تنشر CA الشهادات المعتمدة وكذلك الشهادات الملغاة في الوقت المناسب حتى لا تتعرض البيانات والاتصالات للخطر.

هناك طريقتان يمكن من خلالها التحقق من حالة الشهادة لمعرفة ما إذا كانت سارية أو تم إبطالها. الأولى هي استخدام قائمة الشهادات الملغاة Certificate Revocation List (CRL)، وهي قائمة بالأرقام التسلسلية للشهادة التي تم إبطالها. تحتفظ العديد من سلطات التصديق بقائمة بالشهادات الملغاة عبر الإنترنت التي يمكن الاستعلام عنها بإدخال الرقم التسلسلي للشهادة. بالإضافة إلى ذلك، تتلقى أنظمة التشغيل في أجهزة الكمبيوتر المحلي تحديثات عن حالة الشهادات وتحتفظ بقائمة إلغاء الشهادات المحلية، كما هو موضح في شكل (٣١): قائمة الشهادات الملغاة في نظام ويندوز.



شكل (٣١): *Certificate Revocation List (CRL)*

أما الطريقة الثانية فهي من خلال بروتوكول حالة الشهادة عبر الإنترنت Online Certificate Status Protocol (OCSP)، والذي يقوم بإجراء بحث فوري عن حالة الشهادة عن طلبها. حيث يرسل متصفح الويب معلومات الشهادة إلى كيان موثوق به مثل CA، لتوفير معلومات صلاحية الشهادة المحددة. (Ciampa, ٢٠١٨)

تطبيق عملي (١٢)

الهدف: أن يتعرف المتدرب على قائمة الشهادات الرقمية الملغاة.

الزمن: ١٠ دقائق

يعمل المتدربون على استعراض قائمة الشهادات الملغاة Certificate Revocation List (CRL) وأي شهادات غير موثوق بها على جهاز الكمبيوتر الذي يعمل بنظام التشغيل Microsoft Windows.

الإرشادات:

١. اضغط على زر الويندوز في لوحة المفاتيح + x.
٢. اختر Command Prompt (Admin) من القائمة الظاهرة.
٣. اكتب في الشاشة الظاهرة الأمر certmgr.msc ثم اضغط Enter.
٤. ستظهر أمامك شاشة إدارة الشهادات الرقمية، من الجزء الأيسر من الشاشة قم باختيار Trusted Root Certification Authorities.
٥. اضغط على Certificates، ستظهر لك قائمة سلطات التصديق CA المعتمدة على جهاز الكمبيوتر. قم باستعراض الشهادات الرقمية الخاصة بهم.
٦. من الجزء الأيسر من الشاشة قم باختيار Intermediate Certification Authorities.
٧. اضغط على Certificate Revocation List، ستظهر لك قائمة سيتم عرض كافة الشهادات الملغاة. قم باستعراض الشهادات الرقمية الظاهرة.
٨. من الجزء الأيسر من الشاشة قم باختيار Untrusted Certificates.
٩. اضغط على Certificates، يتم سرد الشهادات التي لم تعد موثوقة في الجزء الأيسر.
١٠. يقوم المدرب بمناقشة النتائج مع المتدربين.

العنصر الرابع: البنية التحتية للمفاتيح العامة:

تعد البنية التحتية للمفتاح العام Public Key Infrastructure (PKI) إحدى أدوات الإدارة المهمة لاستخدام الشهادات الرقمية والتشفير غير المتناظر. لذلك من المهم فهم البنية التحتية للمفتاح العام، وكيفية إدارتها وكيفية تنفيذ إدارة المفاتيح والشهادات الرقمية.

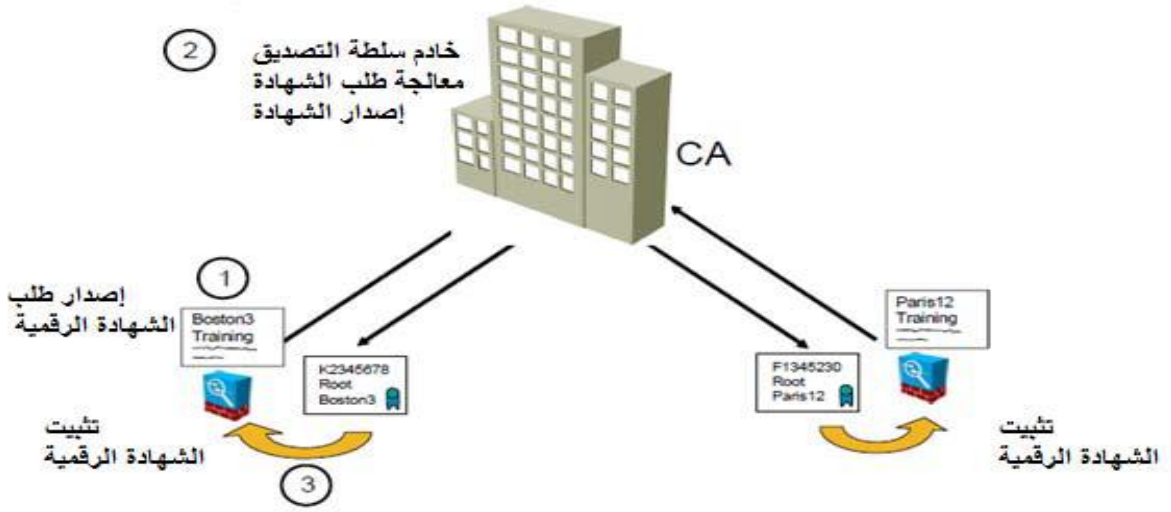
تُعرف البنية التحتية للمفتاح العام (PKI) على إنها البنية التحتية الأساسية لإدارة المفاتيح العامة المستخدمة في الشهادات الرقمية. لذلك هو إطار عمل لجميع الكيانات المشاركة في الشهادات الرقمية لإدارة الشهادات الرقمية بما في ذلك الأجهزة والبرامج والأشخاص والسياسات والإجراءات بهدف إنشاء الشهادات الرقمية وتخزينها وتوزيعها وإبطالها. (Ciampa, ٢٠١٨)

مكونات البنية التحتية للمفاتيح العامة PKI:

- سلطة التصديق CA: تمثل المرجعية في الثقة في البنية التحتية للمفتاح العام وتوفر الخدمات التي تصادق على هوية الأفراد، والحواسيب، والكيانات الأخرى في الشبكة.
- سلطة التسجيل: تقوم سلطة التسجيل بوظائف التحقق الشخصي من هوية ووثائق مقدم طلب الشهادة الرقمية.
- الشهادة الرقمية: بنية البيانات المعرفة في المعيار X.٥٠٩ موقعة رقمياً من قبل سلطة التصديق ويتم فيها ربط هوية حامل شهادة (أو الخدمة) بالمفتاح العام.
- قاعدة بيانات (مجلد نشط) لحفظ الشهادات الرقمية.
- نظام إدارة الشهادات الرقمية.
- بروتوكولSimple Certificate Enrollment and Revocation : يقوم هذا البروتوكول بنقل طلبات تسجيل الشهادات الرقمية وطلبات الحصول على قائمة الشهادات الملغاة بين سلطة التصديق والمستخدم، يتم النقل عبر شبكة الإنترنت.
- قائمة الشهادات الرقمية الملغاة: قائمة شهادات المفتاح العام الملغية، يتم إصدار تلك القائمة والتوقيع عليها رقمياً بواسطة هيئة التصديق.
- التنظيم الإداري: ويشتمل على تحديد الأشخاص ووظائفهم داخل وحدة البنية التحتية للمفاتيح العامة مثل:
  - تحديد مدير لنظام البنية التحتية للمفاتيح العامة يقوم بتهيئة وصيانة النظام.
  - تحديد مسئول للشهادات الرقمية للتحقق من صحة طلبات الشهادات الرقمية وإصدار الشهادات الرقمية.
  - تحديد مدقق سجلات النظام يقوم بتدقيق الأخطاء والتحذيرات التي يقوم النظام بحفظها في سجلات التدقيق (Audit Logs).
- التنظيم القانوني: ويشتمل على السياسات والتشريعات التي تنظم تشغيل واستخدام النية التحتية للمفاتيح العامة.

تسجيل الشهادة الرقمية:

وهي العملية التي يتم بواسطتها حصول المستخدم على الشهادة الرقمية. يلزم المستخدم أن يتقدم بطلب الحصول على الشهادة الرقمية، هذا الطلب له شكل خاص. الطلب يجب أن يحتوي على المفتاح العام وهوية طالب الشهادة الرقمية، وبعد التأكد من هوية طالب الشهادة الرقمية يتم منحة الشهادة، حسب الخطوات الموضحة في الشكل (٣٢).



شكل (٣٢): *عملية تسجيل الشهادة الرقمية*

حيث يستخدم معيار PKCS # ١٠ لطلب الشهادة الرقمية، وتشمل المعلومات في طلب تسجيل الشهادة PKCS # ١٠ التالي:

- المفتاح العام لطالب الشهادة الرقمية ويجب أن يوقع من قبل سلطة توثيق الشهادات الرقمية.
- الاسم المميز لطالب الشهادة الرقمية.
- التوقيع الرقمي وهو عبارة عن القيمة المختزلة للطلب موقعة بواسطة المفتاح الخاص لطالب الشهادة الرقمية.
- خوارزمية الاختزال Hashing Algorithm المستخدمة في إنشاء التوقيع الرقمي الذي تم إنشاؤه.

فعندما تتلقى سلطة التوثيق CA طلب الشهادة الرقمية، تقوم سلطة التوثيق بعمل التالي:

- فك شفرة التوقيع الرقمي في طلب الشهادة باستخدام المفتاح العمومي في الطلب.
- حساب البصمة الرقمية Hash value للطلب باستخدام دالة الاختزال المستخدمة من قبل طالب الشهادة الرقمية.
- هوية الطالب أو المستخدم الذي قدم طلب الحصول على الشهادة الرقمية يتم التحقق منها من خلال حساب البصمة الرقمية للطلب ومقارنتها بالقيمة الناتجة عن فك شفرة التوقيع الرقمي في طلب الشهادة باستخدام المفتاح العمومي في الطلب.
- تقوم سلطة التوثيق بتوقيع المفتاح العام للمستخدم.
- ويتم إضافة توقيع سلطة التوقيع إلى شهادة X.٥٠٩ .
- تقدم الشهادة إلى المستخدم الذي طلب الحصول على الشهادة.

يقوم المستخدم بنشر نسخ من شهادة X.٥٠٩ إلى الكيانات التي يمكن أن تستخدمها لتشفير البيانات التي سيتم إرسالها إلى المستخدم. أيضاً يمكن استخدام شهادة X٥٠٩ للتحقق من صحة التوقيعات.

هذه الكيانات تستطيع التحقق من هوية المستخدم صاحب الشهادة X.٥٠٩ من خلال التحقق من توقيعه باستخدام المفتاح العام للمستخدم والموجود في شهادته الرقمية. يتم التحقق من صحة الشهادة الرقمية من خلال التحقق من التوقيع الرقمي للشهادة والذي يتم إضافته من قبل سلطة التوثيق.

عمليات إدارة مفاتيح التشفير:

لأن مفاتيح التشفير تشكل الركيزة الأساسية لنظم البنية التحتية للمفاتيح فمن المهم أن تدار بعناية. وتشمل إدارة مفاتيح التشفير تخزينها، واستخدامها، والتعامل مع إجراءاتها.

- تخزين المفاتيح:

يعتبر تخزين المفاتيح في نظام البنية التحتية أمر مهم جدا. من الممكن تخزين المفاتيح العامة عن طريق تضمينها داخل الشهادات الرقمية، في حين أن المفاتيح الخاصة تخزن على النظام المحلي للمستخدم. لكن من عيوب سبل التخزين المرتكزة على البرمجيات إمكانية تعرضها للهجمات: نقاط الضعف في نظام التشغيل العميل على سبيل المثال، يمكن أن يعرض المفاتيح للمهاجمين. تخزين المفاتيح في عتاد هو بديل للتخزين القائم على البرمجيات. يمكن استخدام أجهزة خوادم سلطة التصديق لتخزين المفاتيح العامة. ويمكن تخزين المفاتيح الخاصة على البطاقات الذكية أو جهاز الشفرة الأمنية .

- استخدام المفاتيح:

إذا كانت هناك حاجة لرفع المستوى الأمني حيث إن زوجاً واحدًا من مفتاح عام وخاص لم يكن كافيًا، يمكننا إنشاء زوجان من المفاتيح المزدوجة. بحيث يستخدم الأول في تشفير المعلومات وينسخ مفتاحها العمومي في مكان آخر كالشهادة الرقمية على سبيل المثال، أما الزوج الثاني فيستخدم للتوقيعات الرقمية فقط ولا يتم إجراء النسخ الاحتياطي للمفتاح العمومي في هذا الزوج. حيث إنه في حال سرق المهاجم مفتاح التشفير العمومي لا يزال غير قادرًا على إجراء توقيع رقمي للوثيقة.

- إجراءات التعامل مع المفاتيح:

يوجد إجراءات معينة تساعد على ضمان التعامل مع المفاتيح بالشكل السليم. وتشمل هذه الإجراءات ما يلي:

- التأمين: ويشير هذا المصطلح لإدارة المفاتيح من خلال طرف ثالث لحفظها، كسلطة التصديق على سبيل المثال. في تأمين المفتاح يُقسم المفتاح الخاص لنصفين ويشفر كلًا منهما على حدة. ومن ثم يتم إرسال القسمين للطرف الثالث والذي بدوره يقوم بتخزين كل قسم في مكان مختلف. بعد ذلك يمكن للمستخدم استرداد كل من القسمين ودمجهما بعد فك شفرتيهما ليتمكن من استخدام المفتاح مجددًا. هذا الإجراء المتبع لتأمين المفتاح يضمن للمستخدمين عدم ضياع المفاتيح الخاصة لهم. لكن العيب في هذا النظام أن المفتاح الخاص يكون عرضة للهجوم بعد فك شفيرة القسمين ودمجهما.
- انتهاء الصلاحية: لدى المفاتيح تواريخ انتهاء الصلاحية. وهذا يمنع المهاجم الذين قام بسرقة مفتاح خاص من أن يكون قادرًا على فك تشفير الرسائل لفترة غير محددة من الزمن. بعض النظم تضع للمفاتيح فترة زمنية افتراضية معينة لتنتهي صلاحية المفاتيح بعدها.
- التجديد: بدلًا من ترك المفاتيح حتى تنتهي صلاحيتها يمكننا إنشاء مفاتيح جديدة أو تجديد المفاتيح الحالية. في حالة تجديد المفاتيح الحالية تستخدم المفاتيح العمومية والخاصة الأصلية ولا يشترط تغييرها. لكن الاستمرار في تجديد صلاحية المفاتيح الأصلية يجعلها عرضة للسرقة وسوء الاستخدام مع مرور الوقت.

- الإبطال: بما أن جميع المفاتيح لها تاريخ صلاحية وينتهي خلال فترة زمنية معينة، قد نحتاج لإبطال المفتاح قبل مجيء تاريخ انتهاءه في بعض الحالات كما في حالة استقالة الموظف فنحن بحاجة لإبطال المفتاح الخاص الذي بحوزته. ولا يمكن إعادة المفاتيح التي أبطلت صلاحيتها أبدًا.
- الاستعادة: هناك تقنيات مختلفة يمكن استخدامها لاستعادة المفاتيح، فبعض سلطات التصديق لديها نظام مضمن لاسترداد المفاتيح الخاصة وهو نظام مسؤول عن استرداد المفاتيح أو الشهادات الرقمية التالفة.
- التعليق: الإبطال هو إيقاف دائم للمفتاح، لكننا قد نحتاج إيقاف المفتاح لفترة زمنية ومن ثم إعادة صلاحية المفتاح وهذا ما يسمى بالتعليق.
- التدمير: في هذه الحالة يدمر كلًا من المفاتيح العمومية والخاصة جنبًا إلى جنب مع بيانات هوية المستخدم لدى سلطات التصديق الرقيمة.

