الجمهورية الجز ئرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة باجي مختار – عنابة كلية العلوم الإنسانية و الاجتماعية

قسم علم المكتبات السنة الثالثة ليسانس

السداسي 6 السنة الجامعية:- 2019 /2020

محاضرات في
مقياس إدارة المخاطر في أنظمة المعلومات

تقديم: د. الزبير بلهوشات

المحتويات

مقدمة

في عالم يُعد فيه الوصول إلى المعلومات المهمة أمراً أساسياً وحيوياً بالنسبة للأفراد والمؤسسات. غير أن قضية أمن المعلومات أصبحت أكثر أهمية من مسألة الوصول إليها، بسبب التطورات المتسارعة التي يشهدها عالم التكنولوجيات الجديدة للمعلومات والاتصال، وما صحبها من سهولة متز ايدة في الوصول إلى مختلف منافذ ومنابع المعلومات والحصول عليها بالطرق المشروعة وغير المشروعة. وهو ما أدى إلى تعاظم أهمية أمن المعلومات لحمايتها من مخاطر القرصنة والاختراق والاستعمال غير المشروع.

المحاضرة الأولى:- مفهوم نظم المعلومات

تعرف نظم المعلومات بأنها الأنظمة التي تتكون من مجموعة من الأشخاص، وسجلات البيانات، وبعض العمليّات اليدويّة وغير اليدويّة، وتعالج هذه النظم بالعموم البيانات والمعلومات الخاصة بكل منظومة، كما يمكن تعريفه بأنه مجموعة من العناصر التي تتداخل فيما بينها لجمع ومعالجة وتخزين وتوزيع المعلومات عن موضوعٍ معيّن بشكلٍ منهجي، وذلك لإسناد التنظيم، والتحكم به، والتحليل، وتشكيل تصوّر حالي ومستقبلي واضح عن الموضوع قيد البحث. نظم المعلومات هي مجموعة من البرامج التي تستخدم لأرشفة وإدارة وتنظيم البيانات، ومعالجتها بإجراءات معيّنة أُنشئت حسب آلية سير العمل في المؤسسة، وذلك للحصول على المخرجات النهائيّة، ويشار إلى أنّ نظم المعلومات تختلف اختلافاً كليّاً عن تكنولوجيا المعلومات، حيث إن نظم المعلومات تستخدم تقنيات تكنولوجيا المعلومات التي ابتُكرت لخدمة أعمالها القائمة عليها.

كانت نشأة علم نظم المعلومات كواحد من فروع علم الحاسب الآلي، وذلك لمحاولة استيعاب وفهم فلسفة إدارة تقنية المعلومات داخل المنظمات والمؤسسات بأنواعها، وتطور بعد ذلك ليصبح مجالاً بحد ذاته في الإدراة، كما أنّه محور مهم للبحوث في الدراسات الإداريّة، ويشار إلى أنّ نظم المعلومات تُدرَّس في الجامعات الكبرى، والمدارس التجاريّة في مختلف أنحاء العالم. تعتبر نظم المعلومات إلى جانب تقنية المعلومات، والموارد المالية، والمواد الخام، والآلات واحدة من الموارد الأساسيّة الخمسة المتاحة لمدراء المؤسسات، واستُحدث منصب رئيس قسم المعلومات في كثيرٍ من الشركات، والذي يعادل في أهميته الكثير من المناصب الأخرى كالرئيس التنفيذي، ورئيس قسم الماليّة، ورئيس العمليّات، ورئيس التقنيّة.

تطور نظم المعلومات وتستخدم، وتدير البنية التقنية للمعلومات في المنظمة، ولذلك تحولت الشركات من الاعتماد على الإنتاج إلى الاعتماد على المعرفة في عصر المعلومات الذي تلا العصر الصناعي، وبذلك فقد أصبح التنافس في السوق على العمليّة والابتكار بدلاً من التنافس على المنتجات والإنتاج، كما تحوّل التركيز على عمليّة الإنتاج والخدمات المصاحبة لها، وبذلك فقد أصبح العاملون وخبراتهم و ابتكاراتهم من أكبر ممتلكات الشركة في عصرنا الحالي، وحتى يتمكن صاحب المؤسسة من المنافسة في السوق فعليه أن يمتلك قاعدة تقنيّة معلوماتيّة قويّة للقدرة على الابتكاروالتطوير.

مجالات العمل في نظم المعلومات نظم المعلومات الإداريّة. التخطيط الاستر ليجي لنظم المعلومات. تطوير نظم المعلومات بشكلٍ عام.

وكل مجال من المجالات السابقة ينقسم إلى مجموعة من التخصصات الأخرى التي تتداخل مع غيرها من التخصصات والعلوم، فهناك العلوم الإداريّة، وعلوم الحاسوب، والبرمجة، والهندسة، والعلوم البحتة، والعلوم السلوكيّة، وإدارة الأعمال.

