مخاطر الحاسب الالي

❖ **تعريف إدارة المخاطر لأمن المعلومات:**

هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها الشركة في تحقيق الأهداف العامة، والحد والتقليل من نقاط الضعف إن وجدت للحد من المخاطر إلى مستوى مقبول على أساس قيمة موارد المعلومات للشركة.

هناك أمران في هذا التعريف قد يحتاجان إلى بعض التوضيح:

أولا: عملية إدارة المخاطر هي تكرار العمليات الجارية ويجب أن يتكرر إلى ما لا نهاية لان بيئة العمل المتغيرة باستمرار، والتهديدات الجديدة والضعف تظهر كل يوم.

ثانيا: اختيار التدابير المضادة (الرقابة) المستخدمة لإدارة المخاطر يجب أن توازن بين الإنتاجية، والتكلفة، وفعالية التدابير المضادة، وقيمة الموجودات وحماية البيانات.

- **الخطر:** هو احتمال أن شيئا ما سيئا سيحدث يسبب الأذى لأحد الأصول المعلوماتية (أو الخسارة في الأصول).
- **الضعف :**هو الضرر لأحد الأصول المعلوماتية.
- **التهديد: أي** شيء فعل (من صنع الإنسان او فعل من أفعال الطبيعة) لديه القدرة على التسبب في ضرر.

❖ **تقييم المخاطر:**

1. تنظيم أمن المعلومات،
2. إدارة الأصول.
3. امن الموارد البشرية.
4. الاتصالات وإدارة العمليات.
5. التحكم في الوصول.
6. اقتناء نظم المعلومات وتطويرها وصيانتها أو ما يسمى بالتحديث.
7. إدارة استمرارية الأعمال.
8. التوافق التنظيمي.

❖ **خطوات عملية إدارة المخاطر:**

1. إجراء تقييم التهديد. وتشمل: أفعال الطبيعة، أعمال الحرب والحوادث والأفعال الضارة القادمة من داخل أو خارج الشركة.
2. إجراء تقييم الضعف، تقييم السياسات والإجراءات والمعايير، والتدريب، مراقبة الجودة والأمن التقني.
3. استخدام التحليل النوعي أو التحليل الكمي.
4. تحديد واختيار وتطبيق الضوابط المناسبة. النظر في الإنتاجية، وفعالية التكاليف، وقيمة الموجودات.
5. تقييم فعالية تدابير المكافحة. ضمان توفير الضوابط اللازمة لحماية فعالة من حيث التكلفة دون فقدان ملحوظ في الإنتاجية.

❖ **مهددات امن المعلومات:**

✓ **الفيروسات -**

الفيروس هو برنامج صغير مكتوب بأحد لغات الحاسب ويقوم بإحداث أضرار في المنظومة الرئيسية للحاسب الالي والمعلومات الموجودة على منظومة التخزين بمعني انه يتركز على ثلاث خواص وهي التخفي، التضاعف، وإلحاق الأذى.

✓ **مصادر الفيروس -**

يكمن مصادر الفيروس من خلال الرسائل الإلكترونية المجهولة، صفحات الإنترنت المشبوهة، نسخ البرامج المقلدة، استخدام برامج غير موثقة، كذلك تبادل وسائل التخزين دون عمل فحص مسبق مثل الأقراص والذاكرة المتنقلة وارسال الملفات داخل الشبكة المحلية.

✓ **للفيروس ثلاث خواص مؤثرة وهي:**

1. **التضاعف:** تتم عملية تضاعف الفيروس عند التحاق الفيروس بأحد الملفات وهنا تتم عملية زيادة عدد العمليات التي تتم إلى ملاين العمليات مما يسبب البطء في العمل أو توقف الحاسب عن العمل.
2. **التخفي**: لابد للفيروس من التخفي حتى لا ينكشف ويصبح غير فعال، ولكي يتخفى فأنه يقوم بعدة أساليب منها على سبيل المثال، صغر حجم الفيروس لكي يتمكن من الاختباء بنجاح في الذاكرة أو ملف آخر.
3. **إلحاق الأذى:** قد يتراوح الأذى الذي يسببه الفيروس بالاكتفاء بإصدار صوت موسيقي أو مسح جميع المعلومات المخزنة لديك، ومن الأمثلة الأخرى في إلحاق الأذى: إلغاء بعض ملفات النظام، إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت.