المركز الوطني للتصديق الرقمي في المملكة العربية السعودية:

تم إنشاء المركز الوطني للتصديق الرقمي وفقاً لقرار اللجنة الدائمة للتجارة الإلكترونية بتاريخ ١٤٢٢/١/١٠هـ والذي أناط مهمة إنشاء وتشغيل البنية التحتية للمفاتيح العامة لمدينة الملك عبدالعزيز للعلوم والتقنية، وتمت الموافقة السامية على ذلك بتاريخ ١٤٢٢/٥/١٧هـ، ويتمثل دور المركز الوطني للتصديق الرقمي في تقديم منظومة متكاملة لإدارة البنية التحتية للمفاتيح العامة والتي تقوم عليها كافة الأعمال الإلكترونية كالتجارة الإلكترونية والحكومة الإلكترونية. وتمكّن هذه المنظومة المتعاملين عن طريق شبكة الإنترنت بمختلف فئاتهم (حكومة، مواطنون، أعمال) من إجراء مختلف العمليات الإلكترونية بسرية وموثوقية وسلامة تامة. كما تتمثل مهام المركز الرئيسية فيما يلي: (المركز الوطني للتصديق الرقمي، ٢٠٢١).

- إصدار الشهادات الرقمية لمراكز التصديق الرقمي في المملكة.
- إدارة وتشغيل وصيانة الأجهزة والبرمجيات الخاصة بالبنية التحتية للمفاتيح العامة.
- إلغاء الشهادات الرقمية عند الحاجة ونشر قائمة الشهادات الملغاة على الإنترنت.
- تأهيل الجهات المتقدمة للحصول على تراخيص فتح مراكز تصديق للشهادات الرقمية.
- إعداد الأنظمة واللوائح الخاصة بالبنية التحتية للمفاتيح العامة والتنسيق في ذلك مع الجهات المعنية.
- التنسيق الفني والإداري فيما بين مراكز التصديق في المملكة.
- العمل على إعداد الأنظمة اللازمة لإتمام التعاملات الإلكترونية والتنسيق في ذلك مع الجهات المعنية.

العنصر الخامس: البروتوكولات المشفرة لنقل البيانات:

استخدام خوارزميات التشفير ليس حكراً على تشفير البيانات المخزنة أو البيانات قد الاستخدام، إنما يتم الاعتماد عليها في تشفير البينات أثناء النقل في الشبكة، ومن بروتوكولات النقل الشبكي المشفرة ما يلي: (Ciampa, ٢٠١٨).

بروتوكول Secure Sockets Layer (SSL)

يعد هذا البروتوكول من أقدم البروتوكولات التي اعتمدت على خوارزميات التشفير وأكثرها انتشاراً. كان الهدف من تصميم SSL هو إنشاء مسار بيانات مشفر بين العميل والخادم الذي يمكن استخدامه على أي نظام أساسي أو نظام تشغيل.

بروتوكول Secure Shell (SSH)

يعد هذا البروتوكول بديلاً مشفرًا لبروتوكول Telnet المستخدم للوصول إلى أجهزة الكمبيوتر عن بعد. حيث يحتوي SSH على واجهة أوامر وبروتوكول تستند إلى Linux / UNIX للوصول الآمن إلى كمبيوتر من خلال الشبكة. كما يمكن استخدام SSH كأداة للنسخ الاحتياطي الآمن للشبكة.

بروتوكول Hypertext Transport Protocol Secure(HTTPS)

يستخدم هذا البروتوكول لتأمين الاتصالات بين متصفح الويب وخادم الويب. هذا الإصدار الآمن هو في الواقع بروتوكول HTTP عادي يتم إرساله عبر SSL. يستخدم HTTPS المنفذ ٤٤٣ بدلاً من منفذ ٨٠ HTTP. يجب على المستخدمين إدخال عناوين URL باستخدام https: // بدلاً من http: //.

بروتوكول Secure/Multipurpose Internet Mail Extensions (S/MIME)

يستخدم هذا البروتوكول لتأمين رسائل البريد الإلكتروني. حيث يسمح للمستخدمين بإرسال رسائل مشفرة موقعة رقميًا أيضًا.

بروتوكول IP Security (IPsec)

يستخدم هذا البروتوكول لتأمين اتصالات بروتوكول الإنترنت (IP). حيث يقوم IPsec بتشفير كل حزمة بيانات IP مرسلة لجلسة اتصالات بين جهازين أو شبكتين والمصادقة عليها أيضاً.

ولإيضاح أكثر بين البروتوكولات المشفرة والبرتوكولات غير المشفرة، تنبه معظم متصفحات الويب المستخدمين إذا كانوا يتصفحون صفحات ويب غير آمنة عن طريق عرض تحذير "غير آمن". يشير هذا إلى أن صفحة الويب لا توفر اتصالاً آمنًا للزوار. حيث إنه عندما يتصل متصفحك بموقع ويب، يمكنه إما استخدام HTTPS الآمن أو بروتوكول HTTP غير الآمن. إذا بدأ عنوان URL للموقع بـ HTTP، فهذا يعني أن الاتصال غير آمن، مما يؤدي إلى تشغيل تحذير "غير آمن" كما في شكل (٣٣).

شكل (٣٣): *الاتصال بموقع من خلال بروتوكول http*

اليوم التدريبي الخامس

الموضوع العاشر: الهندسة الاجتماعية.

الموضوع الحادي عشر: الاستجابة للأحداث والتعافي من الكوارث.

الموضوع الثاني عشر: الاستراتيجية الوطنية للأمن السيبراني في المملكة العربية السعودية.

المخطط التدريبي لليوم الخامس

الجلسة الأولى

- (٨:٠٠:٩:٣٠)
- الهندسة الاجتماعية.

استراحة (٩:٣٠:١٠:٠٠)

الجلسة الثانية

- (١٠:٠٠:١١:٣٠)
- الإستجابة للأحداث والتعافي من الكوارث.

استراحة (١١:٣٠:١٢:٣٠)

الجلسة الثالثة

- (١٢:٣٠:٢:٠٠)
- الإستراتجية الوطنية للأمن السيبراني في المملكة.

الموضوع العاشر: الهندسة الاجتماعية.

تعرف الهندسة الاجتماعية على أنها فن التلاعب بالناس بهدف تنفيذ المهام المطلوبة. وتستغل الهندسة الاجتماعية غريزة الإنسان الطبيعية في الثقة. وكلما أصبحت التقنية أكثر آمنا، أصبحت الهندسة الاجتماعية أكثر أهمية لوصول المهاجمين إلى الأنظمة المرغوب فيها. (أغروال، كامبو، بيرس، ٢٠١٨)

الهندسة الاجتماعية هي العملية التي يتمكن المهاجمون من خلالها من التسلل والوصول إلى المنظمات والشبكات وحتى الأفراد من خلال استغلال طبيعة الأشخاص بالثقة في الآخرين. فقد يأتي هجوم الهندسة الاجتماعية من شخص يتظاهر بأنه مسوق تابع لشركة حقيقية لبيع وتطوير المنتجات، أو يمكن أن يأخذ شكل بريد إلكتروني ممن يدعي بأنه مدير تنفيذي في منظمة ما يحتاج للمساعدة العاجلة لأنه نسي بيانات تسجيل الدخول الخاصة به إلى النظام أثناء سفره خارج البلاد. غالبًا ما يكون من الصعب في هذه الهجمات من تحديد ما إذا كان الفرد له حق نظامي أو أن لديه نوايا سيئة. (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

الهجمات الاجتماعية تشمل محادثات أو حوار مع مستخدمين بهدف إقناعهم أن يفعلوا شيئاً لا يقومون عادة بفعله. وفي ظروف معينة حتى مستخدمو الحاسب الآلي الأذكياء قد يكونون عرضة لهجمات الهندسة الاجتماعية. (أغروال، كامبو، بيرس، ٢٠١٨)

وحتى نتمكن من توضيح مفهوم الهندسة الاجتماعية بشكل أفضل، سنسلط الضوء من خلال الأمثلة التالية على أكثر من سيناريو محتمل لهجمات الهندسة الاجتماعية الشائعة.

على صعيد الأفراد، من الوارد لأي فرد منا أن يتلقى اتصالاً هاتفياً أو رسالة نصية من شخص يدعي أنه تابع لجهة رسمية- كشركة أو بنك- لطلب معلوماتنا الشخصية إما بهدف الترغيب (مثل أن يخبرنا "تهانينا ، لقد فزت بسيارة في السحب على الجوائز المقدمة من الشركة (س)") أو بهدف الترهيب (مثل أن يطلب منا التجاوب معه بشكل عاجل لتحديث بياناتنا حتى لا يتم تجميد حسابنا البنكي)، ومن منطلق طبيعتنا البشرية غالباً ما تكون النتيجة هي التفاعل مع هذا الشخص وتزويده بالمعلومات الشخصية مثل رقم الهوية أو رقم الحساب البنكي، رغبة في الحصول على الجائزة أو خوفاً من تعطل مصالحنا إذا تم تجميد حساباتنا، وبذلك نكون قد وقعنا ضحية لأحد هجمات الهندسة الاجتماعية والتي لم تتطلب من المهاجم سوى التواصل معنا بشكل مباشر للحصول على المعلومات التي لا نعلم كيف سيتم استغلالها منه.

أما على الصعيد المؤسسي، فمن الممكن أن يكون الموقف التالي موقفاً تقليدياً، ولكنه قد يشكل أيضاً أحد هجمات الهندسة الاجتماعية، وذلك حينما يدخل شخص ما لمبنى أحد المنظمات أو المؤسسات مرتديًا الزي المعتاد لفني الصيانة حاملاً معه مجموعة من الأدوات، يصل إلى موظف الاستقبال ويعرّف نفسه بأنه مرسل من أحد شركات الاتصالات لإصلاح مشكلة ما في المبنى. في الواقع، غالباً ما سيسمح له موظف الاستقبال بالمرور – من منطلق الثقة النابع من هيئة هذا الشخص والحوار معه-بدون التأكد من الهوية المهنية له أو التواصل مع القسم المسؤول في المنظمة للتأكد من وجود مشكلة أصلاً في الاتصالات وأنه قد تم فعلاً طلب فريق الدعم الفني لحلها. بمجرد دخول هذا «الفني» المزعوم إلى المبنى تكون المنظمة ضحية لهجوم هندسة اجتماعية، وبذلك يكون المهاجم قد اخترق الطبقة الأولى من الأمان المتمثلة في موظف الاستقبال (أو موظف الأمن) والذي يعتبر من واجبه حماية المنظمة من الوصول المادي للأشخاص غير المصرح لهم. وبذلك يتمكن هذا الشخص من الوصول إلى المنظمة بأكملها وقد يكون قادراً على المرور بحرية في أي مكان يريد، مع الأخذ في الحسبان بأنه قد يستدرج موظف الاستقبال -بحجة إصلاح العطل

الفني-لمساعدته على معرفة مكان غرفة الأجهزة المزمع إصلاحها حتى يتمكن من الوصول لها مباشرة. لم يتطلب هذا الهجوم أي موهبة أو مهارة أو تقنية معينة بخلاف القدرة على أن تبدو كفني صيانة.

المواقف السابقة توضح أن التكنولوجيا ليست ضرورية دائمًا للهجمات على تقنية المعلومات. فالهندسة الاجتماعية تركز في جمع المعلومات للهجوم بالاعتماد على نقاط ضعف الأفراد. يمكن أن تتضمن هجمات الهندسة الاجتماعية مناهج نفسية بالإضافة إلى إجراءات جسدية.

العنصر الأول: الأساليب النفسية:

تعتمد العديد من هجمات الهندسة الاجتماعية النهج العقلي والعاطفي، فهي تعتمد على التلاعب الذكي للمهاجم بالطبيعة البشرية لإقناع الضحية بتقديم المعلومات أو اتخاذ الإجراءات. ويمكن حصر المبادئ النفسية الأساسية الهندسة الاجتماعية في سبعة مبادئ يستخدمها المهاجم لتوجيه الضحية للتجاوب مع طلباته، وهذه المبادئ موضحة في جدول ١٢، حيث تم توضيح هذه المبادئ مع آلية استخدامها المحتملة في أحد الهجمات الشائعة وهي من خلال التواصل مع أحد موظفي الدعم الفني لإعادة تعيين كلمة المرور لشخص غير المصرح له. (Ciampa, ٢٠١٨).

جدول (١٢): *المبادئ النفسية الأساسية الهندسة الاجتماعية.*

المبدأ	الوصف	مثال توضيحي
السلطة	انتحال المهاجم شخصية ذات سلطة أو منصب مرموق	" مرحبا، أنا الرئيس التنفيذي للشركة"
التخويف	محاولة المهاجم تهديد الضحية	«إذا لم تقم بإعادة تعيين كلمة المرور الخاصة بي، سأتصل بمديرك»
التوافق	تأثر الضحية بسلوك الآخرين	«اتصلت الأسبوع الماضي وقام زميلك بسهولة بإعادة تعيين كلمة المرور الخاصة بي»
الاحتياج	الادعاء بوجود الحاجة الملحة	«ليس لدي الوقت لأضيعه معك»
الاستعجال	الحاجة إلى اتخاذ إجراء فوري	«لدي اجتماع مع مجلس الإدارة بعد ٥ دقائق، وأحتاج كلمة المرور الآن لعرض بعض المستندات عليهم»
الألفة	توطيد الروابط الجيدة مع الضحية	«سوف أحرص على وضع تقييم جيد لك»
الثقة	اتخاذ المهاجم موقف القوة مع الضحية	«هل تعرف من أكون؟»

عصف ذهني (٢)

الهدف: أن يتعرف المتدرب على آليات الاصطياد الإلكتروني.	**الزمن:** ١٥ دقيقة

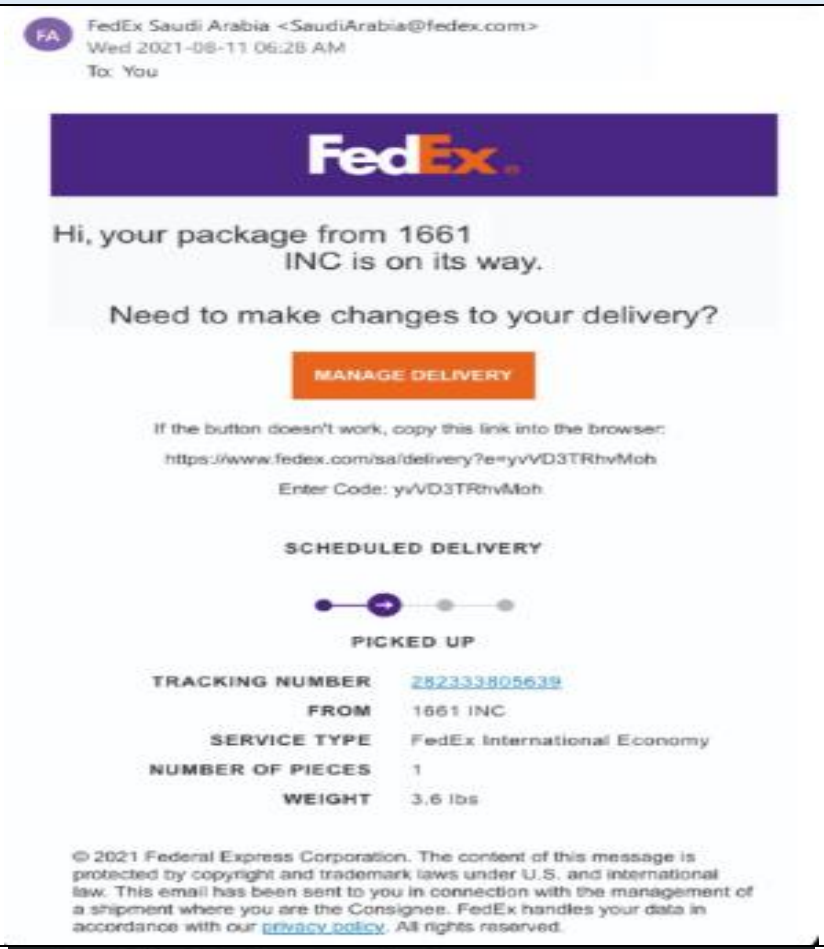
يعتمد التمرين على الاطلاع على نماذج لرسائل بريد إلكتروني تصل باستمرار إلى أغلب المستخدمين، وعلى المتدربين اكتشاف ما إذا كانت محاولة اصطياد إلكتروني أم لا (تم الاعتماد في هذا التمرين على اختبار #صيد_المتصيد المعد من قبل هيئة الاتصالات وتقنية المعلومات)

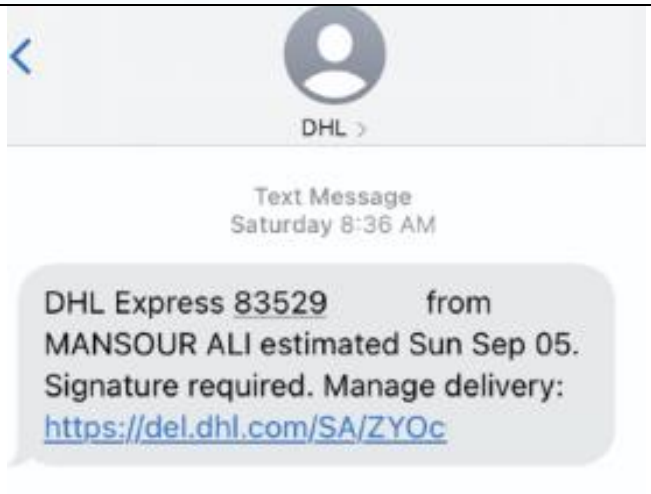
الإرشادات:

١. يقوم المتدربون بالاطلاع على الصور التالية وتحديد ما إذا كانت مفبركة أم لا.