المحاضرة الثانية:- أمن المعلومات

يُقصَد بـأمن المعلومات المجال الذي يُبحَث فيه حول طرق وأساليب منع و اكتشاف محاولات الوصول غير المشروعة للمعلومات المتداولة عبر الشبكة الحاسوبية وعلى أجهزة الحاسوب.

مع مرور الأيام، تتنامى أهميّة تأمين وحفظ المعلومة من المخاطر المتعددة، والسبب يرجع إلى أمرين رئيسيّين:

- الأول: مُتعَلّق بِكَون المعلومات المتداولة على شبكة الانترنت عُرضَة للهجمات المتنوّعة نتيجة انتشار أدوات الاختراق والتنصت على الشبكة وغيرها من البرمجيّات الجاهزة التي تُسهّل عمل المُخترِق، فلم يعد الأمر كما الماضي؛ حيث كانت قدرات ومعرفة الاختراق مقتصرة على كمّ بسيطٍ من محترفي الحاسوب بل أصبحت هذه البرمجيات في مُتناوَل الهُوَاة ومحبي التقنيات.

- الثاني: هو أنّ المعلومات التي يجري تداوُلها على الشبكة هي معلومات قيّمة وهامّة؛ حيث أصبحت معلومات الشبكة تُشكّل هدفًا مُغريًا للمخترقين ومتصيدي البيانات.

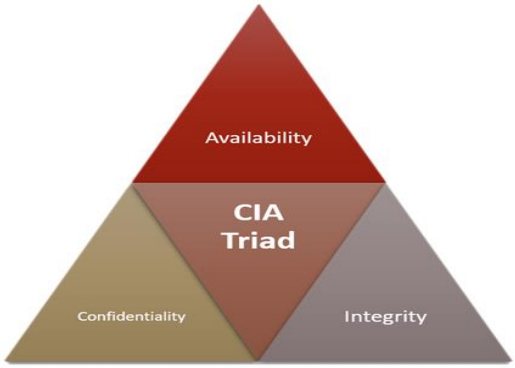
أصبحت حوسبة المعلومة من بديهيّات التقدّم والعمل في أيامنا هذه، حيث لا تخلو مؤسسة وجمعيّة ومدرسة وجامعة وبنك وبيت من الحواسيب، مما جعل هذا الكنز المعلوماتي مكشوفًا للمخترقين أصحاب النو ايا السيئة، حيث أن هناك من المخترقِين مَن هُم بنو ايا حسنة.

قام عُلماء الحماية والتشفير بتحديد عدة عناصر مهمّة يَنبَغي أن تتّصف بها الأنظمة الحاسوبيّة لكي يُمكِنَ القول عنها بأنّها آمنة، وقد حدّدوا ثلاثة عناصر تُشكّل بمجموعها مثلّثًا أُطلِق عليه مثلث CIA للحماية:

1. الموثوقيّة : Confidentiality / يُقصَد بهذا العُنصر أن تكون المَعلومة مَحْمِيّة من الوصول والقراءة غير المشروعة.

2. النّزاهة والتكامُليّة : Integrity / حيث يَجِبُ أن تكون المعلومة التي سنَحميها معلومةً صحيحة غير مغلوطة، مّما يعني أنه يجب حمايتها ليس فقط من محاولة الوصول غير المشروع؛ بل يجب أن نحميها أيضًا من التعديل عليها والتغيير في مُحتواها.

3. التو افريّة : Availability / أي أن تكون المَعلومة متوفّرة حين يُريد المستخدم أن يصل إليها، وأن لا تُحجَب عنه عند حاجته لها.



مثلث الحماية CIA

هناك بعض المفاهيم المُهمّة والشائعة في أمن المعلومات ومنها:

- الوصول غير المشروع :Unauthorized Access / يُقصَد بهذا المصطلح هو أي عمليّة وصول للمعلومة غير مصرّح بها، أي أنّ عمليّات الوصول منها ما هو مشروع ومصرّح به كما هي الحال مع المرسل والمستقبل للمعلومة، ومنها ما هو غير مصرّح له بالوصول لها، كما هو الحال مع الأشخاص الذين لم تُرسَل لهُم المعلومة ويحاولون الوصول لها بطرق غير مشروعة.

- التحقّق من المستخدم :User Authentication / أي أنْ يتمّ التحقّق والتأكد من هويّة المستخدم الذي يُحاول الوصول للمعلومة، هل هو المستخدم المصرّح له بالوصول؟ أم أنّه شخصٌ آخر يحاول القيام بوصولٍ غير مشروع للمعلومة.

- المُساءلة :Accountability / أي أن يكون هُناك إمكانيّة لمعرفة الأشخاص الذين وصلوا للمعلومة وما الذي قاموا به حتى يتسنّى للنظام أن يميّز الوصول المشروع وغير المشروع للمعلومة لكي يأخذ الإجراءات الوقائيّة لهكذا أمر.