✓ **هجوم تعطيل الخدمة:**

هذا النوع من الخدمة يقوم فيه القرصان أو المعتدي بإجراء أعمال خاصة تؤدي إلى تعطيل الأجهزة التي تقدم الخدمة Server في الشبكات.

✓ **مهاجمة المعلومات المرسلة:**

هو اعتراض المعلومات عند ارسالها من جهة إلى أخرى، ويحدث هذا التعامل غالباً أثناء تبادل الرسائل خلال الشبكات:(الإنترنت -شبكات التي تستخدم الهاتف العام).

✓ **هجوم السيطرة الكاملة:**

في هذا النوع يقوم القرصان بالسيطرة الكاملة على جهاز الضحية والتحكم في جميع ملفاته كما لو كانت في جهازه هو ويمكن للقرصان مراقبة الضحية بصورة كاملة. يتم الهجوم بعد أن يضع القرصان ملف صغير على جهاز الضحية (عن طريق البريد الإلكتروني أو أي وسيلة أخرى) أو عن طريق استغلال نقاط الضعف في أنظمة التشغيل.

✓ **هجوم التضليل:**

وفيه يقوم القرصان بانتحال شخصية موقع عام. كما يمكن للقرصان أن ينتحل شخصية مستخدم موثوق به للحصول على معلومات غير مصرّحة له.

➢ **الوصول المباشر لكوابل التوصيل:**

يقوم المهاجم بالوصول المباشر لأسلاك التوصيل والتجسس على المعلومات المارة. ولكنه هجوم صعب ويتطلب عتاد خاص.

➢ **طرق وأدوات لحماية امن المعلومات:**

- التأمين المادي للأجهزة والمعدات.
- تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.
- تركيب أنظمة كشف الاختراق وتحديثها.
- تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.
- عمل سياسة للنسخ الاحتياطي.
- استخدام أنظمة قوية لتشفير المعلومات المرسلة.
- دعم أجهزة عدم انقطاع التيار.
- نشر التعليم والوعي الأمني.

➢ **طرق الحماية من مخاطر امن المعلومات:**

1. الاستعانة ببرامج المخاطر والأمن بشكل رسمي وهي الإدارة والتخطيط والبناء والتشغيل.
2. مؤشر قياس أداء البرنامج، وتحديد الثغرات والفرص المتاحة لتطويره، كما أن هذا المؤشر الموضوعي مفيد لصناع القرار من المدراء التنفيذيين الذين لا يلمون بالأمور التقنية في أغلب الأحيان.
3. استخدام منهجيات مبنية على المخاطر ينبغي على ادارة المخاطر اتباع نهج استباقي لتقييم المخاطر وإدارتها. ويجب على الأطراف المعنية من غير فريق عمل تقنية المعلومات اتخاذ مثل هذه القرارات، وعدم الإلقاء بمسؤوليتها على خبراء تقنية المعلومات فقط.
4. يتوجب على ادارة المخاطر الاستعانة بمؤشرات رائدة وجديدة لأداء الشركة التي تضم كلا من مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية، ولا ينبغي عليها التركيز فقط على مؤشرات الأداء الرئيسية لتقنية المعلومات.
5. مؤشرات المخاطر الرئيسية الجيدة عادة ما تكون بسيطة وقابلة للقياس، ولها تأثير مباشر على مؤشرات الأداء الرئيسية المتعددة.

➢ **مخاطر تهديدات أمن نظم المعلومات المحاسبية الإلكترونية:**

أولا/ من حيث مصدرها

✓ **مخاطر داخلية:(Internal)** يعتبر الموظفين بالإدارة المعنية هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية لأنهم على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق، ومعرفة نقاط القوة والضعف ونقاط القصور ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم.

✓ **مخاطر خارجية (External) :** وتتمثل في أشخاص خارج الشركة ليس لهم علاقة مباشرة بالشركة مثل قراصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية أو قد تتمثل في كوارث طبيعية مثل الزلزال والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام.

ثانيا/ من حيث المتسبب لها:

✓ **مخاطر ناتجة عن العنصر البشري :**

وهي الأخطاء التي تحدث من قبل أشخاص بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل أو السهو أو الخطأ.