٢. يقوم المدرب باستعراض النتائج مع المتدربين وتحليل وضع كل شاشة.

جدول (١٣): اختبار:(صيد_المتصيد).

#	الرسالة الإلكترونية	التحليل
١		
٢		

#	الرسالة الإلكترونية	التحليل
٣		
٤		
٥		

#	الرسالة الإلكترونية	التحليل
٦		
٧		
٨		

العنصر الثاني: أنواع هجمات الهندسة الاجتماعية:

من المهم التعرف أنواع هجمات الهندسة الاجتماعية لزيادة وعي المستخدمين حول كيفية حدوث هذا النوع من الهجمات وبالتالي تجنب الوقوع فريسة لها. حيث سيتم فيما يلي استعراض قائمة ببعض الهجمات الأكثر شيوعًا: (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- الاصطياد (Phising): هو شكل من أشكال الهندسة الاجتماعية حيث تطلب من الضحية الحصول على بعض المعلومات بهدف تحديث أو استكمال البيانات بطريقة تبدو كما لو كان الطلب رسمياً. قد تبدو رسالة البريد الإلكتروني أو الرسالة النصية القصيرة-المُفبركة والواردة للضحية-كما لو كانت من أحد البنوك وتحتوي على بعض المعلومات الأساسية، مثل اسم المستخدم، وغالبًا ما تشير إلى وجود مشكلة في حساب الشخص أو امتيازات الوصول. سيُطلب من المستخدم النقر فوق رابط لتصحيح المشكلة. وبعد النقر على الرابط -الذي ينتقل إلى موقع آخر غير موقع البنك الحقيقي -يُطلب منه إدخال اسم المستخدم وكلمة المرور ومعلومات الحساب وما إلى ذلك. يمكن للمهاجم بعد ذلك استخدام القيم التي تم إدخالها هناك للوصول إلى حساب الضحية. من الممكن في هذا النوع من الهجمات أرسال البريد الإلكتروني إلى مئات أو آلاف المستخدمين، أو أن يتم استهداف شخص محدد تم الحصول على جزء من بياناته بطريقة ما، كأن يتم استهداف إحدى الشخصيات المهمة والمعروفة لمحاولة اصطياد معلوماتها.
- الاصطياد الهاتفي (Vishing): وهو هجمات الاصطياد من خلال المكالمات الهاتفية باستخدام بروتوكول الإنترنت (VoIP – Voice over IP) ،حيث يمكن للمهاجم الاتصال بأي شخص من أي مكان في العالم تقريبًا دون القلق بشأن تتبعهم من خلال معرف الاتصال او الميزات الأخرى المتعلقة بالخطوط الأرضية. ثم ينتحلون أي صفة رسمية من أجل الحصول على بيانات الضحية.
- البحث في سلة المهملات (Dumpster Diving): عادة ما تولد الشركات كميات هائلة من الورق، ينتهي في معظمها المطاف في مكبات القمامة أو صناديق إعادة التدوير، وقد تحتوي هذا الأوراق على معلومات حساسة مثل بينات العملاء أو الموظفين أو نماذج تطوير المنتجات. في البيئات الأمنية العالية والحكومية، يتم تمزيق الأوراق الحساسة أو حرقها. ولكن ليس بالضرورة أن يحصل ذلك في معظم الشركات. بالإضافة إلى ذلك، أدى ظهور الشركات «الخضراء» -وهي الشركات الصديقة للبيئة-إلى زيادة في كمية الورق المعاد تدويره، والتي يمكن أن تحتوي في كثير من الأحيان على جميع أنواع المعلومات المهمة حول الشركة وموظفيها.
- التلصص (Shoulder Surfing): يعتبر التلصص أحد الأشكال الشائعة للهندسة الاجتماعية ولا يتضمن شيئًا أكثر من مشاهدة شخص ما "من خلف كتفه" عند إدخال بياناته الحساسة. يمكنهم رؤيتك تقوم بإدخال كلمة مرور أو كتابة رقم بطاقة ائتمان أو إدخال أي معلومات أخرى ذات أهمية. أفضل دفاع ضد هذا النوع من الهجوم هو التأكد من المنطقة المحيطة بك قبل إدخال البيانات الشخصية. هذا النوع من الهجوم قد يحدث في بيئات العمل أو في أي مكان عام مثل ردهات الفنادق، وأجهزة الصراف الآلي، وما إلى ذلك.

العنصر الثالث: الحماية من هجمات الهندسة الاجتماعية:

وسيلة الحماية الوحيدة للوقاية من هجمات الهندسة الاجتماعية هو التثقيف ورفع مستوى الوعي لدى المستخدمين والموظفين بعدم إعطاء كلمات مرور أو أي بيانات شخصية عبر الهاتف أو عبر البريد الإلكتروني أو لأي شخص لم يتم التحقق منه بشكل قاطع أنه من جهة رسمية. (Emmett Dulaney and Chuck Easttom, ٢٠١٨).

عصف ذهني (٣)

الهدف: أن يميز المتدرب روابط الاصطياد الإلكتروني. | **الزمن:** ٢٠ دقيقة

يعتمد التمرين على إجراء اختبار فحص الاصطياد من أحد المواقع المعدة لذلك لتسليط الضوء على النقاط التي يمكن من خلالها التمييز بين الروابط الإلكترونية الحقيقة وروابط الاصطياد الإلكتروني.

الإرشادات:

١. يُقسم المتدربين إلى مجموعات، بحيث تتكون كل مجموعة من أربعة متدربين.
٢. تقوم كل مجموعة بالدخول على الرابط التالي https://www.opendns.com/phishing-quiz/
٣. يبدأ المتدربون بإجراء اختبار فحص الاصطياد Phising Quiz وذلك بالضغط على زر Get Started!
٤. يبدأ الموقع بعرض صور شاشات، يقوم المتدربون بفحص كل شاشة وتحديد إن كانت حقيقة Real أو مفبركة Fake
٥. يقوم المدرب في نهاية الاختبار باستعراض النتائج مع المتدربين ومناقشة طرق اكتشاف روابط الاصطياد الإلكتروني في كل شاشة مفبركة.

الموضوع الحادي عشر: الاستجابة للأحداث والتعافي من الكوارث.

تُعرف حوادث أمن المعلومات على أنها أي انتهاك أو تهديد وشيك بحدوث انتهاك لسياسات أمن المعلومات وأمن الحاسب الآلي، أو سياسات الاستخدام المقبول، أو ممارسات الأمان الموحدة. ومن أمثلة الحوادث الأمنية المحتملة كأن يتم إرسال تقرير مزيف إلى بعض المستخدمين للمنظمة على أنه تقرير بخصوص سير العمل وهو في الواقع برنامج خبيث يؤدي إلى الحاق الضرر بالأجهزة، أو أن يتمكن مهاجم من الحصول على بيانات حساسة خاصة بالمنظمة ويقوم بمساومة إدارة المنظمة على الحصول على مبلغ مالي معين مقبل عدم نشر هذه المعلومات للعامة. لذلك، يجب على المنظمات أن تقوم بشكل دوري بحصر وتحليل الحوادث الأمنية المحتمل وقوعها ووضع خطة وسياسة للاستجابة لها حال حدوثها، حيث تصف هذه الخطط والسياسات الطرق الموحدة المستخدمة من قبل المنظمة في التعامل مع الحوادث الأمنية للمعلومات، إضافة إلى أن هذه الخطط تساعد على التركيز على الحوادث عند وقوعها دون التشتت بين الإجراءات الإدارية أو الحصول على موافقات الإدارات ذات العلاقة في وقت حرج. (أغروال، كامبو، بيرس، ٢٠١٨)

العنصر الأول: فريق الاستجابة للحوادث الأمنية:

تحرص المنظمات على تعيين فريق محدد للاستجابة للحوادث الأمنية الذي يظهر دوره جلياً قبل وأثناء وبعد وقوع الحوادث، بحيث يعمل أعضاء الفريق بشكل مستمر على متابعة البنية التحتية التقنية والمعلوماتية وتحليل الحوادث المحتملة بالإضافة إلى تطوير خبراتهم في هذا المجال. يعتبر الهدف الرئيسي لفريق الاستجابة للحوادث الأمنية هو الحماية العامة للبنية التحتية التقنية والمعلوماتية للمنظمة، لذلك من الضروري أن يكون أعضاء الفريق بدراية تامة بهيكلة تقنية المعلومات في المنظمة. وتكون المهام الرئيسية للفريق على النحو التالي: (أغروال، كامبو، بيرس، ٢٠١٨)

- التحديد السريع للتهديدات الأمنية المهددة للبنية التحتية التقنية والمعلوماتية.
- تقييم مستوى المخاطر.
- اتخاذ خطوات فورية للتقليل من المخاطر المحتملة.
- التواصل مع الإدارة أو الجهات ذات العلاقة بالحادثة ومخاطرها.
- إبلاغ منسوبي المنظمة بأي مخاطر ذات علاقة بالموارد والأصول التقنية التي يعملون عليها.
- إصدار التقارير المطلوبة حسب الحاجة، متضمناً ذلك الدروس المستفادة.

ومن الأدوات الأساسية التي تساعد فريق الاستجابة للحوادث الأمنية على وضع تصور لوضع المنظمة الأمني، وبالتالي وضح خطط الاستجابة على ضوئها، هي أدوات فحص الاختراق Penetration Testing وماسح الثغرات Vulnerability Scanning. وفيما يلي توضيح لدور كل منهما. (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- اختبار الاختراق Penetration Testing:

أصبح من الشائع أن تقوم المنظمات بإجراء اختبارات الاختراق بشكل دوري لقياس قوة دفاعات أنظمتهم. بشكل عام، سيستخدم مختبري الاختراق نفس الأساليب التي قد يستخدمها المخترقون للعثور على أي ثغرات في أمان النظام. يمكن اكتشاف هذه الثغرات بوسائل أخرى غير الوصول المباشر إلى النظام أو ما يُعرف بالاستطلاع السلبي، مثل جمع المعلومات من قواعد البيانات العامة، والتحدث إلى الموظفين والمستخدمين، والهندسة الاجتماعية. على النقيض من ذلك، ممكن تطبيق الاختبار باستخدام آلية الاستطلاع النشط والتي تعمل بشكل مباشر على النظام عمليات مسح المنافذ وتتبع مسارات البيانات ورسم خرائط الشبكة وما إلى ذلك، لتحديد نقاط الضعف التي يمكن استغلالها لشن هجوم. عند إجراء اختبار الاختراق، من المهم أن يكون هناك وثيقة تحدد نطاق ومدى الاختبار الذي يتعين القيام به، بالإضافة إلى ضرورة الحصول على موافقة كتابية من المسؤول الذي يملك صلاحية التصريح بإجراء مثل هذا الاختبار.

- ماسح الثغرات Vulnerability Scanning:

يتيح فحص الثغرات الأمنية تحديد نقاط ضعف معينة في الشبكة، وسيبدأ معظم مختبري الاختراق بهذا الإجراء حتى يتمكنوا من تحديد الأهداف المحتملة للهجوم، حيث أن اختبار الاختراق هو في الأساس محاولة لاستغلال هذه الثغرات الأمنية. العنصر الأساسي لفحص الثغرات الأمنية هو دائمًا تحديد الثغرات، كتحديد الإعدادات الخاطئة الشائعة أو تحديد نقص الضوابط الأمنية. في الواقع، تساعد أدوات فحص الثغرات الأمنية الشائعة، مثل Nessusفي تحديد إعدادات الشبكات الخاطئة الأكثر شيوعاً.

العنصر الثاني: خطط الاستجابة للحوادث:

خطة الاستجابة للحوادث incident response plan (IRP) هي مجموعة من التعليمات المكتوبة للاستجابة في حال وقوع حادث أمني. بدون هذه الخطط، ستتعرض المنظمات لخطر عدم القدرة على تحديد الهجوم بسرعة واحتواءه وبالتالي انتشاره وصعوبة التعافي منه أو عدم الاستفادة والتعلم من الهجوم الذي حصل لتحسين الدفاعات. تشكل الخطوات التي يجب اتخاذها عند وقوع حادث، والتي تسمى عملية الاستجابة للحادث، على الخطوات الستة التالية: (Ciampa, ٢٠١٨)

- الإعداد Preparation:

التجهيز المسبق لموظفي تكنولوجيا المعلومات والإدارة والمستخدمين للتعامل مع الحوادث المحتملة حال وقوعها.

- الاحتواء Containment:

الحد من الضرر الناجم عن الحادث وعزل الأنظمة التي قد تتأثر لمنع زيادة الضرر.

- الاستئصال Eradication:

البحث عن سبب الحادث إجراء الإزالة المؤقتة لأي أنظمة قد تتسبب في حدوث ضرر.

- الاستعادة Recovery:

بعد التأكد من زوال التهديد، السماح للأنظمة المتأثرة بالعودة إلى التشغيل الطبيعي.