المحاضرة الثالثة:- تنظيم إدارة المخاطر

يمكن تعريف إدارة المخاطر على أنها تلك الإدارة المتعلقة بترقُّب وتحديد التحديات أو التهديدات التي تؤثر على المنظمات في مختلف مراحل عمليات الاستثمار أو التجارة أو التسويق، والتي يمكن أن تؤثر بشكل سلبي على سير العملية الإدارية في المنظمات، ويختلف تعريف إدارة المخاطر حسب طبيعة النشاط الذي تمارسه المنظمة و أنشطتها اليومية، حيث يؤثر هذا الاختلاف على نوعية المخاطر التي يمكن أن تهدد النشاط المُنظمي، وبعد تحليل المخاطر المحتملة أو تلك التي وقعت فعلًا يتم اتخاذ مجموعة من الإجراءات التي تستهدف القضاء على تلك المخاطر بشكل نهائي أو التخفيف من حدة الأضرار الناجمة عن وقوعها كي لا تؤدي إلى خسائر مادية أو غير مادية فادحة.

يدخل في تعريف إدارة المخاطر وجود مجموعة متنوعة من المخاطر التي تختلف في حدة تأثيرها على الأنشطة اليومية والعمليات التنظيمية في المنظمات، ومن ذلك المخاطر الاستثمارية المتعلقة بارتفاع أو انخفاض في أسهم المنظمة في الأسواق المالية، أو ما يتعلق بالأوراق المالية المناسبة للعمليات الاستثمارية نفسها، وما يؤثر به ذلك على رأس مال المنظمة، بالإضافة إلى السوق التنافسي الذي يلقي بظلاله على التباين الذي قد يحصل في الحصة السوقية المحتملة للمنظمة مقارنة بالمنافسين المماثلين لها في الأسواق، خاصة في حالة وجود سلع متشابهة تعطي المستهلك مزيدًا من البدائل. وهناك بعض المخاطر المتعلقة بالعملية الاستثمارية، من حيث إدخال خطوط إنتاج جديدة أو توسعة خطوط الإنتاج القائمة، وقد تتخذ بعض المنظمات قرارًا بتوسيع حجم النشاط المنظمي بالكامل، وما يترتب على ذلك من فو ائد أو تهديدات، فضلًا عن الأزمات الاقتصادية التي قد تلقي بظلالها على وضع الاقتصاد المنظمي والسوق التنافسي في العديد من القطاعات المختلفة، بالإضافة إلى وجود بعض التقلبات في الأسواق من حيث العرض والطلب على بعض السلع والخدمات، كما أن هناك بعض المخاطر الأخرى كالمخاطر الائتمانية، والكوارث الطبيعية، والالتزامات القانونية، واحتمالية فشل بعض العمليات المنظميّة أثناء التنفيذ كعمليات التصميم أو التطوير، أو أي أحداث سلبية قد تتعرض لها المنظمة وتؤثر على نشاطها.

يدخل في تعريف إدارة المخاطر وجود خطة مُحكمة تسمى خطة إدارة المخاطر، حيث تهدف هذه الخطة إلى وضع مجموعة من التنبؤات الخاصة بالمخاطر المُحدقة بالمنظمة خلال الفترات الزمنية المستقبلية، كما تساعد على وضع بعض السياسات والإجراءات المتعلقة بمواجهة تلك المخاطر في حالة وقوعها بحيث يتم تحجيم الأضرار الناجمة على وقوع هذه المخاطر إلى أقل نسبة ممكنة، وغالبًا ما تكون خطة إدارة المخاطر على شكل وثيقة تحتوي على التهديدات المحتملة، ويتم التصريح بهذه الوثقية للأطراف التي تُعنى بمواجهة هذه المخاطر، كما يتم دراسة خطة إدارة المخاطر مُسبقًا بشكل تحليلي لتقييم إذا ما كانت هذه الخطة متناسبة مع طبيعة المنظمة وما يهددها مخاطر. ومن أبرز ما يجب أن تتميز به خطة إدارة المخاطر المرونة العالية بحيث تكون قادرة على تقدير حجم الأضرار المترتبة على كل نوع من المخاطر المحتملة، ليتم مقاومة أضرارها بأفضل الطرق المُتاحة، فهناك أضرار ذات تأثير طفيف، وأضرار أخرى ذات تأثير مرتفع، كما يجب أن يتم إجراء تحديثات وفقَ ما تقتضيه الظروف والحاجة على خطة إدارة المخاطر، ليكون هذه الخطة متكاملة وقادرة على التجاوب مع جميع المستجدات الفعلية التي لم تكُن في الحسبان سابقًا، كما يدخل في تعريف إدارة المخاطر وخطة إدارة المخاطر ما يُعرف بسياسات التحوُّط، والتي تكون على شكل عقود يتم فيها تشارك حجم الضرر بواسطة عقود تأمين أو معاملات تحوُّط خاصة.

