إجراءات الأمن والوقاية من الجرائم الإلكترونية في المكتبات ومراكز المعلومات

أ. كادي زين الدين
مخبر أنظمة المعلومات والأرشيف في الجزائر
قسم علم المكتبات والعلوم الوثائقية
جامعة وهران1- احمد بن بلة

ملخص

يعد موضوع أمن وسلامة الأنظمة المعلوماتية في الوقت الراهن أكثر من ضرورة، لاسيما على مستوى المؤسسات الوثائقية التي تحولت إلى صيغة العمل الإلكتروني 100 %، فهذه المؤسسات في أي لحظة معرضة لأي خطر من الأخطار التي تتعلق إما بتعطيل أو إتلاف جزء من النظام أو النظام بالكامل، وقد تعددت هذه الجرائم لتشمل تخريب الأجهزة الإلكترونية بشقيها المادي وعلى مستوى البرامجيات، و باتساع رقعة استعمال شبكة انترنت في المؤسسات الوثائقية ما يجعل هذه الأخيرة معرضة لمجموعة من المخاطر التي تتعلق بالبرامجيات أو القرصنة أو تخريب الأقراص الصلبة أو سرقة الكلمات السرية للدخول إلى غير ذلك من المخاطر التي ما فتئت تظهر يوم بعد يوم في هذا المجال.

فمن خلال هذه الورقة البحثية سوف نتناول التعريف بهذه المخاطر وكذا إجراءات الأمن والوقاية منها بغية الاستفادة منها في إدارة مؤسساتنا الوثائقية مع الإشارة إلى موضوع أساسي له علاقة بالمعايير والمواصفات القياسية في ذلك، ونركز على وجود أنظمة وقائية ذات فعالية عالية بالأخص ما يتعلق بالفيروسات ومضاداتها وإمكانية الاستفادة من التأمين على هذه المخاطر وهو ما تعاني منه أغلب المؤسسات في العالم .

الكلمات المفتاحية :المخاطر، إدارة المخاطر، أمن المعلومات، تكنولوجيا المعلومات، المؤسسات الوثائقية، المواصفات القياسية، الأنظمة المعلوماتية

مقـدمة:

مع مرور الأيام يوم بعد يوم وجدت المؤسسات نفسها في مواجهة العديد من المخاطر والأزمات التي قد تتعرض لها في أي لحظة وما أن تجد نفسها قد استكملت الإجراءات الخاصة بالوقاية من خطر معين إلا وتجد نفسها أمام خطر جديد يهدد كيان ووجود هذه المؤسسة سواء كان ماديا أو معنويا.

هذا التطور الذي يلاحق هذه المؤسسات لم يأت وليد الصدفة بل يدخل في كنف التطورات التي جرت وتجري على نطاق واسع من التكنولوجيات الحديثة التي أصبحت جزء لا يتجزأ من العملية التسييرية لهذه المؤسسات، وخير دليل على ذلك ما حدث في الأيام الأخيرة من شهر سبتمبر على مستوى مكاتب البريد واتصالات الجزائر، حيث تعطلت الشبكة الخاصة بتسيير الحسابات البريدية لمدة 48 ساعة تقريبا على المستوى الوطني، ووقوع أزمة كبيرة في تسيير الحسابات البريدية للمواطنين وهو ما نتج عنه أيضا أزمات أخرى ذات علاقة لسنا بصدد دراستها الآن.

لا ندرى نسبة الخسائر التي تكبدتها مؤسسة اتصالات الجزائر عقب هذا الخلل الذي في الأخير تم الاستنجاد بمهندسين من فرنسا لتصليح الخلل، وهو ما يعطي إشارة واضحة للمشرفين على النظام بالتفكير في وضع إجراءات لعدم الوقوع في مثل هذه الأزمة التي لها تأثير وخلق أزمات على عدة مستويات أخرى من نواحي المجتمع.