- الدروس المستفادة Lessons learned:

استكمال توثيق الحادث وإجراء تحليل مفصل لزيادة مستوى الأمن وتحسين جهود الاستجابة المستقبلية

ولتنفيذ خطط مجدية للاستجابة للحوادث، يجب أن تحتوي IRP على المعلومات التالية: (Ciampa, ٢٠١٨)

- تعريفات موثقة للحوادث. يجب أن تقدم IRP أوصافًا واضحة لأنواع وفئات وتعريفات الحوادث، والتي تحدد بالتفصيل ما هو -وما هو ليس -حادثًا يتطلب استجابة.
- فرق الاستجابة للحوادث السيبرانية. يتولى فريق الاستجابة للحوادث السيبرانية مسؤولية الاستجابة للحوادث الأمنية. بالإضافة إلى المتخصصين الفنيين الذين يمكنهم معالجة تهديدات محددة، يجب أن يشمل أيضًا أعضاء من موظفي العلاقات العامة والمديرين الذين يمكنهم توجيه أصحاب القرار في المنظمة بشأن الاتصال المناسب. يجب أن يكون لكل عضو واجبات محددة إضافة إلى تحديد الأدوار والمسؤوليات في فريق الاستجابة للحوادث السيبرانية.
- متطلبات الإبلاغ/ التصعيد. تشير متطلبات الإبلاغ / التصعيد إلى من يجب توزيع المعلومات وفي أي مرحلة يجب تصعيد الحدث الأمني إلى الدرجة التي ينبغي فيها تنفيذ إجراءات محددة.
- فحوصات. من المهم اختبار IRP عن طريق إجراء تمارين محاكاة لإجراء التعديلات اللازمة. يمكن إجراؤها من خلال التمارين التي تحاكي حالة الطوارئ ولكن في بيئة غير رسمية وخالية من الإجهاد.

عصف ذهني (٤)

الهدف: أن يطبق المتدرب خطط الاستجابة للحوادث. | **الزمن:** ١٥ دقيقة

في عام ٢٠١٧ تعرض أحد البنوك في شرق آسيا عملية احتيال أدت إلى خسائر فادحة، حيث قام مجموعة من المهاجمين من اختراق نظام SWIFT –وهو نظام عالمي لربط أسواق المال وتنفيذ الحوالات الدولية-وتمكنوا من تحويل الأموال من البنك بشكل احتيالي إلى حسابات مختلفة في المملكة المتحدة واليابان وسنغافورة والولايات المتحدة الأمريكية.

اكتشف البنك حدوث هذه المعاملات غير القانونية في وقت متأخر، لذلك لم تتمكن الا من إيقاف تحويل جزء يسير من الأموال. ولأن هذه كانت مشكلة أمنية معقدة تتعلق بدول أخرى، كان على البنك إبلاغ السلطات القانونية والبنك المركزي، حيث أثبتت التحقيقات الذي أجرته الجهات المختصة أن الحادث كان نتيجة من ضعف أمني من داخل البنك نتج عنه كشف عن أنظمة حرجة.

وفقًا لنتائج التحقيق، اتضح أن هناك ستة موظفين في البنك قاموا باستخدام الكمبيوتر الخاص نظام SWIFT لمهام أخرى غير ذات صلة. قد يكون هذا الإجراء قد كشف نظامSWIFT ، مما سمح للمهاجمين باختراقه. نتيجة للحادث، قرر البنك نقل الموظفين الستة إلى إدارات أخرى أقل حساسية.

- ما رأيك بهذه الواقعة؟
- ما رأيك في الإجراءات التي اتخذها البنك بعد حدوث الواقعة؟
- من وجهة نظرك، ماهي الدروس المستفادة؟

الإرشادات:

١. يُقسم المتدربين إلى مجموعات، بحيث تتكون كل مجموعة من أربعة متدربين.
٢. دراسة الحالة من قبل المجموعة ومحاولة الإجابة على الأسئلة السابقة.
٣. يعمل المتدرب على مناقشة وجهات النظر مع المتدربين.

العنصر الثالث: استمرارية الأعمال:

يتم تعريف استمرارية الأعمال على أنها قدرة المنظمة على الحفاظ على عملياتها وخدماتها في حال التعرض لحادثة أو عطل، سواء كان الحدث تقليدياً مثل انقطاع التيار الكهربائي أو كارثيًا مثل الإعصار. حيث يشمل ذلك وضع خطة لاستمرارية الأعمال، وتحليل تأثير الأعمال، وخطط التعافي من الكوارث.

التخطيط لاستمرارية الاعمال(BCP) Business Continuity Planning :

تخطيط استمرارية الأعمال (BCP) هو تطوير الخطط الاستراتيجية التي توفر طرق تشغيل بديلة لأنشطة وأعمال المنظمة التي يمكن أن تؤدي إلى خسارة كبيرة في حال توقفها لأي سبب، كأن يكون بسبب حادث طبيعي كزلزال أو فيضان أو بسبب حادث مصطنع مثل الهجمات الإلكترونية. لذلك، فهي عملية تحديد مدى احتمالية التعرض للتهديد، وتحديد الطرق الوقائية وإجراءات التعافي، ثم اختبارها لتحديد ما إذا كانت كافية ام لا. بشكل عام، تتكون خطط استمرارية الأعمال من ثلاثة عناصر أساسية: (Ciampa, ٢٠١٨)

- خطط استعادة الأعمال والتي تتضمن آليات وإجراءات استئناف وظائف وعمليات العمل الهامة التي تتعلق بتقديم الخدمات الأساسية للمنظمة وتدعمها.
- إدارة الأزمات والاتصالات والتي من خلالها إعطاء استجابة سريعة وفعالة لحدث ما عن طريق التواصل الفعال مع أصحاب القرار.
- خطط التعافي من الكوارث والتي تتناول آليات استرداد أصول تكنولوجيا المعلومات الهامة، بما في ذلك الأنظمة والتطبيقات وقواعد البيانات والتخزين وأصول الشبكة.

تحليل تأثر الأعمال(BIA) Business Impact Analysis :

يعد تحليل تأثر الأعمال (BIA) أحد الأدوات المهمة في خطط استمرارية الأعمال، حيث يتم من خلالها تحديد وظائف الأعمال وتحديد مدى التأثير الذي قد تحدثه خسارة هذه الوظائف على عمليات المنظمة الأساسية. وتتراوح درجة التأثر من التأثير على الممتلكات والأصول، والتأثير على التمويل والاستثمار أو التأثير على السمعة. لذلك، يتم تصميم BIA لتحديد العمليات ذات الأهمية للمنظمة حسب أولوياتها.

خطط التعافي من الكوارث:

تساعد خطط التعافي من الكوارث المنظمة على الاستجابة بفعالية عند وقوع كارثة. حيث قد تشمل الكوارث فشل أحد الأنظمة أو فشل الشبكة أو فشل البنية التحتية أو الكوارث الطبيعية. التركيز الأساسي لمثل هذه الخطة هو إعادة تفعيل الخدمات بأسر وقت ممكن وتقليل الخسائر إلى أدنى مستوى. أحد العناصر الرئيسية لخطط التعافي من الكوارث هو التركيز على الوصول إلى المعلومات وتخزينها. لذلك تعد عمليات النسخ الاحتياطي للبيانات جزءًا لا يتجزأ من هذه الخطط. لذلك لا بد من مناقشة خطط النسخ الاحتياطي وآليات استعادة الأنظمة واستخدام مواقع بديلة عند الحاجة. هذه هي العناصر الرئيسية لخطة التعافي من الكوارث، فهي تشكل جوهر كيفية استجابة المنظمة عند حدوث فشل خطير أو كارثة. (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- خطط عمليات النسخ الاحتياطي:

يتم التركيز عند تحديد خطة عمليات وإجراءات النسخ الاحتياطي على قيمة البيانات والمعلومات. حيث يجب أن تحدد خطة النسخ الاحتياطي ماهي المعلومات التي سيتم تخزينها، وكيف سيتم تخزينها، والمدة التي سيتم تخزينها فيها بالإضافة إلى آلية جدولة عمليات النسخ الاحتياطي التي من المفترض أن تتم بشكل دوري. إضافة إلى ذلك يجب أن تحدد خطة النسخ الاحتياطي أنواع الأنظمة والتطبيقات التي ستدعمها، ويمكن إيضاح ذلك حسب ما يلي: (Emmett Dulaney and Chuck Easttom, ٢٠١٨)

- أنظمة قواعد البيانات: توفر معظم أنظمة قواعد البيانات الحديثة القدرة على نسخ البيانات احتياطيًا أو أقسامًا معينة من قاعدة البيانات دون صعوبة تذكر. كما توفر إمكانات وخدمات تدقيق السجلات واستعادة البيانات. تحتوي معظم أنظمة قواعد البيانات على ملفات كبيرة تحتوي على عدد قليل نسبيًا من السجلات المحدثة بالنسبة إلى عدد السجلات المخزنة. لذلك يتم إدارة ذلك من ضبط عمليات النسخ الاحتياطي للسجلات المحدثة فقط.
- ملفات المستخدمين: تعد المستندات التي يعمل عليها الموظفون ذات قيمة كبيرة للمنظمة. ولكن، على الرغم من أن عدد الملفات التي يحتفظ بها الأشخاص عادة ما يكون كبيرًا، فإن عدد الملفات التي تتغير بعد إنشائها صغير نسبيًا. لذلك، من خلال إجراء نسخ احتياطي منتظم على أنظمة المستخدم، يمكنك حماية هذه المستندات والتأكد من إمكانية استردادها في حالة فقدانها إذا تم إنشاء نسخ احتياطية تخزن الملفات التي تم تعديلها فقط، مما يجعل عملية النسخ الاحتياطي تتطلب وقت وجهد أقل.
- التطبيقات: عادةً لا تتغير التطبيقات مثل معالجات النصوص والأنظمة الخاصة بالمنظمة والبرامج الأخرى بشكل دوري، كما أنه عندما يتم إجراء تغيير أو ترقية لتطبيق ما، فعادة ما يتم ذلك عبر المنظمة بأكملها. لذلك لن يكون هناك حاجة إلى الاحتفاظ بنسخة من التطبيق لكل مستخدم، ولكن يجب عليك الاحتفاظ بإصدار واحد محدث متاح للتنزيل وإعادة التثبيت.

الموضوع الثاني عشر: الاستراتيجية الوطنية للأمن السيبراني في المملكة العربية السعودية

انطلاقًا من إدراك المملكة العربية السعودية لمتغيرات ومستجدات العصر التقنية والثورة المعلوماتية، وترجمةً لنهج خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وسمو ولي العهد حفظهم الله في قيادة بلادنا لتكون نموذجًا ناجحًا ورائدًا في العالم على كافة الأصعدة، ولرؤية المملكة ٢٠٣٠ التي جعلت التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية ضمن مستهدفاتها، واستشعاراً لأهمية البيانات والأنظمة التقنية والبنى التحتية الحساسة وارتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني يأتي تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك -حفظه الله- وذلك وفق الأمر الملكي الكريم بالموافقة على تنظيمها بتاريخ ١١/٢/١٤٣٩ هـ لتكون الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية. ولا يخلي ذلك أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهمات الهيئة الواردة في تنظيمها. (الهيئة الوطنية للأمن السيبراني، ٢٠٢١)

العنصر الأول: دور الهيئة الوطنية للأمن السيبراني :National Cybersecurity Authority:

ولقد عرف تنظيم الهيئة الأمن السيبراني على أنه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها". (الهيئة الوطنية للأمن السيبراني، ٢٠٢١).

وتتمثل اختصاصات ومهام الهيئة فيما يلي:

١. إعداد الاستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها، واقتراح تحديثها.
٢. وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها.
٣. تصنيف وتحديد البنى التحتية الحساسة والجهات المرتبطة بها، وتحديد القطاعات والجهات ذات الأولوية بالأمن السيبراني.
٤. وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.
٥. إشعار الجهات المعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني.
٦. وضع أطر الاستجابة للحوادث المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.
٧. بناء مراكز العمليات الوطنية الخاصة بالأمن السيبراني – وما في حكمها – بكافة أنواعها، بما في ذلك مراكز التحكم والسيطرة والاستطلاع والرصد وتبادل وتحليل المعلومات، وكذلك بناء مراكز العمليات القطاعية الخاصة بالأمن السيبراني – عند الحاجة -، وبناء المنصات ذات العلاقة، والإشراف عليها، وتشغيلها.
٨. القيام – بنفسها أو من خلال غيرها – بالأنشطة والعمليات المتعلقة بالأمن السيبراني.

٩. تنظيم آلية مشاركة المعلومات والبيانات المرتبطة بالأمن السيبراني بين الجهات والقطاعات المختلفة في المملكة، والإشراف على ذلك.

١٠. تقديم المساندة للجهات المختصة – في حال طلبها وفقاً للإمكانيات المتاحة لدى الهيئة-خلال الاستدلال والتحقيق في الجرائم المتعلقة بالأمن السيبراني.

١١. وضع السياسات والمعايير الوطنية للتشفير، ومتابعة الالتزام بها، وتحديثها.

١٢. وضع ما يلزم من معايير أو ضوابط للفسح والترخيص باستيراد وتصدير واستخدام الأجهزة والبرمجيات ذات الحساسية العالية للأمن السيبراني التي تحددها الهيئة، ومتابعة الالتزام بها، وتحديثها، وذلك دون إخلال بأي معايير أو ضوابط معتمدة لدى الجهات الأخرى ذات العلاقة.

١٣. بناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها، وإعداد المعايير المهنية والأطر وبناء وتنفيذ المقاييس والاختبارات القياسية المهنية ذات العلاقة.

١٤. الترخيص بمزاولة الأفراد والجهات غير الحكومية للأنشطة والعمليات المتعلقة بالأمن السيبراني التي تحددها الهيئة.

١٥. التواصل مع الجهات المماثلة خارج المملكة والجهات الخاصة لتبادل الخبرات، وتأسيس آليات للتعاون والشراكة معها، وفقاً للإجراءات المتبعة.

١٦. تبادل الإنتاج التقني والمعرفي وتبادل البيانات والمعلومات مع الجهات المماثلة خارج المملكة.

١٧. تمثيل المملكة في المنظمات والهيئات واللجان والمجموعات الثنائية والإقليمية والدولية ذات الصلة، ومتابعة تنفيذ التزامات المملكة الدولية الخاصة بالأمن السيبراني.

١٨. رفع مستوى الوعي بالأمن السيبراني.

١٩. تحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه.

٢٠. إجراء الدراسات والبحوث والتطوير وعمليات التصنيع، ونقل التقنية وتطويرها في الأمن السيبراني وما يرتبط به من مجالات.

٢١. اقتراح آليات رفع كفاءة الإنفاق في مجالات الأمن السيبراني.

٢٢. تطوير مؤشرات قياس الأداء الخاصة بالأمن السيبراني، وإعداد التقارير الدورية حول حالة الأمن السيبراني في المملكة على المستويين الوطني والقطاعي.

٢٣. اقتراح إصدار وتعديل الأنظمة واللوائح والقرارات ذات الصلة بالأمن السيبراني.

وحيث إن تعزيز الأمن السيبراني للمملكة يتطلب تعاون كافة الجهات للعمل في منظومة وطنية متكاملة قادرة على مواجهة المخاطر السيبرانية وتقليل أثرها. ولذلك فإن الهيئة الوطنية للأمن السيبراني تعتبر كل جهة، عامة كانت أو خاصة، شريكا أساسياً لتحقيق الأهداف التي أنشئت من أجلها الهيئة. وقد أكد تنظيم الهيئة على أنها الجهة المختصة في المملكة بالأمن السيبراني، وأن ذلك لا يخلي أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهمات الهيئة الواردة في تنظيمها.

كما أكد الأمر السامي الكريم بتاريخ ١٠/١١/١٤٣٩ هـ "بأن على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات بهذا الشأن". (الهيئة الوطنية للأمن السيبراني، ٢٠٢١).

وبحسب تنظيم الهيئة تلتزم كافة الجهات ذات العلاقة بما يأتي:

١. تمكين الهيئة من مباشرة اختصاصاتها، وتنفيذ مهماتها بشكل كامل.
٢. إبلاغ الهيئة – بشكل فوري – بأي خطر أو تهديد أو اختراق لأمنها السيبراني واقع أو محتمل.
٣. تنفيذ السياسات وآليات الحوكمة والأطر، وتطبيق المعايير والضوابط التي تقرها الهيئة.
٤. التعاون التام مع الهيئة عند قيامها بأي أعمال تحرٍ أو تدقيق أو تقييم للأمن للسيبراني.
٥. تزويد الهيئة بالوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاتها ومهماتها، وتمكينها من فحص الأجهزة والشبكات والنظم والبرمجيات الخاصة بتلك الجهات.