بعد تعريف إدارة المخاطر لا بُدَّ من توضيح الخطوات العملية التي يتم بها تطبيق تعريف إدارة المخاطر على أرض الو قع المُنظَّمي، حيث إن هناك مجموعة من الإجراءات والخطوات المتتابعة يتم تنفيذها على أرض الو قع وهي كما يأتي:

- ✓ تحديد المخاطر التي من المحتمل أن يكون لها تأثير على الو قع المنظمي في مختلف مراحل الأنشطة المنظمية اليومية؛
- ✓ تحليل جميع المخاطر المأخوذة بعين الاعتبار في عملية إدارة المخاطر، والتفكير في طرق الوقاية من حدوثها؛
- ✓ مراجعة الأحداث السابقة التي واجهتها المنظمة في مجال المخاطر واحتوائها، ومحاول الاستفادة ممَّا مضى من أحداث تسببت في وقوع مخاطر بعينها، وكيف تمت معالجة تلك المخاطر؛
- ✓ وضع تخمينات متعلِّقة بإمكانية تجدُّد المخاطر التي عايشتها المنظمة فيما مضى، ومقارنة هذه المخاطر على مستوى المنظمات التي تمتلك أنشطة مشابهة، وكيف تنظر هذه المنظمات إلى المخاطر؛
- ✓ إدخال تطويرات على أنظمة الحماية من المخاطر ووضع كافة التكاليف المتعلقة بإحداث هذه التطويرات، ومقارنتها بالنتائج المتوقعة منها؛
- ✓ إعداد تقارير تفصيلية يتم تقديمها للمُلَّاك والمسؤولين عن الشؤون الإدارية في المنظمة من أجل وضعهم في صورة السياسات المتعلقة بإدارة المخاطر؛
- ✓ تتبع كافة العمليات الجارية في المنظمة، والتأكد من مو قفة هذه العمليات للمعايير التي تحول دون وقوع المخاطر، وإعطاء الموظفين التدريب الكافي لتجنب الخطر، وكيفية معالجته حين وقوعه؛
- ✓ إعادة تقييم الوضعية الراهنة للمنظمة، ومدى استجابتها مع خطة إدارة المخاطر الموضوعة، ويفضل أن تكون عملية إعادة التقييم نصف سنوية من أجل الوقوف على المخاطر التي تعرضت لها المنظمة في الفترات السابقة وتجنب حدوثها مستقبلًا.

المحاضرة الر بعة:- المخاطر المعلوماتية

مع الاعتماد الهائل على الأنظمة والتطبيقات الإلكترونية لدى الجهات الحكومية ومؤسسات الأعمال ومع تز ايد المخاطر والتهديدات المحدقة بتلك الأنظمة والتطبيقات بات من المهم إدارة الحوادث الأمنية الإلكترونية عند تعرض تلك الأنظمة والتطبيقات لأي خطر قد يعكر ديمومة عملها بالأداء والكفاءة المرجوة. إن تكرار توقف الأنظمة والتطبيقات الألكترونية المستمر مع طول فترة إستعادة عملها يعرض المؤسسات الربحية والغير ربحية إلى العديد من العو قب التي لا تحمد عقباها، قد يتبادر إلى ذهن القارىء ما هي الخسائر التي قد تتكبدها الجهات الغير ربحية جراء سوء إدارة الحادثة الأمنية الالكترونية، ونقول بأن الإستثمارات التي تم تخصيصها لتطوير تلك الأنظمة والتطبيقات قد لا تؤتي أكلها ومردودها وخصوصاً عند فقدان المتعامل الثقة في كفاءة القنوات الألكترونية لتلك الجهة والذي بدوره ينذر بهجران المتعاملين لتلك القناة وتأثر ما يسمى بالـ Welfare سمعة الجهة سلباً بين مثيلاتها من الجهات الحكومية وبالتالي دفع المتعاملين إلى اللجوء إلى القنوات التقليدية والذي يتعارض مع الأهداف التي من أجلها وجدت الخدمات الألكترونية والذكية. إما فيما يتعلق بالمؤسسات الربحية فأن توقف الأنظمة وسوء إدارة الحادثة الأمنية الألكترونية قد يعرضها لتكبد خسائر مالية كبيرة علاوة على فرصة خسارة العديد من عملائهم وخصوصا إذا ما توفر البديل من الشركات المنافسة.

نهدف من وراء هذه المحاضرة المختصرة إلى تسليط الضوء على الخطط اللازم توفرها لدى الجهات الحكومية ومؤسسات الأعمال و إبراز أهم المحاور الجوهرية التي تكفل إدارة المخاطر المعلوماتية وفق عمل مؤسسي ممنهج

يكفل لهم الإستجابة للحوادث في فترة قياسية والخروج منها بأقل الخسائر. ويعرف الخطر في علم أمن المعلومات من خلال المعادلة البسيطة التالية:

الخطر = التهديد * نقاط الضعف	التهديد Threats	نقاط الضعف Vulnerability	تصنيف الخطر
	عالي High	عالي High	عالي High
	عالي High	منخفض low	متوسط Medium
	منخفض low	منخفض Low	منخفض low