✓ **مخاطر ناتجة عن العنصر غير البشري :**

وهي المخاطر التي قد تحدث بسبب كوارث طبيعية ليس للإنسان علاقة بها مثل حدوث الزلازل والبراكين والفيضانات والتي قد تؤدي إلى تلف النظام ككل أو جزء منه.

ثالثا/ مخاطر متعمدة:

✓ **مخاطر ناتجة عن تصرفات مقصود:**

وتتمثل في تصرفات يقوم بها الشخص متعمدا مثل ادخال بيانات خاطئة وهو يعلم ذلك، أو قيامه بتدمير بعض البيانات بهدف الغش والتلاعب والسرقة.

✓ **مخاطر ناتجة عن تصرفات غير مقصودة:**

وتتمثل في تصرفات يقوم بها الأشخاص نتيجة الجهل وعدم الخبرة الكافية كإدخالهم لبيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق ادخالها أو السهو في عملية التسجيل وتعتبر هذه المخاطر أقل ضررا من المخاطر المقصودة وذلك لإمكانية إصلاحها.

رابعا/ من حيث الآثار الناتجة عنها:

✓ **مخاطر تنتج عنها أضرار مادية:**

وهي المخاطر التي تؤدي إلى حدوث أضرار للنظام وأجهزة الكمبيوتر أو تدمير لوسائل تخزين البيانات والتي قد يكون سببها كوارث طبيعية لا علاقة للإنسان بها أو قد تكون بسبب البشر بطريقة متعمدة أو عفوية.

✓ **مخاطر فنية ومنطقية :**

وهي المخاطر الناتجة عن أحداث قد تؤثر على البيانات وإمكانية الحصول عليها للأشخاص المخول لهم بذلك عند الحاجة لها أو إفشاء بيانات سرية لأشخاص غير مصرح لهم بمعرفتها وذلك من خلال تعطيل في ذاكرة الكمبيوتر أو إدخال فيروسات للكمبيوتر قد تفسد البيانات أو جزء منها وتلك المخاطر قد تؤثر على الموقف التنافسي للشركة.

خامسا/ المخاطر من حيث علاقتها بمراحل النظام:

✓ **مخاطر المدخلات :**

وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال وتتمثل في:

1. خلق بيانات غير سليمة :ويتم ذلك من خلال خلق بيانات غير حقيقية ولكن بواسطة مستندات صحيحة يتم وضعها داخل مجموعة من العمليات دون أن يتم اكتشافها.

2. تعديل أو تحريف بيانات المدخلات: ويتم ذلك من خلال التلاعب في المدخلات والمستندات الأصلية بعد اعتمادها من قبل المسؤول وقبل ادخالها إلى النظام.

3. حذف بعض المدخلات ويحدث ذلك من خلال حذف أو استبعاد بعض البيانات قبل ادخالها إلى الحاسب الآلي، وذلك إما بشكل متعمد أو غير متعمد.

4. ادخال البيانات أكثر من مرة :والمقصود بذلك قيام الموظف بتكرار ادخال البيانات إلى الحاسب إما بطريقة مقصودة أو غير مقصودة.

✓ **مخاطر تشغيل البيانات :**

هي المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتتمثل مخاطر تشغيل البيانات في الاستخدام غير المصرح به لنظام وبرامج التشغيل وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غير قانونية أو سرقة البيانات الموجودة على الحاسب الآلي.

✓ **مخاطر مخرجات الحاسب :**

وهي المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية تشغيل ومعالجة البيانات، وقد تحدث تلك المخاطر من خلال طمس أو تدمير بنود معينة من المخرجات أو خلق مخرجات زائفة وغير صحيحة أو سرقة مخرجات الحاسب أو إساءة استخدامها.

➢ **مخاطر نظم المعلومات حسب الغرض منها:**

1. خرق النظم الحاسوبية بهدف الاطلاع على المعلومات المخزنة فيها والوصول إلى معلومات شخصية أو أمنية عن شخص ما.

2. خرق النظم الحاسوبية بهدف التزوير أو الاحتيال.

3. خرق النظم الحاسوبية بهدف تعطيل هذه النظم عن العمل لأغراض تخريبية.