المراكز التابعة للهيئة الوطنية للأمن السيبراني:

تم انشاء مجموعة من المراكز التابعة للهيئة الوطنية للأمن السيبراني والتي تمثل كيانات مختلفة وباختصاصات محددة تصب جميعها في تحقيق الاستراتيجية الوطنية للأمن السيبراني إضافة إلى رفع مستوى الأمن في الفضاء السيبراني والبُنى التحتية في المملكة، حيث تتمثل هذه المراكز فيما يلي: (الهيئة الوطنية للأمن السيبراني، ٢٠٢١)

- مركز الأمن الالكتروني:

يعمل مركز الأمن الإلكتروني بشكل مستمر في رصد المخاطر والتهديدات الإلكترونية وتحليلها ومشاركة المعلومات مع الجهات الحكومية والحيوية والحساسة للحماية من تلك التهديدات والتعامل معها حال وقوعها لاحتوائها ومنع تفاقم أضرارها؛ حيث يتولى المركز عمليات مراقبة التهديدات على مدار الساعة لتحديد أي إشارات لاختراق أنظمة الجهات الحكومية والحساسة. كما يقوم بتوعية الجهات بالحالة الأمنية الراهنة لتلك التهديدات بشكل تفصيلي ومبكر بما يساعد في التنسيق والحماية ضد الحوادث الإلكترونية واتخاذ قرارات مبنية على معلومات كافية تساعد على حماية الأنظمة الحساسة.

- المركز الوطني الإرشادي للأمن السيبراني Saudi CERT

يعمل المركز الوطني الإرشادي للأمن السيبراني على تعزيز جهود المملكة في رفع مستوى الوعي بالأمن السيبراني وذلك من خلال رفع الوعي والمعرفة بالأمن السيبراني لتجنب المخاطر السيبرانية وتقليل آثارها عن طريق إصدار التنبيهات بآخر وأخطر الثغرات، وإطلاق حملات وبرامج توعوية والتعاون مع المراكز الإرشادية الأخرى. لذلك ينصح بمتابعة التحذيرات الأمنية التي يتم اطلاقها من المركز الوطني الإرشادي للأمن السيبراني على الموقع https://cert.gov.sa/ كونها الجهة التوعوية الرسمية في هذا المجال.

- الأكاديمية الوطنية للأمن السيبراني National Cybersecurity Academy:

تعمل الأكاديمية للهيئة الوطنية للأمن السيبراني على بناء وتأهيل الكوادر الوطنية المتخصصة في مجالات الأمن السيبراني لسد الفجوة الموجودة في هذا المجال والمساهمة في حماية الفضاء السيبراني للمملكة وأمنها الوطني.

العنصر الثاني: الاستراتيجية الوطنية للأمن السيبراني:

إن وجود بنية تحتية رقمية وطنية متكاملة وآمنة يعد أحد أهم العوامل الممكنة للنمو والازدهار؛ إلا أن التوسع في استخدام التقنية يفتح آفاقاً جديدة للثغرات الأمنية والتهديدات السيبرانية؛ مما يستوجب تعزيز الأمن السيبراني لحماية الشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وحماية ما تقدمه من خدمات، وما تحويه من بيانات من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال، وكذلك لتعزيز الربط التقني الآمن بين الخدمات الحكومية، ودعم الاقتصاد الرقمي.

ولقد قامت الهيئة الوطنية للأمن السيبراني بإعداد الاستراتيجية الوطنية الأولى للأمن السيبراني تنفيذاً لاختصاصاتها المحددة في تنظيمها الصادر بالأمر الملكي رقم ٦٨٠١ وتاريخ ١١/ ٢/ ١٤٣٩هـ، الذي قضى في مادته الرابعة باختصاص الهيئة بإعداد استراتيجية وطنية للأمن السيبراني. اشتملت منهجية إعداد الاستراتيجية على الخطوات الأساسية التالية: (السيبراني، ٢٠٢٠)

- الرجوع إلى الوثائق الوطنية، وفي مقدمتها رؤية المملكة ٢٠٣٠، والأنظمة الوطنية ذات العلاقة ومنها تنظيم الهيئة الوطنية للأمن السيبراني.
- دراسة أبرز المخاطر السيبرانية العالمية والمحلية.
- تصميم إطار مرجعي خاص بالاستراتيجية مستنداً على أفضل الممارسات العالمية الناجحة والمستجدات الحديثة في الأمن السيبراني لبناء هذه الاستراتيجية، يغطي جميع جوانب الأمن السيبراني من التنظيمات والسياسات، وعمليات الدفاع السيبراني وبناء القدرات. ويشتمل هذا الإطار على ستة محاور وهي: التكامل والتنظيم والتوكيد والدفاع والتعاون والبناء.
- تجارب الدول المتقدمة في هذا المجال وأفضل الممارسات حيث تمت دراسة تجارب ٢٠ دولة.
- تحليل الوضع الراهن في المملكة.
- صياغة الاستراتيجية وتحديد العناصر المختلفة لها.

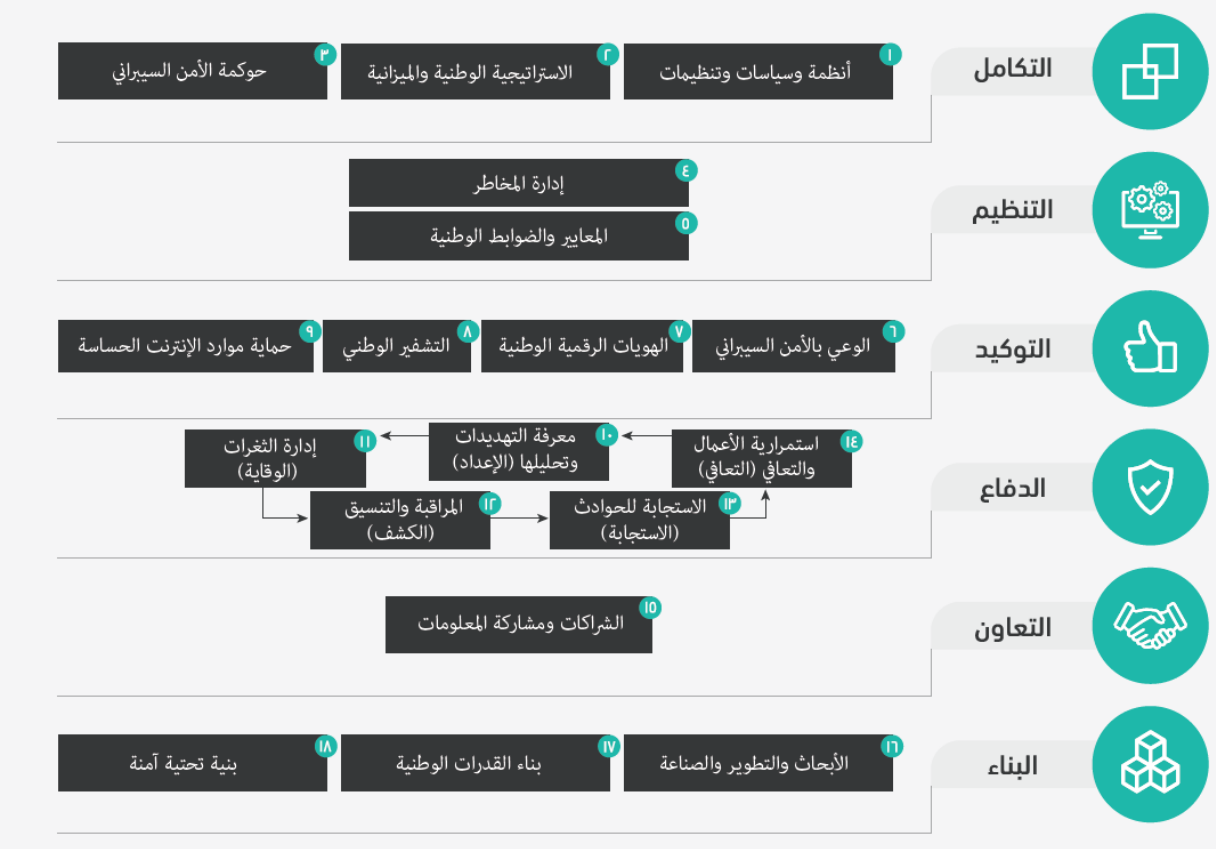
ويوضّح الشكل (٣٤) مدى ارتباط محاور رؤية المملكة ٢٠٣٠ بالاستراتيجية الوطنية للأمن السيبراني.

شكل (٣٤): *رؤية المملكة ٢٠٣٠ والاستراتيجية الوطنية للأمن السيبراني*

الإطار المرجعي لتطوير الاستراتيجية الوطنية للأمن السيبراني:

من أجل وضع مرجع عملي للجوانب المختلفة في الأمن السيبراني على المستوى الوطني، حرصت الهيئة الوطنية للأمن السيبراني على تصميم إطار مرجعي للأمن السيبراني خاص بالمملكة مبني على أفضل الممارسات المحلية والعالمية وأهم المستجدات والتحديات التي تواجه الأمن السيبراني، بحيث يعد نموذجًا متقدمًا يشمل الجوانب المختلفة للأمن السيبراني على مستوى الدول. ويحتوي هذا الإطار على ستة محاور تتضمن ثمانية عشر عنصرًا رئيسيًا من عناصر الأمن السيبراني، ويساعد هذا الإطار على تعميق الفهم لفضاء المملكة السيبراني. وتم استخدام هذا الإطار لتصميم الاستراتيجية على المستوى الوطني. ويوضح شكل (٣٥): محاور وعناصر الإطار المرجعي لتطوير الاستراتيجية الوطنية للأمن السيبراني

الإطار المرجعي (السيبراني، ٢٠٢٠)



شكل (٣٥): *محاور وعناصر الإطار المرجعي لتطوير الاستراتيجية الوطنية للأمن السيبراني*

وتعرف المحاور الستة الرئيسية لهذا الإطار كما يلي: (الهيئة الوطنية للأمن السيبراني، ٢٠٢١).

- محور "التكامل":

يعنى هذا المحور بتكامل جميع مكونات منظومة الأمن السيبراني، ويحتوي على ثلاثة عناصر هي:

- أنظمة وسياسات وتنظيمات: الأطر والآليات اللازمة لإدارة التوجهات الاستراتيجية بالشكل المطلوب، وذلك من خلال الصلاحيات والسياسات والأنظمة والتشريعات اللازمة.
- الاستراتيجية الوطنية والميزانية: تطوير ومراجعة التوجهات الاستراتيجية الوطنية للأمن السيبراني، من خلال العمل على إعداد ومراجعة النطاق والأهداف والمبادرات والميزانيات المتوقعة ومؤشرات الأداء لقياس مدى الالتزام بالخطة التنفيذية.
- حوكمة وإدارة الأمن السيبراني: إعداد إطار حوكمة يوضح الأدوار والمسؤوليات الصلاحيات للجهات والأفراد المعنيين.

- محور "التنظيم":

يعنى هذا المحور بتحديد البنى التحتية الحساسة وإدارة المخاطر السيبرانية، ويحتوي على عنصرين:

- إدارة المخاطر السيبرانية: تقليل المخاطر من التهديدات والثغرات، عن طريق تنفيذ عمليات إدارة المخاطر التي تبدأ بتحديد البنى التحتية الحساسة، وتعريف المخاطر وتقييمها والعمل على تقليلها، انتهاءً بمراقبة المخاطر ورصدها للمساهمة بتعزيز الصمود السيبراني.
- المعايير والضوابط الوطنية: توفير نموذج مرجعي للمعايير الوطنية والضوابط السيبرانية، بحيث تعمل على تحديد نطاق الضوابط الأساسية والفرعية، ونوعيتها ومدى شموليتها وكيفية العمل على تنفيذها مع مختلف القطاعات والجهات ذات العلاقة، ووضع الآليات اللازمة للتأكد من التزام الجهات بهذه الضوابط.

- محور "التوكيد":

يعنى هذا المحور بالتأكد من حماية الفضاء السيبراني، ويحتوي على أربعة عناصر هي:

- الوعي بالأمن السيبراني: التوعية في المجال السيبراني على المستوى الوطني عن طريق حملات التوعية والتدريب؛ مما يساهم في تحسين السلوك وتبني أفضل الممارسات وتطبيقها.
- الهويّات الرقمية الوطنية: تعزيز جوانب الأمن السيبراني في الهويات الرقمية على المستوى الوطني، مما يساهم في رفع مستوى موثوقية الهويات الرقمية في الفضاء السيبراني للتجارة وتوفير الخدمات الحكومية وغيرها.
- التشفير الوطني: الآلية الوطنية لتشفير البيانات وتشمل تطوير وتقييم أنظمة وخوارزميات ومعايير التشفير الوطنية.
- حماية موارد الإنترنت الحساسة: عن طريق تعزيز جوانب الأمن السيبراني لحماية موارد الإنترنت الحساسة وتعزيز اعتمادية الإنترنت من جوانب الأمن السيبراني.

- محور "الدفاع":

يعنى هذا المحور بمواكبة آليات الدفاع الوطنية السيبرانية للمخاطر والتهديدات المتسارعة، ويحتوي على خمسة عناصر هي:

- معرفة التهديدات وتحليلها: رصد التهديدات السيبرانية ومشاركتها مع الجهات ذات العلاقة من القطاعين العام والخاص.
- إدارة الثغرات: تشمل العمل بشكل مشترك مع الأفراد والجهات ذات العلاقة؛ للبحث عن أي ثغرات يمكن استغلالها ومشاركة التوصيات مع الجهات المتأثرة لاتخاذ الإجراءات المناسبة.
- المراقبة والتنسيق: تعزيز مستوى الدراية الأمنية وتصنيف التهديدات واختبار خطط الاستجابة للحوادث على هجمات محددة ومن ثم احتواؤها في حال حدوثها قبل أن تتسبب بأضرار كبيرة.
- الاستجابة للحوادث: آليات الاستجابة للحوادث واختبار خططها على هجمات محددة لخلق تحسينات مستمرة للتكيف مع التهديدات والمخاطر السيبرانية، ويتم تنسيق الأنشطة على المستوى الوطني لاحتواء الهجمات السيبرانية وتقليل أضرارها والحد من تكرارها.
- استمرارية الأعمال والتعافي: يشمل هذا العنصر التأكد من وجود خطط للطوارئ واختبار البنى التحتية الحساسة والخدمات الإلكترونية الهامة، وكذلك إجراءات محددة لاستعادة عملها بعد الحوادث السيبرانية، والعمل باستمرار على إجراء هذه الاختبارات للتحقق من سلامة البنى التحتية الحساسة والخدمات الهامة، وجاهزيتها مستقبلًا.

- محور "التعاون":

يعنى هذا المحور بوضع الآليات المناسبة لبناء الشراكات ومشاركة المعلومات، ويحتوي على:

- الشراكات ومشاركة المعلومات: يمكّن من وضع السياسات والآليات وأفضل الممارسات التي تتيح مشاركة المعلومات المتعلقة بالتهديدات السيبرانية مع الجهات الوطنية والدولية، وكذلك المساعدة في التنسيق والتعاون مما يسهم في رفع الجاهزية والاستعداد والوقاية وسرعة الاستجابة في حالة وقوع حادث سيبراني.