- ادارة المخاطر المعلوماتية

إن الإستعداد و إتخاذ جميع الخطط والأجراءات الوقائية والأحترازية قبل وقوع الحوادث الأمنية الألكترونية يكفل لفرق الإستجابة لحوادث وطواريء الحاسب الألي CERT التعاطي مع الازمة والحادثة بكفاءة وفاعلية، وكما هو معلوم لدى المختصين في الشبكات ومهندسي أمن المعلومات بأن التوقف للأنظمة والتطبيقات الإلكترونية نوعان (النوع الأول: توقف مخطط له Planned Shutdown والنوع الثاني: التوقف الغير مخطط له Unplanned Shutdown) سنركز على الحوادث الأمنية غير المخطط لها والتي تقع في الغالب بسبب العوامل الثلاثة الأتية:

1. توقف ناجم عن المخاطر وتهديدات الأنترنت وشبكات الحاسب الألي كالإختراق للأنظمة وقواعد البيانات وتعرض التطبيقات و أنظمة التشغيل للفيروسات والملفات الضارة والذي يتسبب في توقفها أو عدم إستقرارها وتأثر أدائها سلباً بشكل عام؛
2. توقف ناتج عن عطل تقني كتوقف قاعدة البيانات أو النظام الإلكتروني الناتج عن ثغرة برمجية System Bugs أو بسبب عطب أو تلف في جزء أو كل القاعدة Corrupted أو عدم التو فق Incompatibility مع برمجيات وتطبيقات أخرى تتسبب في تلف النظام عند عملية التنصيب أو عند إنقطاع التيار الكهربائي؛
3. توقف الإنظمة والتطبيقات الألكترونية الناتج عن الكوارث والحوادث الطبيعية، كتعرض المنطقة الجغر فية المستضيفة لتلك الأنظمة والتطبيقات إلى زلالزل أو عواصف تسفر عن تلف عدد من الموارد اللازمة لعمل تلك الأنظمة.

- خطط أمن المعلومات

ونود أن نشير هنا بأنه قد تختلف الممارسات والأدوات المعمول بها في إدارة المخاطر بإختلاف المجال، فان إدارة المخاطر المعلوماتية تختلف عن إدارة مخاطر المشاريع وإدارة المخاطر العسكرية وإدارة المخاطر الطبية وإدارة المخاطر المالية، فلكل مجال أدو اته التي تميزه عن المجال الأخر.

ويكفي أن تعلم أن عدد خطط أمن المعلومات هي ثلاثة (3) خطط رئيسية تهدف جميعها إلى التعامل مع الحادثة الأمنية في مختلف مراحلها بكفاءة وذلك لضمان إستعادة الأنظمة الإلكترونية في أسرع وقت ممكن وبأقل الخسائر

المحققة، يوضح النموذج أدناه مختلف خطط طوارىء الحاسب الألي وفترة دخول كل منها حيز التنفيذ وذلك من المنظور العملي:

- مراحل صياغة وصناعة خطط أمن المعلومات

نشير هنا بأن جميع خطط التعامل مع حوادث أمن المعلومات يتم وضعها وتطويرها قبل وقوع الحادثة الأمنية، إلا انه على القائمين على أمن المعلومات في الجهات الحكومية ومؤسسات الأعمال أن يولوا عددا من عناصر الاهمية وخصوصاً في المراحل الأولى من صياغة الخطط وهي كالتالي:

وقبل صياغة الخطط المذكورة أنفاً، يجب تنفيذ عدد من الأنشطة والتي تعتبر كمدخل لتلك الخطط وتعتبر جوهرية ولا يمكن بأي حال من الأحوال تطوير تلك الخطط دون الإنتهاء منها، ونؤكد عزيزي القارى على أهمية تلك الأنشطة وخصوصاً في المراحل الأولى من مراحل وضع لبنات تلك الخطط، ونسردها تاليا:

1. أولاً: قائمة الأصول المعلوماتية :Assets Registry يتم في هذه المرحلة تحديد جميع التطبيقات والأنظمة الإلكترونية في المؤسسة والأجهزة الحيوية Hardware's ومن ثم يتم تحليل أولوية تلك الأنظمة والأجهزة عبر تصنيفهم بالمستويات التالية (أولوية عالية، أولوية متوسطة، أولوية منخفظة) ونستفيد من تحديد أولويات النظام والعتاد إلى حسن إدارة الحادثة الامنية الألكترونية عند توقف عدد من الانظمة Systems Outage في نفس الوقت علاوة على مالك النظام أو التطبيق.Ownership ؛

2. ثانياً: مصفوفة الاعتمادية :Dependencies Matrix وتتم في هذه المرحلة من مراحل تقييم الوضع الراهن تحديد العلاقة بين الأنظمة والتطبيقات الإلكترونية من خلال مصفوفة الأعتمادية، حيث تعتمد بعض الأنظمة على