إدارة المخاطر أصبح جزء لا يتجزأ من العملية التسييرية في الإدارة انطلاقا من وظائف أو عناصر الإدارة (العملية الإدارية)[1] والمتمثلة في التخطيط والتنظيم والتوجيه والرقابة، فأثناء قيام الإدارة بهذه العناصر الأربعة وجب عليها الأخذ في الحسبان الجزء الخاص بإدارة المخاطر في ذلك، هذا على العموم أما إذا أخذنا على

1نور الدين ،عصام،**إدارة المعرفة والتكنولوجيا الحديثة** ،دار أسامة للنشر والتوزيع :الأردن،2009،ص18

سبيل المثال المؤسسات الوثائقية فهل أدخل المشرفون على هذه المؤسسات نمط تسييري يتعلق بوضع خطط لمواجهة أي خطر ما قد يحدق بها وفي هذا السياق، أنا لا أتحدث الآن عن المخاطر أيا كانت بل سوف أدقق على وجه التحديد في المخاطر المتعلقة بأمن وسلامة المعلومات والأنظمة المعلوماتية التي أصبحت تمثل عصب وشريان الحياة بالنسبة لهذه المؤسسات .

مفهوم الخطر : يتعرض الإنسان منذ نشأته للعديد من الأخطار التي يترتب على تحقيقها خسارة مالية أو معنوية وتختلف هذه الأخطار من حيث طبيعتها ونوعيتها وحجم الخسارة المترتبة على تحقيقها حسب تطور الحياة البشرية وبسبب وسائل التكنولوجيات الحديثة وتقدمها المستمر...، إذ يتعرض الشخص للعديد من الأخطار التي تهدد ممتلكاته مثل خطر الحريق والسرقة والإتلاف والهلاك الاختلاس وغير ذلك من الأخطار التي تنجم عن عدم التأكد الممكن قياسه [1].

تعريف الخطر : تناول العديد من الباحثين والكتاب تعريف الخطر كل حسب وجهة نظره وغالب ما تكون وجهات النظر هذه متأثرة بنوع وطبيعة دراساتهم والأغراض التي يرمون إليها والمدارس التي ينتمون إليها إلا أن غالبية هذه التعريفات تؤكد على أنه عدم التأكد أو الشك أو الخوف من تحقق ظاهرة معينة أو موقف معين، بالنظر لما يترتب عليه من نتائج ضارة من الناحية المالية أو الاقتصادية ويمثل الخطر ظاهرة عامة ترتبط ارتباطا وثيقا بحياة الإنسان اليومية...وينبع الخطر أساسا من عدم التأكد الذي يحيط بالفرد من كل جانب، ويرجع عدم التأكد إلى مصدرين رئيسيين وهما:

-عدم القدرة على التنبؤ.

-عدم دقة المعلومات اللازمة للتنبؤ.

[1] أبو بكر عيد أحمد، وليد اسماعيل السيفو ، **إدارة المخاطر والتأمين** ،دار اليازوري العلمية للنشر والتوزيع ،عمان 2009،ص25

ومنه يمكن القول أن الخطر هو ظاهرة مركبة تنطوي على عدم التأكد الممكن قياسه بطريقة موضوعية من تجاوز الخسارة المادية الفعلية للخسارة المحتملة نتيجة وقوع حادث مفاجئ [1].

إذا كان هذا هو تعريف ومفهوم الخطر فينبغي بطبيعة الحال التعرف على إدارة الخطر، التي تختص بالتعامل مع الخطر أو الأزمة منذ ظهورها فماذا عن ما قبل الأزمة وما بعدها.

ونقصد بما قبل الأزمة فترة الاستقرار والأمان الذي يستمر منذ بدء إنشاء المنظمة(بداء من بزوغ فكرة إقامة المشروع) وحتى وقوع الأزمات[2].

وكما ذكرت آنفا فإن إدارة المخاطر في المؤسسات الوثائقية متشعب إلى عدة فروع وتخصصات شتى من بين هذه التخصصات أمن وسلامة المعلومات داخل هذه المؤسسات وطرق الحماية من المخاطر التي تهددها، إذ يتسع مفهوم أمن المعلومات ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية مختلف مصادر البيانات خصوصا المسجلة على وسائط إلكترونية وما يهددها من مخاطر العمل في البيئة الإلكترونية

أمن المعلومات في المؤسسات الوثائقية:

مع تطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لأخر أصبح النظر إلى أمن تلك البيانات

[1] أبو بكر عيد أحمد ،نفس المرجع ،ص 28

[2] صلاح عباس،**إدارة الأزمات في المنشآت التجارية** ،القاهرة: مؤسسة شباب الجامعة،2007،ص42

والمعلومات بشكل مهم للغاية، حيث يمكن تعريف أمن **المعلومات** بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية وكذا المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات. إن أمن المعلومات هو أمر ليس بجديد ولكن بدأ استخدامه بشكل فعلي منذ بدايات التطورات التكنولوجية، خصوصا شبكة الإنترنت ويرتكز أمن المعلومات إلى:

- أمن وحماية الولوج أو الدخول إلى الأنظمة.
- أمن حماية أنظمة التشغيل
-أمن وحماية البرامج والتطبيقات
- أمن وحماية قواعد البيانات

إن مسألة أمن المعلومات في المؤسسات الوثائقية أقل حدة مما يحدث في المؤسسات المالية والاقتصادية فطبيعة المعلومات بالنسبة لكلا النمطين من المؤسسات مختلفة، فالمؤسسة الوثائقية غالبا ما تعاني من إشكالية سرقة كلمات المرور أو تخريب بعض قواعد البيانات أو أنظمة التشغيل أو التجسس على بعض المعلومات الشخصية لمنتسبي هذه المؤسسات على العكس من ذلك في المؤسسات المالية والاقتصادية فإن الاختراق أو الحصول على الأرقام السرية للدخول يكبد خسائر مالية جد معتبرة.

مكونات أمن المعلومات: [1]

1. سرية المعلومات : شخصية، موقف مالي، معلومات استخباراتية.
2. سلامة المعلومات : من التحريف أو التزييف سواء كان بقصد أو بغير قصد.

[1] خالد الغثبر، محمد بن عبدالله القحطاني،**أمن المعلومات بلغة ميسرة**،الرياض:مركز التميز لأمن المعلومات،2007.ص35.

3. ضمان الوصول إلى المعلومات: لمن لهم الحق في ذلك. [1]

أسباب الجريمة الإلكترونية:

- وجود دافع قوي :المال، الانتقام، التنافس، دافع سياسي، إثبات قدرات فنية.
- وجود أسلوب معين لتنفيذ الجريمة :بوجود خطة واضحة المعالم للقيام بذلك.
- وجود ثغرة : نقطة ضعف ما في النظام المعلوماتي.

وفيما يلي سوف نتطرق إلى العناصر التي من الممكن أن نراها أساسية في حماية ووقاية المكتبات ومراكز المعلومات من الجرائم الإلكترونية، لكن قبل ذلك لابد من أن نتعرف على الجرائم الإلكترونية التي يمكن أن تحدث على مستوى هذه المؤسسات .

1. أمن وحماية الولوج أو الدخول إلى الأنظمة:

كلمات المرور: كلمة المرور تعني للنظام أنك الشخص المرخص له بالدخول فعلا وتعمل على حماية البيانات .

الأخطار التي تهدد كلمات المرور:

- الاختراق أو التصديع
- استخدام الهندسة الاجتماعية
- البحث والتصنت التقليدي والحديث

الاختيار الأمثل لكلمة المرور: لتفادي اختراق أو تصدع كلمة المرور يجب أن تكون قوية وأن لا تكون صيدا سهلا لبرامج التصديع وذلك وفق الخطوات التالية:

- أن لا تتكون كلمة المرور من كلمة واحدة.

---

[1] حسنين، رجب عبد الحميد،**أمن شبكات المعلومات الإلكترونية: المخاطر والحلول**-.**Cybrarians Journal** -.ع 30 (ديسمبر 2012) .- تاريخ الاطلاع 2013/10/10> البحث -. <متاح في > http://journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=9

[2] حسنين، رجب عبد الحميد،**أمن شبكات المعلومات الإلكترونية: المخاطر والحلول**،مرجع سابق

- لا تتضمن كلمة المرور معلومات شخصية.
- أن لا يقل عدد الخانات عن 10 أرقام أو حروف.
- المزج بين الحروف والأرقام.
- استخدام اختصار جملة أو عبارة ما .
- تجنب تضمين اسم المستخدم داخل كلمة المرور. [1]

التعامل الصحيح مع كلمة المرور: لتفادي الطرق التي يتحصل بها أصحاب الجرائم الإلكترونية على كلمة المرور يجب احترام ما يلي:

- لا تخبر أحداً بكلمة مرورك.
- لا تكتب كلمة المرور على أوراق خارجية.
- لا تحفظ كلمة المرور في جهازك بدون تشفير.
- كلمة مرورك مسئوليتك .. لذلك أنت المسؤول عن سوء استخدامها.
- لا تستخدم خاصية ﴿الدخول التلقائي﴾ خصوصاً إذا كنت تستخدم جهازاً عاماً.
- استخدم مجموعة من الحروف و الأعداد و الرموز التي يمكن كتابتها بسرعة.
- لا تستخدم كلمات مرورٍ يَصعُب تذكرها.
- إذا كنت تمتلك حسابات مختلفة فمن الحكمة تخصيص كلمة مرور لكل منها طالما انك تستطيع تذكُرها.
- لا ترسل كلمة المرور عبر البريد الإلكتروني أو غرف المحادثة.
- احذر من استخدام الأجهزة العامة (مثل مقاهي الإنترنت) في الدخول على حساباتك الشخصية.
- تغيير كلمة المرور بشكل دوري

[1] خالد الغثبر، محمد بن عبدالله القحطاني،**أمن المعلومات بلغة ميسرة**،،مرجع سابق،ص45.

كلمة المرور أحد مكونات منظومة حماية المعلومات فهي تساعد على التحقق من هوية المستخدم، وفاعليتها تعتمد على درجة انضباط العنصر البشري في اختيار كلمة المرور والتعامل معها وفق الأساليب الصحيحة.

2.**أمن وحماية البرامج والتطبيقات:**

الفيروسات :

ما هي إلا أحد أنواع البرامج الخبيثة التي تعمل على تخريب أو إفساد عمل برنامج ما أو نظام تشغيل ما أو انتحال صفة معينة داخل الجهاز وفي مجمل الأحيان لها تأثير سلبي غير معلوم بالنسبة للمستخدم ومن أمثلة البرامج الخبيثة كذلك نجد: الديدان، البرامج التجسسية، البرامج الإعلانية الأحصنة الطروادية.....الخ

طرق الإصابة بها : تتعرض الأنظمة المعلوماتية في أي لحظة ما للإصابة بأحد البرامج الخبيثة كالفيروسات وذلك عبر الطرق الآتية :

-عن طريق وسائط التخزين

-عن طريق البريد الإلكتروني:وفق عدة أشكال منها:

- عن طريق المرفقات

- عن طريق مجرد قراءة الرسالة البريدية

- عن طريق رابط في الرسالة.

-تصفح مواقع مشبوهة.

-المراسل الآني MSN

-عن طريق المنافذ المفتوحة

-تحميل برامج من الإنترنت

طرق الوقاية :لاعتماد منهج الوقاية والسلامة من الفيروسات وأشباهها في المكتبات ومراكز المعلومات يجب اتخاذ التدابير الآتية :

- لا تقم بفتح أي ملف مرفق مع رسالة من شخص مجهول.
- لا تقم بفتح ملف مرفق مع رسالة من شخص معلوم إلا إذا كنت تتوقع ذلك الملف.
- لا تقم بفتح وقراءة رسالة من أشخاص مجهولين تحمل عنوانا غريبا.

-قم بتعطيل ميزة تحميل الملفات المرفقة مع الرسالة الإلكترونية.

-من الأفضل عدم استعراض الرسائل المعدة بواسطة لغة HTML

-لا تقم بتحميل أي ملف غريب عن طريق البريد الإلكتروني أو المراسل الآني .

-افحص أي ملف تريد تحميله وتأكد من خلوه من أي شبهة كانت.

-استخدام برنامج مكافحة الفيروسات وتحديثه بشكل دوري .

-القيام بعمل نسخة احتياطية للملفات بشكل دوري في وحدة تخزين خارجية .

-عدم استخدام برامج مشاركة الملفات .

-تحديث جميع برامج الجهاز بشكل دوري لتفادي الثغرات التي يمكن أن تكتشف بها.

وتجدر الإشارة إلى أن كل هذه الإجراءات الأمنية الوقائية تدخل ضمن سياق الإجراءات الاحترازية أي قبل وقوع أي أزمة أو جريمة إلكترونية، أما في حالة وقوع الأزمة فالضرورة تستدعي احتضار شيء أساسي وهو موضوع التأمين على الخطر في مجال المعلوماتية .

المخاطر المعلوماتية:

منذ بضع سنوات ومستخدموا المعلوماتية، وحديثا مسئولو الشركات يولون اهتماما متزايدا بالمخاطر المعلوماتية، ويأملون في أن يساهم التأمين في تقديم لهذه

المخاطر، فالمعلوماتية لها تأثير كبيرا على الشركات والمؤسسات ومن بينها المؤسسات الوثائقية، وإذا بحثنا عن الأسباب في ظهور المخاطر المعلوماتية نجد أنها ترجع إلى عدة أشياء منها :

1. ازدياد آلية الأنظمة واندماجها فيما بينها .
2. الأنظمة أصبحت أكثر تعقيدا من حيث الجوهر.
3. التطور السريع للأنظمة المعلوماتية.
4. عزوف بعض الموظفين عن الاندماج مع هذه الأنظمة
5. لا زالت الأنظمة المعلوماتية مكلفة في السوق وحساسة من حيث التهديدات.
6. عدائية الموظفين أنفسهم للأنظمة المعلوماتية.