4. أخطار فشل التجهيزات في العمل، أعطال كهربائية، حريق، كوارث طبيعية.

➢ **أصناف مخاطر نظم المعلومات الرئيسية:**

أولا: مخاطر المدخلات: وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام وهي مرحلة ادخال البيانات إلى النظام الآلي وتتمثل تلك المخاطر في البنود التالية:

1. الادخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.

2. الادخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.

3. التدمير غير المتعمد للبيانات بواسطة الموظفين.

4. التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.

ثانيا: مخاطر تشغيل البيانات:

وهي المخاطر التي تتعلق بالمرحلة الثانية من مراحل النظام وهي مرحلة تشغيل ومعالجة البيانات المخزنة في ذاكرة الحاسب وتتمثل تلك المخاطر في البنود التالية:

1. المرور (غير المرخص به) للبيانات والنظام بواسطة الموظفين.

2. المرور (غير المرخص به) للبيانات والنظام بواسطة أشخاص من خارج الشركة.

3. اشتراك العديد من الموظفين في نفس كلمة السر.

4. إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام.

5. اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.

ثالثا: مخاطر مخرجات الحاسب :

هي تلك المخاطر تتعلق بمرحلة مخرجات عمليات معالجة وتشغيل البيانات وما يصدر عن هذه المرحلة من قوائم للحسابات أو تقارير وأشرطة ملفات ممغنطة وكيفية استلام تلك المخرجات وتتمثل تلك المخاطر في البنود التالية:

1. طمس أو تدمر بنود معينة من المخرجات.

2. خلق مخرجات زائفة/ غير صحيحة.

3. سرقة البيانات/ المعلومات.

4. عمل نسخ غير مصرح (مرخص) بها من المخرجات.

5. الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.

6. طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.

7. المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم /ليس لهم الحق في استلام نسخة منها.

8. تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.

رابعا: مخاطر بيئية:

تحدث بسبب عوامل بيئية مثل الزلازل والعواصف والفيضانات والأعاصير المتعلقة بأعطال التيار الكهربائي والحرائق، وسواء كانت تلك الكوارث طبيعية أو غير طبيعية فإنها قد تؤثر على عمل النظام المحاسبي وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة نظم المعلومات المحاسبية الالكترونية.

➢ **أسباب لها علاقة بالموظفين وهي كالتالي:**

1. عدم كفاية وفعالية الأدوات الرقابية المطبقة لدى إدارة الشركة.

2. ضعف نظم الرقابة الداخلية لدى الإدارة المختصة وعدم فعاليتها.

3. اشتراك بعض الموظفين في استخدام نفس كلمات السر من أجل الدخول إلى النظـام والعبث بمحتوياته.

4. عدم الفصل بين المهام والوظائف المتعلقة بنظم المعلومات فـي الشركة.

5. عدم وجود سياسات واضحة وبرامج محددة ومكتوبة فيمـا يخـتص بـأمن نظـم المعلومات لدى الدارة المختصة.

6. عدم توفر نظام الحماية الكافية ضد مخاطر فيروسات الكمبيوتر.

7. ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب.

8. عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات بالشركة.

9. عدم التوصيف الـدقيق للهيكـل الـوظيفي والاداري الـذي يحـدد المـسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي لدى الشركة.

10. عدم توافر الخبرة اللازمة والتدريب الكافي والمهـارات المطلوبـة لتنفيذ الأعمال من قبل الموظفين

11. عدم إلزام الموظفين بأخذ إجازاتهم الدورية.

12. عدم الاهتمام الكافي بفحص التاريخ الوظيفي المهني للموظفين الجدد مما قد يـؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.

13. عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي الشركة.

14. عدم وجود الوعي الكافي لدى الموظفين بضرورة فحص البرامج أو الأقـراص الممغنطة الجديدة.

➢ **متطلبات حماية أمن نظم المعلومات وتتمثل في:**

1. وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمـل وتطبيقات الشركة.

2. يجب على الإدارة العليا دعم أمن نظم المعلومات لديها.

3. يجب أن توكل مسؤولية أمن نظم المعلومات لأشخاص محددين.

4. تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة.

5. تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية.

6. الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن.

7. تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط.

8. تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهـة المخاطر المتعلقة بنظم المعلومات.