أنظمة أخرى في عملها بالشكل الأمثل، ونسرد هنا المثال التالي للتوضيح، إذا ما تعرض نظام إدارة الموارد المؤسسية ERP وخادم توزيع عناوين الشبكة DHCP Server للتوقف Outage في نفس الوقت، نقول إنه من المنطقي معالجة وإستعادة عمل خادم DHCP في المقام الأول نظراً لإعتماد الأول على الاخير في الإتصال بالشبكة؛

3. ثالثاً: الوتيرة المحتملة لوقوع الحوادث :Incidents Likelihood ويحدد هذا الجزء مدى إحتمالية تكرار حصول التوقف او تعرض كل نظام لخطر التوقف، ويتم من خلال هذه المرحلة التعاطي مع كل نظام من الأتظمة على حدى؛
4. ر ابعاً: تحليل الأثر على قطاع الأعمال :Business Impact Analysis ومن خلال مرحلة تحليل الأثر على قطاع الأعمال، يقوم الفريق المعني بوضع وتطوير الخطة إلى تحليل الأثار المترتبة على المؤسسة إذا ما تم إنقطاع النظام أو التطبيق عن الخدمة وما هي النتائج المترتبة عند توقفها ولو لبرهة معينة، مثال على ذلك، عند إنقطاع وتوقف نظام تداول الأوراق المالية والسلع في سوق الأوراق المالية والبورصة، فأن النتائج ستسفر عن توقف تداول الأوراق المالية بين المستثمرين حملة الأسهم وكنتيجة لهذا التوقف ستتأثر حجم الإيرادات المالية الواردة جراء هذا التوقف. تعمد العديد من المؤسسات بتحليل الأثار المترتبة عن إنقطاع وتوقف النظام إما نوعياً أو كمياً، إلا وأن أغلب الجهات الحكومية ومؤسسات قطاع الأعمال تفضل تطبيق المنهجية النوعية للتعرف على مستوى المخاطر التي قد تنجم جراء إنقطاع الخدمات وتوقف تلك الأنظمة من خلال مصفوفة تحليل الأثر. يتم وضع ميزان Scale وذلك إما بناء على المنهجية العالمية لأمن المعلومات ISO 2700X أو يتم إستحداثها من قبل الفنيين ومهندسي أمن المعلومات في المؤسسة وذلك بناء على تقديرهم النسبي للأصول ومدى حيوية وأهمية الأنظمة والتطبيقات الإلكترونية والعو قب المنطوية جراء إنقطاعها وتوقفها، يوضح النموذج التالي آلية إحتساب الأثر:

التصنيف		الأثر Impact		الوتيرة Likelihood	الوتيرة + الأثر
عالي High	=	عالي High	+	عالي High	
متوسط Medium	=	منخفض low	+	عالي High	
منخفض low	=	منخفض Low	+	منخفض low	

يتم تحديد مدى تؤثر المؤسسة عند تعرض تلك الأنظمة والتطبيقات وقواعد البيانات للتوقف، (الاثر عالي، الأثر متوسط، الأثر منخفظ)، تجدر الأشارة بأنه من الضرورة بمكان إشراك المتعامل مالك النظام في مرحلة تحليل الأثر، ونعزو ذلك إلى أن فريق إدارة الحوادث الأمنية قد لا يتمتع بالقدر الكافي من المعلومات التي تمكنه من تحديد مستوى الخطر والأثر الناجم عن توقف تلك الانظمة على المؤسسة أو الجهة دون إشراك المتعامل والمستفيد من النظام في المؤسسة Business Users .

- خطة إستمرار الاعمال Business Continuity Plan

تعتبر خطة استمرار الاعمال BCP من أهم عناصر ضمان عمل الانظمة في كل الاوقات والظروف،وكما تم الذكر سابقا فإن البيانات التي تم جمعها أنفاً في مرحلة دراسة الوضع الراهن وحصر الانظمة والتطبيقات وتحديد الاثر المترتب عن انقطاع تلك الانظمة في مصفوفة المخاطر Risk Registry بمثابة مدخلات لجميع الخطط، يتم توزيع

تلك الانظمة وبحسب أهميتها والاثر المترتب على توقفها الى (3) فئات لمر اكز البيانات الرديفة كما هو موضح في النموذج التالي:

1. موقع رديف بارد :Cold Site ويتم تخصيص خوادم لاستضافة وإحتضان الأنظمة والتطبيقات الالكترونية المصنفة بالأثر المنخفض عند توقها و انقطاعها عن الخدمة، حيث يتم تخصيص المو قع الرديفة الباردة للأنظمة والتطبيقات التي لا يترتب على توقفها خطر كبير على المؤسسة وبالإمكان جدولة عملية إستعادة عملها متى تيسر ذلك؛
2. موقع رديف دافء :Warm Site ويتم إستضافة الانظمة والتطبيقات وقواعد البيانات المصنفة بالاثر المتوسط على المؤسسة عند تعرضها للتوقف أو الإنقطاع، الفارق بين الموقع الرديف الدافء والساخن هو عدم تهيئة الموقع الرديف الدافء بالأدوات والانظمة الرديفة للاستجابة الفورية واللحظية عند توقف الانظمة والتطبيقات الرئيسية في مركز البيانات الرئيسي وبالامكان جدولة عملية المزامنة مع قواعد البيانات والانظمة بحسب ما يتم تقديره من قبل المعنيين بوضع خطة إستمرارية الاعمال في المؤسسة؛
3. موقع رديف ساخن :Hot Site ويتم تخصيص هذا الموقع لإحتضان وإستضافة الانظمة والتطبيقات وقواعدالبيانات المصنفة بالاثر العالي عند توقفها على المؤسسة اذا ما تم انقطاع وتوقف الخدمة لاي سبب كان، يميز المو قع الساخنة بتوفر رديف لأغلب مكونات الشبكة والبنية التحتية علاوة مع المزامنة اللحظية لبيانات الانظمة Instant Replication بين مركز البيانات الرئيسي والموقع الرديف الساخن وهذا ما يفسر إرتفاع التكلفة التشغيلية لها.

تحتوي خطة إستمرارية الأعمال Business Continuity Plan على (3) عناصر مهمة وهي كالتالي:

1. :Recovery Time Objective وهي الفترة الزمنية المقبولة لإستعادة التطبيقات والأنظمة الألكترونية الحيوية من لحظة توقفها، ويتم تحديدها بناء على دراسة وتحليل الاثار المترتبة عن توقفها و إنقطاعها عن الخدمة وتحديد الوقت المسغرق لإستعادة عملها بالشكل الطبيعي؛
2. :Recover Point Objective وهي كمية البيانات التي من المحتمل خسارتها من لحظة أخر عملية نسخ إحتياطي تمت على البيانات الحيوية أو المعاملات التي تمت من قبل الموظفين، وهنا نشير بأن فريق الاستجابة للحادثة الامنية في المؤسسة قد يستطيع إستعادة النظام إلى العمل، الا وان الفجوة التي تمت من أخر لحظة تم أخذ بها النسخة الاحتياطية قد لا تكفل إستعادة كافة البيانات والمعاملات التي تم إدراجها من قبل مستخدمين النظام من الفترة بين أخر نسخة إحتياطية وبين الفترة التي تمت بها الحادثة الامنية الالكترونية؛

3. Maximum Tolerant Downtime: وهي كمية البيانات والوقت المقدر والمقبول والمُحتمل خسارته لدى الجهة أو المؤسسة عند تعرض التطبيقات والأنظمة الألكترونية للعطب أو التوقف لاي سبب كان وعند تعذر الفرق التقنية المعنية لاستعادة عملها لاي ظرف كان.

- خطة التعافي من الكوارث الأمنية Disaster Recovery Plan

تدخل خطة الكوارث الأمنية Disaster Recovery Plan حيز التنفيذ أثناء الحادثة الأمنية، ونسرد هنا أبرز محتويات خطة التعافي من الكوارث الأمنية كما هو موضح تالياً:

1. إجراءات طلب الدعم والمساندة :Escalation Process أنشطة تحويل وإسناد حل العطب والحادثة الامنية إلى جهة أخرى، كشريك إستر لنجي أو شركة خاصة تم التعاقد معها لحل ومعالجة التوقف و إنقطاع الخدمة عن تلك الانظمة، يجب أن تحتوي الخطة على تفاصيل تتعلق بخطوات وإجراءات إستدعاء المعنيين في فريق طوارى الحاسب الألي في الجهة أو المؤسسة وبنقاط الأتصال للمعنيين من خارج المؤسسة والفترة الزمنية لمعالجة الحادثة الأمنية ومن هي الجهة الثانية المطلوب التواصل معها لطلب الدعم والمساندة عند تعذر الفريق الفني في المؤسسة معالجة الحادثة علاوة على إجراءات وقنوات الابلاغ عن توقف و انقطاع الخدمة وقائمة بارقام الطوارىء؛
2. الفترة الزمنية للإستجابة :Response Time وفي هذا البند من الخطة، يتم تحديد الفترة الزمنية للإستجابة للحادثة وفق ما تم تصنيفها عند صياغة الخطة، فإذا كانت الحادثة مصنفة بالعالي فأنه يتطلب الأستجابة الفورية للحادثة، يجب أن يتم تحديد الفترة الزمنية للإستجابة لكل حادثة على حدى في الخطة وذلك بناء على التصنيف الممنوح لها؛
3. الفترة الزمنية لإستعادة عمل الأنظمة :Recovery Time وفي هذا البند من الخطة يتم تحديد الفترة الزمنية المقبولة لإستعادة عمل النظام المتوقف عن العمل، فقد تكون الإستجابة والإنتقال إلى موقع الأنظمة التي تتطلب المعالجة والإستعادة سريعة إلا أن إجراءات معالجتها تتطلب فترة زمنية طويلة، وهنا يتم تحديد ما هي الفترة الزمنية المخصصة للفريق الفني لمعالجة التوقف و إنقطاع الخدمة وما هي نقطة الإتصال التالية لطلب الدعم والمساندة عند تعذر معالجة العطل.