- محور "البناء":

يعنى هذا المحور بالتأكد من وجود قاعدة وطنية متينة وآمنة، ويحتوي على ثلاثة عناصر كالتالي:

- الأبحاث والتطوير والصناعة: تشجيع الأبحاث في مجال الأمن السيبراني وفقاً لأولويات مشتركة على المستوى الوطني، ودعم الابتكار والاستثمار في مجال الأمن السيبراني لتحويل مخرجات الأبحاث والتطوير إلى منتجات وخدمات. كما يشمل تحفيز صناعة الأمن السيبراني لضمان بناء قدرات كافية.
- بناء القدرات الوطنية: يشمل هذا العنصر إعداد وتأهيل كوادر وطنية متخصصة في الأمن السيبراني وتطوير تلك الكوادر بالمحافظة عليها؛ وذلك لسد الاحتياج الوطني في هذا المجال من خلال برامج تعليم وتدريب عالية الجودة.
- بنية تحتية آمنة: العمل على تبني نهج استباقي لضمان أمن الأنظمة والأجهزة والخدمات عبر سلسلة التوريد بأكملها، بدءًا من التصميم حتى الإنتاج ومن ثم التشغيل وانتهاءً بالإتلاف، وتطوير آليات ومعايير للتقييم والاختبار والفسح لمعدات وبرامج وخدمات الأمن السيبراني؛ للتأكد من سلامتها واستعدادها.

عناصر الاستراتيجية الوطنية للأمن السيبراني:

تتمثل العناصر الأساسية للاستراتيجية الوطنية للأمن السيبراني في المبادئ الأساسية للتطوير والرؤية والأهداف الاستراتيجية ومؤشرات الأداء، وسنتعرف فيما يلي على كل عنصر على حدة. (السيبراني، ٢٠٢٠).

❖ المبادئ الأساسية للاستراتيجية الوطنية للأمن السيبراني:

تعتمد الاستراتيجية على سبع مبادئ أساسية، وهي:

١) مواءمة وطنية شاملة:

يعنى بتكامل وتنسيق الجهود عبر القطاع الحكومي والقطاع الخاص، وسياسات وتنظيمات مركزية بمسؤوليات مشتركة تسهم بتكامل منظومة الأمن السيبراني في المملكة.

٢) مركزية الحوكمة واللامركزية في التشغيل:

يعنى بوضع الأدوار والمسؤوليات على المستوى الوطني مما يسهم في وضوحها وسرعة في التنفيذ.

٣) مواكبة مع التطور السريع:

يعنى بالمرونة والمواكبة مع المستجدات في الفضاء السيبراني، والتعامل الفعّال مع التطورات التقنية، والاستفادة من التقنيات الناشئة والمتطورة للحد من التهديدات المتجددة.

٤) ترتيب الأولويات حسب مستوى المخاطر:

يعنى بمواءمة الموارد والقدرات حسب مستوى تأثير المخاطر، وإعادة تقييم المخاطر بشكل مستمر للتحقق من الاستخدام الأمثل للموارد المتوفرة.

٥) التعاون والدعم:

يعنى بمشاركة المعلومات والدروس المستفادة مع الشركاء المحليين والدوليين.

٦) بأيدٍ سعودية وفرص استثمارية:

يعنى بالاستثمار في الكفاءات الوطنية، والتحفيز على الابتكار وتطوير صناعة وطنية وجذب الاستثمارات الدولية لتعزيز الأثر الاقتصادي للمملكة.

٧) وضع معايير قياس ومؤشرات الأداء:

يعنى بقياس الأداء، لضمان ان تحقيق الأهداف ومعالجة الصعوبات.

❖ رؤية الاستراتيجية الوطنية للأمن السيبراني:

تم وضع رؤية للاستراتيجية الوطنية للأمن السيبراني تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو، وتتضمن الرؤية التي تسعى الهيئة إلى الوصول لها على

" فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار"

وهذه الرؤية تتضمن المصطلحات التالية: (الهيئة الوطنية للأمن السيبراني، ٢٠٢١)

- فضاء سيبراني: يشمل الفضاء السيبراني السعودي بأكمله.

- سعودي: لتلبية أولويات المملكة وتطلعاتها.
- آمن: التأكيد على حماية وصمود الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة.
- موثوق: يعزز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي.
- يمكّن النمو والازدهار: إسهام حماية الفضاء السيبراني في النمو الاقتصادي والاجتماعي للمملكة.

❖ الأهداف الرئيسية الاستراتيجية الوطنية للأمن السيبراني:

تسعى الاستراتيجية الوطنية للأمن السيبراني إلى تحقيق ستة أهداف رئيسية موضحة في الشكل (٣٦).

التكامل

- حوكمة متكاملة للامن السيبراني على المستوى الوطني

التنظيم

- إدارة فعالة للمخاطر السيبرانية على المستوى الوطني

التوكيد

- حماية الفضاء السيبراني

الدفاع

- تعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية

التعاون

- تعزيز الشراكات والتعاون في الأمن السيبراني

البناء

- بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني

شكل (٣٦): *الأهداف الاستراتيجية الوطنية للأمن السيبراني*

وفيما يلي وصف لكل هدف من أهداف الاستراتيجية: (السيبراني، ٢٠٢٠).

١) حوكمة متكاملة للأمن السيبراني على المستوى الوطني:

من أجل ضمان تحقيق درجات عالية من التنسيق والمواءمة؛ يلزم تبني توجه وطني شامل للأمن السيبراني، وذلك من خلال تحديد أدوار ومسؤوليات الجهات ذات العلاقة بالأمن السيبراني على المستوى الوطني وتكاملها لأجل تطوير التنظيمات والسياسات وتنفيذها، ومتابعة الالتزام بالمعايير الوطنية في جميع جوانب الأمن السيبراني. بالإضافة إلى وجود آليات موحدة للتخطيط والميزانية، وترتيب الأولويات في مجال الأمن السيبراني بفعالية، مما يعزز رفع كفاءة الإنفاق.

٢) إدارة فعالة للمخاطر السيبرانية على المستوى الوطني:

إدارة المخاطر السيبرانية على مستوى الجهات والقطاعات، وعلى المستوى الوطني، وتحديد العناصر المتضررة في الفضاء السيبراني، ومدى حدّة الضرر، واختيار أفضل الطرق لمعالجتها، أو الحد من آثارها. بالإضافة إلى تحديد إجراءات الحماية والدفاع، حسب درجة المخاطر.

٣) حماية الفضاء السيبراني:

إن وجود ضوابط شاملة ومعايير وطنية، ونظام لمتابعة الالتزام؛ يحقق حماية منظومة الأمن السيبراني، بالإضافة إلى رفع مستوى وعي المجتمع بالأمن السيبراني، واستمرار التواصل وتعزيزه معه؛ من خلال حملات توعوية إعلامية عامة

للأفراد والجهات. وهذا مما يحقق النضج والتطبيق لضوابط الأمن السيبراني على مستوى الأفراد والقطاعات والجهات الوطنية.

٤) تعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية:

التعزيز والتطوير المستمر، للقدرات الوطنية في الدفاع ضد التهديدات السيبرانية، وذلك لكشف الهجمات والتهديدات السيبرانية، والتعامل معها، والاستجابة ومن ثم التعافي منها في حال الإصابة بها.

٥) تعزيز الشراكات والتعاون في الأمن السيبراني:

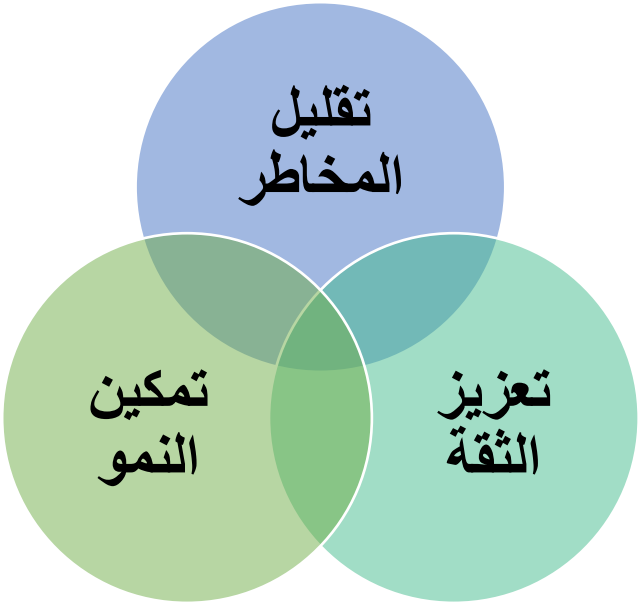
يتطلب الأمن السيبراني وجود شراكات محلية ودولية فعالة، ومعززة بآليات متطورة لمشاركة المعلومات؛ حتى تمكّن من التطوير والتحسين المستمر، ومشاركة أفضل الممارسات والمعلومات الاستقصائية والتدابير اللازمة. بالإضافة إلى أهميتها العالية في مواكبة التهديدات، والحد من المخاطر. والوصول إلى الدرجة المرجوة من التعاون، ويسهم في تعزيز الشراكات، وبناء قنوات لمشاركة المعلومات داخل المملكة وخارجها، في مشاركة المعلومات المتعلقة بالأمن السيبراني.

٦) بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني:

حماية الفضاء السيبراني للمملكة يتطلب وجود قاعدة قوية من الكوادر الوطنية المؤهلة في هذا المجال؛ بالإضافة لصناعة أمن سيبراني وطنية مزدهرة، ومن التوجهات الرئيسية؛ بناء القدرات الوطنية في الأمن السيبراني، من خلال برامج تعليم وتدريب عالية الجودة؛ بالإضافة إلى برامج تحفز الصناعة والبحث والتطوير والابتكار والاستثمار في الأمن السيبراني وتدعمها؛ لتمكين النمو والازدهار.

❖ مؤشرات الأداء:

تم تصميم عدد من مؤشرات الأداء الرئيسية لقياس مستوى تحقيق كل هدف من أهداف الاستراتيجية. كما تم تحديد خط أساس ومستهدف سنوي لكل مؤشر؛ وذلك بناءً على نتائج دراسة الوضع الراهن والتجارب الدولية وورش العمل مع المختصين والاستشاريين. وقد تم ربط المؤشرات بثلاثة نتائج استراتيجية موضحة في الشكل (٣٧) يتم الوصول لها من خلال احتساب المؤشرات بما يحقق الوصول إلى رؤية الاستراتيجية، وتسعى المملكة إلى تحقيقها خلال خمس سنوات، من خلال تطور تنفيذ الاستراتيجية، والتزام الجهات الوطنية بالأدوار والمسؤوليات، والأطر والمعايير المناطة بها، وسوف تظهر المخرجات الوطنية تحسناً كبيراً على المدى البعيد. (السيبراني، ٢٠٢٠)



شكل (٣٧): *مؤشرات الأداء*

العنصر الثالث: سياسات ومعايير الأمن السيبراني:

فيما سبق ناقشنا الجوانب التقنية المختلفة لرفع مستوى الأمن والحماية للفضاء السيبراني في المنظمات، ولكن من المهم جداً الإشارة إلى أن الأساليب والتدابير التقنية في الأمن السيبراني لا تُعد كافية مالم تكن معززة بإجراءات إدارية تحددها المنظمة - بحسب استراتيجيتها وطبيعة عملها-والتي تهدف إلى تقليل احتمالية حدوث الانتهاكات الأمنية وذلك من خلال وضع سياسات ومعايير أمنية لضبط وتوجيه سلوك المستخدم للمحافظة على أصول المعلومات في المنظمة.

بشكل عام، لابد أن يتم وضع السياسات الأمنية في المنظمات بناءً على بعض المعايير الدولية في مجال أمن المعلومات وأن يكون هناك درجة عالية من الالتزام بها لضمان مواكبة المعايير العالمية إضافة إلى رفع المستوى الأمني المعلوماتي بناءً على تجارب وخبرات دولية تم ترجمتها واختزالها من خلال هذه المعايير مثل معيار ISO/IEC ٢٧٠٠١ وإطار NIST CSF.

يحدد معيار ISO / IEC ٢٧٠٠١ المتطلبات المستمرة لإنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات في المنظمات. ويشمل أيضًا متطلبات تقييم ومعالجة مخاطر أمن المعلومات المصممة خصيصًا لاحتياجات المنظمة. المتطلبات المنصوص عليها في هذا المعيار عامة وتهدف إلى أن تكون قابلة للتطبيق على جميع المنظمات، بغض النظر عن النوع أو الحجم أو الطبيعة. أما إطار NIST للأمن السيبراني NIST Cybersecurity Framework (NIST CSF) فهو عبارة عن مجموعة من المعايير ذات الصلة المصممة لتقديم إرشادات حول الأمن السيبراني. (Emmett Dulaney and Chuck Easttom, ٢٠١٨).

السياسات الأمنية:

تعتبر السياسة الأمنية –المُعدة من قبل الإدارة العليا في المنظمة-من الوسائل المهمة لتقليل المخاطر المهددة لأمن المعلومات في المنظمات. يتم تعريف السياسة الأمنية على أنها "وثيقة مكتوبة توضح كيف تخطط المنظمة لحماية أصول تكنولوجيا المعلومات الخاصة بها" (Ciampa, ٢٠١٨)، حيث تحدد السياسة إجراءات الحماية التي يجب تطبيقها للتأكد من وصول المخاطر الأمنية

التي تواجه أصول المؤسسة إلى الحد الأدنى، مثلا تحديد إجراءات الاستخدام المقبول للإنترنت داخل المنظمة. تعد السياسة الأمنية، جنبًا إلى جنب مع الإجراءات والمعايير والإرشادات المصاحبة لها، أمرًا أساسيًا لرفع مستوى الأمن السيبراني في المنظمة. إن وجود سياسة أمنية مكتوبة يمكّن المنظمة من اتخاذ الإجراء المناسب –عند الحاجة-لحماية أصولها المعلوماتية.

تكمن أهمية السياسة الأمنية في المنظمات في النواحي التالية: (Ciampa, ٢٠١٨)

- تعتبر وسيلة لإيصال ثقافة أمن المعلومات للمنظمة والسلوك المقبول لأمن المعلومات، وبالتالي تساهم في خلق ثقافة تنظيمية واعية للأمن السيبراني.
- تساعد في ضمان توجيه سلوك الموظف ومراقبته وفقًا لمتطلبات الأمان.
- يتم من خلالها الإسهاب في توضيح مخاطر محددة وكيفية معالجتها، وبالتالي يوفر الضوابط التي يمكن للمديرين استخدامها لتوجيه سلوك الموظف.

لذلك تكمن الحاجة في ضرورة وجود السياسة الأمنية في المنظمات من خلال تفصيل النقاط التالية في السياسة:

- تحديد موارد المنشأة الرئيسة، التي تعتبر ذات قيمة كبيرة للمنشأة؛ والتي يجب حمايتها.
- بموجب السياسة الأمنية يتم تحديد مهام ونطاق عمل فريق (أو إدارة) أمن المعلومات.
- تشكل مرجعاً رئيساً وموحداً للرجوع إليه عند تعارض المهام الخاصة بأمن المعلومات مع بعضها، أو مع غيرها، أو عند عدم قبولها أو عدم تطبيقها.
- تحدد أهداف المنشأة المتعلقة بأمن المعلومات.
- توضح مسؤوليات الموظفين وتحددها، فيما يخص معالجة المعلومات.
- تساعد في منع حدوث المفاجآت في الإجراءات أو الطلبات أو أحداث العمل اليومية.
- توضح مسؤوليات الاستجابة للأحداث التي تقع والتي تخص أمن المعلومات.
- توضح استجابة والتزام المنشأة ومسؤوليتها تجاه القوانين والمعايير العامة والخاصة.