الخطة البديلة لطوارى الحاسب الألي Contingency Plan

وإما خطة الطوارىء البديلة فتعرف على أنها الإجراءات التقليدية والورقية التي سيتم القيام بها وتنفيذها عند تعذر إستعادة التطبيقات والأنظمة الألكترونية من قبل الفنيين خلال الفترة التي تم تحديدها في خطة التعافي من الكوارث، يتبين للعديد بأن معظم الجهات الحكومية وشركات الأعمال تفتقد لخطة الطوارىء البديلة. نستشف ذلك عند مراجعتنا لإنجاز معاملة ما في أحد الجهات أو مؤسسات الأعمال فإن الموظف يتعذر بتوقف النظام عن العمل والذي بدوره يحرم المتعامل من الأستفادة من الخدمة، حيث يُثبت ذلك عدم توفر خطة الطواريء البديلة لاستقبال المعاملات بالوسائل التقليدية.

- ممارسات جوهرية:-

1. إختبارات تنظيمية :إختبار الخطط مرتان في كل سنة للوقوف على كفاءة وفاعلية الأجراءات والممارسات للتعاطي مع الازمات والحوادث والمخاطر الامنية من جانب وللتحقق من أداء فريق العمل والفرق الاخرى المعنية باستعادة عمل الانظمة والتطبيقات. إن إختبار الخطط عبر حوادث وسيناريوهات وهمية يبين للقائمين على تلك الخطط

الثغرات والفجوات التي تتطلب المعالجة قبل وقوع الحوادث وعلى ضوئها يتم تحديث إصدارات ومحتويات تلك الخطط؛

2. إختبارات تقنية :إختبار المو قع الرديفة مرتان في العام للوقوف على أية ثغرات تقنية تؤثر على سرعة الأستجابة للتوقف الطارىء والغير مجدول. كإختبار بطاريات الطاقة UPS واختبار سرعة إستجابة الانظمة الرديفة وكفاءة خطوط الربط الإلكتروني مع الموقع الرديفة التي تم ذكرها في سياق المقالة؛
3. إختبارات الكفاءة البشرية :وكأحد المحاور الجوهرية في إدارة المخاطر المعلوماتية يتم إختبار الموظفين بكافة فئاتهم ومستوياتهم الوظيفية للتحقق من إلمامهم بالاجراءات التي من اللازم إتباعها عن تعرض الانظمة والتطبيقات لاي من انواع الحوادث أو الكوارث الامنية الالكترونية كإجراءات وقنوات الابلاغ عن الحوادث الامنية ومدى إلمامهم بإجراءات الإخلاء والتجمع.

خاتمة

ينبغي أن تقوم منهجية إدارة المخاطر على تفادي الخسائر قدر الإمكان، مع تقبل مستوى معين من الخسائر (المخاطر المتبقية)، ثم التخطيط لاستمرار العمل ومعالجة نتائج ما يتبقى من مخاطر. فإدارة المخاطر والتخطيط لاستمرارية العمل هما عمليتان متلازمتان، بحيث لا ينبغي فصل إحداهما عن الأخرى. إن إدارة المخاطر هي صمام الأمان الأول في سياسة أمن المعلومات.

قائمة المراجع

1.- خالد بن سليمان الغثبر. محمد بن عبد الله القحطاني. أمن المعلومات بلغة ميسرة. ط. 1 . الرياض: مكتبة الملك فهد الوطنية. 2009، ص. ص. 22- 23

2.- رسلان، نبيلة إسماعيل. التأمين في مجال المعلوماتية والشبكات. القاهرة: دار الجامعة الجديدة، 2007

3.- سعد غالب ياسين. تحليل وتصميم نظم المعلومات. ط.1. عمان: دار المناهج للنشر والتوزيع، 2000. ص. ص. 17- 18

4.- الشر يعة، أحمد عبد العزيز. فارس، سهير عبد الله. الحاسوب و أنظمته. عمان: دارو ائل للنشر. 2000 . ص. 100

5.- علاء عبد الرزاق السالمي. تكنولوجيا المعلومات. عمان: دار المناهج، 2000. ص. 391

6.- محمد محمد الهادي. التطورات الحديثة لنظم المعلومات المبنية على الكومبيوتر. ط.1 . بيروت: دار الشروق، 1993، ص. 55

7.- نور، محمد إبراهيم. إدارة المخاطر. عمان: دار المسيرة للنشر والتوزيع والنشر، 2012

8.- DESROCHES, Alain. LEROY, Alain, VALLEE, Frédérique. La gestion de risques: principes et pratiques. Paris: Lavoisier, 2003.

9.- SCHICK, Pierre. Mémento d’audit interne: méthode de conduite d’une mission. Paris : Dunod, 2007