أنواع السياسات الأمنية:

غالباً ما يكون لدى المنظمات سياسة أمنية عامة وشاملة للغاية وغالبًا ما تكون مفصلة، وبالتالي تميل معظم المنظمات إلى تقسيم السياسة الأمنية العامة إلى "سياسات أمنية فرعية" بحيث تكون تخصصية أكثر وتغطي مجالات عدة وبالتالي يسهل الرجوع إليها عند الحاجة، ويمكن إيضاح كلا النوعين كما يلي:

- السياسة الأمنية العامة:

السياسة الأمنية العامة هي السياسة التي تعتمد على رؤية المنشأة وأهدافها العامة، وتحدد توجهاتها ونطاق الأعمال الخاصة بأمن المعلومات فيها. وتبدأ السياسة الأمنية العامة بتحديد برنامج أمن المعلومات وأهدافه، ثم تنتقل إلى منح الصلاحيات وتحديد

المسؤوليات إلى اللازمة لتنفيذه، وتنتهي بوضع الآليات والطرق التي تضمن فرض البرنامج وتطبيقه على أرض الواقع. (Vacca, ٢٠١٣)

وللسياسة الأمنية العامة معايير ومميزات يجب وتطبيقها، وهي:

- أن يتم إنشاء السياسة الأمنية وتطبيقها وفق أهداف المنشأة العامة، بل يجب أن تكون أهداف المنشأة هي المحرك لها وتحت مظلتها. وبعبارة أخرى: يجب ألا تتعارض السياسة الأمنية مع أهداف المنشأة.
- يجب أن تكون سهلة الفهم واضحة المعاني ومرجعاً أساساً لموظفي المنشأة كافة.
- يجب أن تعد بطريقة يتم فيها تضمين أمن المعلومات في جميع إجراءات المنشأة وأقسامها.
- يجب أن تعد بالاستناد إلى القوانين والتشريعات والقواعد المطبقة على المنشأة (من الحكومة أو الجهات التشريعية)، وأن تدعمها.
- يجب أن تتم مراجعتها وتحديثها دورياً، وعند إضافة أو حذف نشاط أو قسم من أقسام المنشأة، وأن عند دمج المنشأة مع غيرها، أو عند تغيير مرجعيتها أو ملكيتها.
- أن يتم إصدار وتحديث السياسة الأمنية على شكل إصدارات أو طبعات مؤرخة.
- أن يكون لدى الوحدات والأشخاص المطبقة عليهم السياسة الأمنية إمكانية الوصول إلى الأجزاء التي يحتاجون إليها بسهولة، ولا يشترط عليهم قراءة باقي أجزاء السياسة.
- أن تكون قابلة للتطبيق لعدة سنوات، بحيث يمكن الاستفادة منها على المدى القريب والمتوسط، وأن تكون لديها القدرة على استيعاب المتغيرات خلال تلك الفترة.
- استخدام لغة سهلة ومحددة المعاني، والبعد عن استخدام الألفاظ التي تحتمل أكثر من معنى أو لا تكون محددة، مثل " ربما " أو " من الأفضل " أو " يحسن "، وكذلك البعد عن الألفاظ التي لا تكون معروفة لدى عموم المستخدمين.
- غالباً ما تكون السياسة الأمنية العامة ثابتة وقليلة التحديث.

يمكن القول بأنه من النادر أن توجد سياسة أمنية قادرة على أن تغطي كافة جوانب أمن المعلومات في جميع إجراءات المنشأة. لذلك، لا بد من وضع طريقة مناسبة للتعديل أو الإضافة على السياسة الأمنية، وترك مجال لذلك وفق ضوابط وشروط محددة، ويجب مراعاة إمكانية مراجعة السياسة الأمنية، والتعديل فيها مع مرور الزمن أثناء التطبيق حسب الحاجة.

- السياسة الأمنية التخصصية:

السياسة الأمنية التخصصية هي سياسة أمنية متخصصة في موضوع أو تخصص معين بشكل تفصيلي أكثر من السياسة الأمنية العامة وتحتاج إلى التحديث بشكل مستمر حسب الموضوع أو التقنية التي تتناولها السياسة. ويتم إعداد مثل هذه السياسات عندما تظهر الحاجة للتركيز على تخصص أو إجراء أو قسم معين لأهميته، أو لكثرة التفاصيل فيه التي يجب أن يكون الموظفون على اطلاع عليها وعلم بها.

مثل أن يكون لدى المنظمة " سياسة مكافحة البرمجيات الخبيثة" والتي تحدد إرشادات فعالة للحد من تهديدات البرمجيات الضارة على شبكة وأجهزة كمبيوتر المنظمة، او "سياسة أمان VPN" والتي تحدد متطلبات الاتصال من خلال الشبكة الخاصة الافتراضية (VPN) للوصول عن بُعد إلى شبكة المنظمة. بشكل عام، تمتلك معظم المنظمات على الأقل سياسات أمنية فرعية تتناول الجوانب معينة حسب حاجتهم كسياسة الاستخدام المقبول وسياسة البريد الإلكتروني وغيرها من السياسات. (Ciampa, ٢٠١٨)

- سياسة الاستخدام المقبول:

تعتبر سياسة الاستخدام المقبول أمن أهم سياسات أمن المعلومات والتي يُوصى بإعدادها في كل منظمة. وهي سياسة تحدد الإجراءات التي قد يقوم بها المستخدمون أثناء الوصول إلى الأصول المعلوماتية مثل الأنظمة والشبكات.

يتم من خلال سياسة الاستخدام المقبول إيضاح كل ما يجب على المستخدم الالتزام به أثناء التعامل مع البنية التحتية التقنية والمعلوماتية للمنظمة بما يحقق الأمن المعلوماتي، كأن يتم تحديد النقاط التالية للمستخدم من خلال السياسة:

- تعد الأنظمة التقنية ومعدات الكمبيوتر والبرامج وأنظمة التشغيل ووسائط التخزين وموارد الشبكة التي توفر البريد الإلكتروني وتصفح الويب ملكًا للمنظمة. وبالتالي يتم استخدامها لأغراض العمل ولخدمة مصالح المنظمة، وليست للاستخدام الشخصي.
- حافظ على أمان كلمات المرور ولا تشاركها مع أحد. المستخدمون مسؤولون عن أمان كلمات المرور والحسابات الخاصة بهم والتي يجب اختيارها بعناية وعدم ربطها بمعلومات شخصية عن المستخدم. يجب تغيير كلمات المرور كل ٦٠ يوماً.
- يجب تأمين جميع أجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة باستخدام شاشة توقف محمية بكلمة مرور مع ميزة التنشيط التلقائي التي تم ضبطها على ١٠ دقائق أو أقل، أو عن طريق تسجيل الخروج من الكمبيوتر.

- سياسة البريد الإلكتروني:

غالباً ما تغطي سياسة البريد الإلكتروني في معظم المنظمات ثلاثة جوانب أساسية: استخدام البريد الإلكتروني الخاص بالمنظمة لإرسال رسائل البريد الإلكتروني الشخصية، واستخدام البريد الإلكتروني الشخصي من خلال شبكة المنظمة، وإعادة توجيه رسائل البريد الإلكتروني الخاصة بالشركة إلى حساب بريد إلكتروني شخصي. فيما يلي نماذج لبعض عناصر سياسة البريد الإلكتروني:

- يستخدم البريد الإلكتروني الخاص بالمنظمة لأغراض العمل فقط ومن قبل المستخدمين المصرح لهم بذلك.
- يُمنع مشاركة المعلومات السرية الخاصة بالمنظمة مع أي جهات اتصال خارجية دون إذن.
- يُحظر تمامًا إعادة توجيه رسائل البريد الإلكتروني الخاصة بالمنظمة إلى البريد الإلكتروني الشخصي.
- يُمنع تزييف معلومات الموظفين في توقيع البريد الإلكتروني الخاص بالمنظمة.

تطبيق عملي (١٣)

الهدف: أن يطبق المتدرب كيفية إعداد سياسة أمنية تخصصية.

الزمن: ١٥ دقيقة

يعمل المتدربون على استعراض نماذج سياسات الأمن السيبراني المعدة من قبل الهيئة الوطنية للأمن السيبراني والتي تغطي العديد من المجالات المتعلقة بأمن المعلومات في الجهات الحكومية، وهي عبارة عن محتوى يشمل نماذج توضيحية غير إلزامية لسياسات ومعايير ووثائق الأمن السيبراني.

الإرشادات:

١. يُقسم المتدربين إلى مجموعات، بحيث تتكون كل مجموعة من أربعة متدربين.
٢. تقوم المجموعات بالدخول على الرابط التالي والخاص بأدوات الأمن السيبراني والمُعدة من قبل الهيئة الوطنية للأمن السيبراني https://nca.gov.sa/pages/kit.html
٣. تقوم المجموعات باستعراض نماذج السياسات واختيار أحدها لتطبيقها ومناقشتها (من الأفضل أن يقوم المدرب بتوجيه المجموعات لاختيار نماذج مختلفة).
٤. يقوم المدرب بمناقشة النتائج مع المتدربين.

العنصر الرابع: نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية:

قبل الاطلاع عل نظام ولوائح الجرائم المعلوماتية في المملكة، لا بد من الاطلاع على أوجه الاختلاف بينها وبين الجرائم التقليدية، حيث تختلف الجريمة المعلوماتية عن الجريمة التقليدية من النواحي التالية: (القاضي، ١٤٣٦هـ).

- مستحدثة: ليست تقليدية، ذلك أن الجرائم المعلوماتية ظهرت حديثاً مع ظهور الثورة التقنية في المعلومات والاتصالات.
- متغيرة: حيث تستمر بالظهور بأشكال جديدة لتتماشى مع التطور التقني والمعلوماتي.
- عالمية: تعتبر الجريمة المعلوماتية عابرة للحدود، فليس شرطاً تواجد المجرم في مسرح الجريمة، حيث يمكن للمهاجم أن يكون في دولة ويرتكب جريمته في دولة أخرى.
- صعبة الاكتشاف والاثبات: لكون هذا النوع من الجرائم لا يترك آثاراً مادية محسوسة.
- خطرة: يعتمد هذا النوع من الجرائم على التقنية، لذلك فهي قد تشكل خطورة على الاقتصاد الوطني أو الدولي، كما أنها قد تشكل خطورة على مستوى الأمن الشخصي للأفراد.
- عدم وجود الاتساق الدولي في مجال مكافحتها بسبب اختلاف تصنيف الجريمة المعلوماتية من دولة إلى أخرى.

وبناءً على ذلك تم إصدار نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية والصادر بالمرسوم الملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨هـ، وفيما يلي مواد اللائحة.

المادة الأولى:

يقصد بالألفاظ والعبارات الآتية -أينما وردت في هذا النظام -المعاني المبينة أمامها ما لم يقتض السياق خلاف ذلك:

١. الشخص: أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة.
٢. النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.
٣. الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت).

٤. البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

٥. برامج الحاسب الآلي: مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.

٦. الحاسب الآلي: أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له.

٧. الدخول غير المشروع: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

٨. الجريمة المعلوماتية: أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

٩. الموقع الإلكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

١٠. الالتقاط: مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح.

المادة الثانية:

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

١. المساعدة على تحقيق الأمن المعلوماتي.

٢. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

٣. حماية المصلحة العامة، والأخلاق، والآداب العامة.

٤. حماية الاقتصاد الوطني.

المادة الثالثة:

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

١. التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح -أو التقاطه أو اعتراضه.

٢. الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا.

٣. الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

٤. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

٥. التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

المادة الرابعة:

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

١. الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.
٢. الوصول -دون مسوغ نظامي صحيح -إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

المادة الخامسة:

يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

١. الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
٢. إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
٣. إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

المادة السادسة:

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

١. إنتاج ما من شأنه المساس بالنظام العام، او القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.
٢. إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.
٣. إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.
٤. إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المادة السابعة:

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

١. إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

٢. الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

المادة الثامنة:

لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:

١. ارتكاب الجاني الجريمة من خلال عصابة منظمة.

٢. شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلًا سلطاته أو نفوذه.

٣. التغرير بالقُصَّر ومن في حكمهم، واستغلالهم.

٤. صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المادة التاسعة:

يعاقب كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا النظام؛ إذا وقعت الجريمة بناءً على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

المادة العاشرة:

يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة.

المادة الحادية عشرة:

للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

المادة الثانية عشرة:

لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفًا فيها.

المادة الثالثة عشرة:

مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها. كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقًا نهائيًّا أو مؤقتًا متى كان مصدرًا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه.

المادة الرابعة عشرة:

تتولى هيئة الاتصالات وتقنية المعلومات وفقًا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة.

المادة الخامسة عشرة:

تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام.

عصف ذهني (٥)

الهدف: أن يحلل المتدرب انتهاك أمني وتحديد تصنيفه كجريمة من عدمه.

الزمن: ١٥ دقيقة

في شهر سبتمبر من عام ٢٠٠٦ قام أربعة من الطلاب بالتنمر على طفل مصاب بالتوحد وذلك في مدرسة في مدينة تورين بإيطاليا. وقاموا بتصوير ذلك في مقطع فيديو ونشره على اليوتيوب التابع لشركة جوجل. انتشر مقطع الفيديو وحصد مشاهدات تتجاوز ٥٥٠٠ مشاهدة خلال شهرين.

وعندما تم إعلام شركة جوجل بذلك من قبل الشرطة الإيطالية، تم إزالة مقطع الفيديو. ولكن والد الطفل وبالتعاون مع أحد المنظمات التي تدعم حقوق الأطفال المصابين بالتوحد، قاموا برفع دعوى قضائية ضد أربعة من المديرين التنفيذيين في جوجل بتهمة التشهير وتهمة معالجة بيانات شخصية بطريقة غير مشروعة. وكان رد جوجل على الدعوى أنها تجاوبت بشكل سريع من خلال إزالة الفيديو عندما تم ابلاغها.

وفي شهر فبراير من عام ٢٠١٠ بَرّأت محكمة ميلانو جميع المديرين التنفيذين من تهمة التشهير، لكن المحكمة رأت أن ثلاثة من المديرين التنفيذيين مذنبون في معالجة البيانات الشخصية بصورة غير مشروعة، وفي تباطئهم في إزالة الفيديو عندما تم إبلاغهم من قبل الشرطة. وهؤلاء المديرون هم: نائب الرئيس ومدير الشؤون القانونية وأحد أعضاء مجلس إدارة جوجل ومستشار الخصوصية العالمية. وتم تحميلهم المسؤولية الشخصية بذلك لأن القانون الإيطالي ينص على أن الموظفين مسؤولون قانونياً عن أنشطة الشركات التي يعملون فيها. ولم يكن هؤلاء المديرون في إيطاليا وقت المحاكمة، كما تم تعليق الحكم بانتظار الاستئناف لذا لم يكن أي منهم تحت التهديد المباشر بالسجن.

كان موقف جوجل الذي أعلنوا عنه بأنهم لم يقوموا بتصوير المقطع أو تحميله أو مراجعته، ومع ذلك تم الحكم عليهم بأنهم مذنبون نظرا لأن قانون حماية البيانات يتطلب الحصول على إذن مسبق قبل التعامل مع البيانات الشخصية، لذلك جوجل كانت مسؤولة عن التأكد من أن المستخدم الذي نشر الفيديو قد حصل على موافقة كل من شارك في محتوى الفيديو. ولكن في عام ٢٠١٢، تم الغاء الإدانة من قبل محكمة الاستئناف الإيطالية وتم تبرئة المديرين التنفيذيين.

- ما رأيك بهذه الواقعة؟
- ماهي الإجراءات والسياسات الأمنية التي من الواجب اتخاذها –من وجهة نظرك-من قبل المواقع التي تعتمد على صناع المحتوى؟

الإرشادات:

١. يُقسم المتدربين إلى مجموعات، بحيث تتكون كل مجموعة من أربعة متدربين.
٢. دراسة الحالة من قبل المجموعة ومحاولة الإجابة على الأسئلة السابقة.
٣. يعمل المتدرب على مناقشة وجهات النظر مع المتدرب

حالة دراسية مطولة(٤)

الهدف:

- أن يحلل المتدرب كافة المفاهيم التي تم طرحها بالبرنامج.
- أن يربط المتدرب مفاهيم البرنامج بحالة واقعية لانتهاك أمني معلوماتي.

الزمن: ٢٥ دقيقة.

في عام ١٩٧٦، تم انشاء شركة T.J.Maxx التي تعتبر واحدة من أكبر الشركات في مجال بيع الملابس بالتجزئة في الولايات المتحدة الأمريكية والمعروفة بأسعارها التنافسية. تمتلك شركة T.J.Maxx سلسلة متاجر تصل إلى أكثر من ١٠٠٠ متجر في الولايات المتحدة لبيع الملابس والأحذية الرجالية والنسائية وللأطفال، إضافة إلى الألعاب ومستحضرات التجميل والإكسسوار وقطع الأثاث والمستلزمات المنزلية.

في عام ٢٠٠٧ بدأ اهتمام الشركات بأمن المعلومات يزداد بشكل كبير وذلك بعد الكشف عن الخروقات الأمنية المُربِكة في العديد من الشركات المعروفة. وتمكن العديد من القراصنة من الوصول الكامل إلى قواعد بيانات بطاقات الدفع الائتمانية في العديد من متاجر التجزئة الرائدة بما في ذلك شركة T.J.Maxx وشركة Barnes and Noble وشركةOffice Max . إضافة إلى حدوث أكبر وأشهر عملية سرقة لأرقام بطاقات الائتمان في صيف ٢٠٠٥ والتي استهدفت متجر Marshalls والمتخصص في بيع الملابس بأسعار مخفضة والواقع بالقرب من سانت بول بولاية مينيسوتا. ويعتقد المحققون في الحوادث الأمنية أن المهاجمين قد تمكنوا من توجيه جهاز لالتقاط الموجات اللاسلكية باتجاه المتجر واستخدموا جهاز كمبيوتر محمول لفك تشفير البيانات المنقولة لاسلكيا بين الأجهزة المحمولة للتحقق من الأسعار وسجلات النقد وأجهزة الكمبيوتر في المتجر. وقد ساعدهم ذلك في اختراق قاعدة البيانات المركزية لشركة TJX Cos وهي الشركة الأم لكل من متاجر Marshalls ومتاجر شركة T.J.Maxx . حصل ذلك بسبب ضعف مستوى أمان الشبكات اللاسلكية لمتاجر التجزئة التي تُقدر تكلفتها ١٧,٤ مليار دولار، حيث تم إعدادها بمستوى أمان أقل مما يتمتع به كثير من الأشخاص على شبكاتهم المنزلية.

تقول شركة TJX Cos والتي اكتشفت عملية الاحتيال في ديسمبر ٢٠٠٥، إن المهاجمين الذين لم يتم العثور عليهم حينها، قاموا بتنزيل ٤٥,٧ مليون رقم على الأقل من أرقام بطاقات الائتمان credit card وبطاقات الحسم المباشر debit card من قائمة السجلات السنوية. الرقم القياسي السابق لأرقام البطاقات التي تعرضت للسرقة تجاوز ما قدره ٤٠ مليون. حصل قراصنة TJX أيضًا على معلومات شخصية مثل أرقام رخصة القيادة والهوية العسكرية وأرقام الضمان الاجتماعي لـ ٤٥١٠٠٠ عميل -وهي البيانات التي يمكن استخدامها لسرقة الهوية. وقد اعتذرت الشركة عن الخطأ الأمني وعززت نظامها آنذاك بناءً على ذلك. كما قامت TJX بحذف نسخها الخاصة من السجلات التي سرقها المهاجمون، ولكنها لم تتمكن من فك تشفير الملفات التي تركها المهاجمون في نظامها. لذلك قد تستغرق تكلفة الاحتيال سنوات حتى يتم احتسابها. يمكن أن تنفق البنوك في العام الواحد ما قيمته ٣٠٠ مليون كمصاريف استبدال البطاقات المسروقة بياناتها، على الرغم من انتهاء صلاحية نصف البطاقات تقريبًا إضافة إلى إخفاء بعضها في البيانات المسروقة.

عصابة القراصنة (المهاجمون) كانوا على علم بأنه من الأفضل أمنياً أن يكون المهاجم خارج البلد المستهدف، وذلك لتجنب الملاحقة القضائية. لذلك كان يُعتقد في البداية أن الهجمات كانت تأتي من قراصنة من خارج البلاد. لكن التحقيقات كشفت بأن أكثر الهجمات مصدرها محلي مما أدى إلى محاكمة ١١ رجلاً في ٥ دول متضمناً ذلك الولايات المتحدة الأمريكية. وما يُثير الاهتمام أكثر بأن زعيم العصابة كان مُخبراً في جهاز الخدمة السرية في الولايات المتحدة الأمريكية.

في أغسطس من عام ٢٠٠٨، اتهمت الحكومة الأمريكية ١١ شخصاً بعدة تهم منها الاحتيال المالي الإلكتروني، وتلف أنظمة الحاسب الآلي، والتآمر، والمصادرة الجنائية، وغيرها من التهم بسبب سرقة معلومات بطاقات الدفع الائتمانية من شركات مثل شركة T.J.Maxx وشركة Barnes and Noble وشركةOffice Max . وفي شهر أغسطس من عام ٢٠٠٩ اتُهم العديد من أفراد العصابة نفسها مرة أخرى بسرقة بيانات ما يقارب ١٣٠ مليون بطاقة ائتمانية من شركة Heartland Payment Systems وهي الشركة التي تعالج بطاقات الدفع الائتمانية. وتم توجيه لوائح الاتهام لخمسة منهم في يوليو من عام ٢٠١٣.

تشكلت العصابة التي شاركت في جميع تلك الحوادث في عام ٢٠٠٣. وبين عامي ٢٠٠٣ و٢٠٠٧ كانت العصابة تستخدم طرقاً سهلة لاستغلال الثغرات الموجودة في أمن الشبكات اللاسلكية في متاجر التجزئة، حيث لاحظت العصابة أنه لا يوجد تدابير أمنية كافية لشبكاتهم اللاسلكية. ونتيجة لذلك فأن عملية الحصول على اسم المستخدم وكلمة المرور الخاصة بالموظفين أمر سهل حيث يتطلب ذلك الانتظار صباحا بأجهزة الحاسب الآلي المحمولة خارج متاجر التجزئة. ومن ثم يتم التنصت على حركة مرور الشبكة عندما يقوم الموظفون والمديرون بتسجيل الدخول إلى حساباتهم الوظيفية.

ومما يزيد الأمر سوءاً أن لتلك الحسابات الوظيفية صلاحية الوصول إلى أنظمة تقنية المعلومات الأخرى في شركة تي جي ماكس، متضمناً ذلك الأنظمة التي تحفظ بيانات البطاقات الائتمانية. وباستخدام هذه المعلومات كان للمهاجمين وصول مباشر لمعلومات بطاقات الدفع الائتمانية. وقد قام أفراد العصابة لمدة عام تقريباً على استخراج البيانات وتخزينها على خوادم الشركة الخاصة وذلك بهدف استرجاعها في الوقت المناسب لهم. وكان هدف العصابية بيع بيانات البطاقات الائتمانية بمبالغ زهيدة.

وشكلت هذه الطريقة التي استخدمتها العصابة في هجماتها الأساس للائحة الاتهام في عام ٢٠٠٨.وبدءاً من أغسطس من عام ٢٠٠٧ قامت العصابة بتطوير مهاراتها وبدأت باستخدام هجمات حقن SQL لتثبيت برامج ضارة على تطبيقات البكة والوصول إلى قواعد بيانات الشركة. واستخدمت العصابة هذه الطريقة في هجماتها والتي جاءت في لائحة الاتهام التي وُجهت لهم في عام ٢٠٠٩.

زعيم العصابة هو ألبرت غونزاليس، وهومن سكان مدينة ميامي في ولاية فلوريدا. وبدءاً من عام ٢٠٠٣، كان ألبرت يتجول بسيارته في منطقة ميامي بحثاً عن شبكة لاسلكية غير آمنة لأحد متاجر التجزئة مستعيناً في ذلك بجهازه المحمول. وتقوم محلات التجزئة عادة باستخدام هذه الشبكات لنقل معلومات بطاقات الائتمان من آلة تسجيل المدفوعات النقدية إلى خوادم شركة T.J.Maxx . وعندما تجد العصابة شبكة مفتوحة تقوم باستخدام برنامج خاص للتصنت على الشبكة Sniffer مجهز خصيصاً لسحب بيانات وأرقام بطاقات الائتمان ومن ثم يتم بيع هذه البيانات في السوق السوداء. أحد أشهر هذه البرامج هو برنامج Wireshark وهو

برنامج مجاني ومفتوح المصدر وسهل الاستخدام، يعمل على تحليل الحزم Packet Analyzer المنقولة عبر الشبكة، يتم استخدامه غالباً لاستكشاف أخطاء الشبكة وتحليل البيانات وتطوير البروتوكولات. كانت الضحية الأكبر لهذا الهجوم هي شركة T.J.Maxx والتي فقدت بيانات أكثر من ٤٠ مليون بطاقة ائتمانية. بعد ذلك تطورت العصابة وقامت باستخدام هذه المعلومات لتحديد استراتيجية الهجوم المناسبة لاستهداف أنظمة محددة تستخدمها تلك الشركات. كما كانت العصابة تحلل المواقع الالكترونية لتلك الشركات بهدف معرفة تطبيقات الانترنت المستخدمة، ومن ثم تضع العصابة الاستراتيجية المناسبة للهجوم على تلك المواقع.

وحصل زعيم العصابة ألبرت غونزاليس على أكثر من مليون دولار كأرباح بيع بيانات البطاقات الائتمانية، وفي شهر أغسطس من عام ٢٠٠٩ أقر ألبرت غونزاليس بأنه مذنب بما نسب إليه من اتهامات في قضية شركة T.J.Maxx.

في عام ٢٠٠٣ أصبح ألبرت غونزاليس مخبراً لجهاز الخدمة السرية وذلك بعد القبض عليه لارتكابه جرائم مختلفة. وبطبيعة عمله هذه، ساعد ألبرت غونزاليس في عام ٢٠٠٤ في القبض على ٢٨ فرداً تابعين لموقع shadowcrew.com والذي كانت تتم من خلاله سرقة بيانات عشرات الآلاف من البطاقات الائتمانية وبيعها بهدف تحقيق الأرباح. وبعد انتهاء ألبرت من عملية موقع shadowcrew.com، بدأ في مزاولة أعماله الاستغلالية.

الضرر المباشر الناتج من هجمات الاحتيال على بطبقات الدفع الائتمانية كان محدوداً. ففي شهر مارس من عام ٢٠٠٧ تم القبض على عصابة كانت تنوي استخدام البطاقات الائتمانية المسروقة من شركة T.J.Maxx لشراء منتجات تقارب قيمتها ٨ ملايين دولار من محلات Wal-Marts ومحلات Sam's Club والمنتشرة في ولاية فلوريدا. لكن الأضرار الجانبية كانت بالغة الأثر، حيث اضطرت شركة T.J.Maxx إلى عمل تسوية مع شركة Visa بمبلغ وقدره ٤٠ مليون دولار في نوفمبر ٢٠٠٧، كما عملت تسوية أخرى بقيمة ٢٤ مليون دولار مع شركة Mastercard في ابريل من عام ٢٠٠٨.

لم يطال تأثير هذه الهجمات شركة T.J. Maxx فقط، بل طال عشرات الملايين من العملاء الذي اضطروا إلى اصدار بطاقات ائتمان جديدة. أما بخصوص العملاء الذي اعتمدوا خاصية الدفع الآلي على بطاقاتهم الائتمانية المسروقة، فقد تلقوا اشعارات من مقدمي الخدمات لإشعارهم بأن المبالغ المطلوبة لم يتم خصمها بسبب إلغاء البطاقات وإصدار بطاقات جديدة بدلاً منها.

ولكن مما يلفت الانتباه، تم ملاحظة أن مبيعات شركة T.J. Maxx لم تتضرر بشكل كبير بسبب تلك الهجمات مع أن الحادثة قد تم توثيقها في الصحافة بشكل كبير. كما أن شركات الائتمان ومن خلال برامج الحماية التلقائية التي تقدمها بطاقات الائتمان، بإعادة جميع الأموال للعملاء الذين تعرضت بطاقاتهم لتلك الهجمات (ترجمة جعفر،٢٠١٤)، (Pereira,٢٠٠٧).

محاور النقاش:

- بناءً على السيناريو الذي حدث، ماهي أوجه الانتهاك لكل من عناصر أمن المعلومات الثلاثة CIA وهي السرية والنزاهة والتوافر؟
- ماهي الأخطاء التي وقعت بها شركة T.J.Maxx والتي جعلتها عرضة لهذه الهجمات؟
- ما هو التقييم العام لطريقة الشركة في التعامل مع الحادثة؟

المراجع العلمية

www.ipa.edu.sa

أولاً: المراجع العربية:

أغروال، كامبو، بيرس. (٢٠١٨). *أمن المعلومات وإدارة مخاطر تقنية المعلومات، (ترجمة جعفر العلوان)*. معهد الإدارة العامة، (العمل الأصلي نشر في عام ٢٠١٤).

الهيئة الوطنية للأمن السيبراني. (ديسمبر، ٢٠٢٠). *الاستراتيجية الوطنية للأمن السيبراني*.

خالد بن ناصر آل حيان. (٢٠١٩). *الحوسبة السحابية أساسيات ومبادئ وتطبيقات*. معهد الإدارة العامة.

ذيب بن عايض القحطاني. (٢٠١٥). أمن المعلومات. مدينة الملك عبدالعزيز للعلوم والتقنية.

لؤي القاضي. (١٤٣٦هـ). حقيبة البرنامج التدريبي "الجرائم المعلوماتية". معهد الإدارة العامة.

(٢٠٢١). تم الاسترداد من الهيئة الوطنية للأمن السيبراني: https://nca.gov.sa/

(١١، ٢٠٢١). تم الاسترداد من المركز الوطني للتصديق الرقمي: https://www.ncdc.gov.sa/

ثانياً: المراجع الأجنبية:

Ciampa, M. (٢٠١٨). Security+ Guide to Network Security Fundamentals. Cengage Learning.

Cisco. (٢٠١٧). Cisco visual networking index: Global mobile data traffic forecast update, ٢٠١٦-٢٠٢١. Cisco.

David Kim, Michael G. Solomon. (٢٠١٤). Fundamentals of Information System Security. Jones and Bartlett Learning.

Emmett Dulaney and Chuck Easttom. (٢٠١٨). CompTIA Security+ Study Guide. Sybex.

https://www.statista.com/. (٢٠٢١, ١١ ٢٠). Retrieved from https://www.statista.com/.

Michael E. Whitman, Herbert J. Mattord. (٢٠١٨). Principles of Information Security. Cengage Learning.

Organizations 'Social Media Accounts Cybersecurity Controls تم الاسترداد من .National (١١، ٢٠٢١). Cybersecurity Authority: https://nca.gov.sa/

Stallings, W. (٢٠١٩). Effective Cybersecurity Understanding and Using Standards and Best

Pereira, J. "How credit-card data went out wireless door," Wall Street Journal, May ٤،٢٠٠٧

"T.J.Maxx" https://en.wikipedia.org/wiki/TJ_Maxx, ٢٠٢١

Practices. Addison-Wesley.

Vacca, J. (٢٠١٣). Cyber Security and IT Infrastructure Protection. Syngress.

(٢٠٢١). Retrieved from Cybersecurity Venture: https://cybersecurityventures.com/

إدارة تصميم وتطوير البرامج
progdev@ipa.edu.sa