إذا كانت هذه بعض الأسباب في ظهور المخاطر المعلوماتية، فإنه من جانب آخر هناك العديد من الحالات تلعب المعلوماتية فيها دورا في تضخيم الضرر، هذا لأن النظام المعلوماتي يختلف عن النظام غير المعلوماتي من حيث الهيكل والتنظيم والإجراءات الاحتياطية وإجراءات الحماية، وعقلية الأفراد التي تختلف تبعا لكل نظام .

بمعنى آخر أن المؤسسة التي تأخذ في اعتبارها تولي الخطر وتأمل في حماية نفسها منه تكون بحاجة إلى تحليل الأخطار المعلوماتية وفقا لمعايير غالبا ما تكون هيكلية خاصة بها، مع الأخذ في الاعتبار نوعية الأخطار المعلوماتية، مع تحليلها بطريقة مترابطة، وحتى إذا كانت هذه المخاطر مضمونة في عقود، فلا تكون هذه العقود بالضرورة عقودا معلوماتية. [1]

[1] رسلان،نبيلة إسماعيل، **التأمين في مجال المعلوماتية والشبكات**،القاهرة:دار الجامعة الجديدة،2007، ص15-16.

عقد التأمين من الأخطار المعلوماتية:

عقد التأمين ضد أخطار المعلوماتية لا يختلف عن غيره من عقود التأمين، إلا أنه متميز قليلا، فبالإضافة للجوانب ذي الطبيعة القانونية (تكوين العقد، الإثبات، التزامات الأطراف)، هناك بعض الجوانب ذي الطبيعة الفنية والبعض الآخر نجده يتعلق بالأمن.

تعريف عقد التأمين:

يعرف عقد التأمين بأنه " العقد الذي بمقتضاه يقوم شخص اعتباري المؤمن بالالتزام في مقابل الحصول على مبلغ من المال هو قسط التأمين، بدفع تعويض محدد سواء للشخص المؤمن عليه والذي قام بتوقيع العقد أو البوليصة، أو لأشخاص آخرين محددين في هذه البوليصة وذلك عند حادث غير معين وفي المستقبل يوصف على أنه خطر"[1]

وعليه فإن التأمين في مجال المعلوماتية وبالضبط في مجال المكتبات ومراكز المعلومات هو تأمين هذا النظام كاملا ككل أو تامين جزء معين منه، ومع أننا بصدد دراسة المخاطر المعلوماتية فإن التأمين سوف يقع فقط على كل ما يتعلق بالحواسيب وأجهزة الإعلام الآلي، سواء في شقها المادي أو على مستوى البرمجيات، وبما أن إجراءات التأمين في هذه الحالة تتم بشكل عادي ككل إجراءات التأمين الأخرى العادية في حياتنا اليومية، ومع أي شركة من شركات التأمين التي توفر هذه الفئة من عقود التأمين، وعلى سبيل المثال لا الحصر فإن المجالات التي يمكن أن تخضع للتأمين في المكتبات ومراكز المعلومات هي:

* تأمين الأرصدة الوثائقية لما هناك من أخطر وكوارث طبيعية وبشرية تهددها.

[1] رسلان،نبيلةإسماعيل،نفس المرجع السابق،ص19.

* تأمين المباني ومحلات الحفظ.

* تأمين الأجهزة والمعدات والبرامج المعلوماتية

*تأمين الأشخاص من عمال وموظفين

وقد يكون هذا التأمين من جميع المخاطر جملة واحدة أو يخص البعض منها حسب عقد التأمين المنجز بين المؤمن والمؤمن له.

الخاتمة :

في حقيقة الأمر موضوع إدارة المخاطر في أنظمة المعلومات موضوع متشعب جدا، فعند اختيارنا لموضوع الوقاية من الجرائم الإلكترونية، أي من المخاطر المتعلقة من بالمعلوماتية والتي لا يزال المتخصصون يبحثون عن السبل القانونية لحماية هذه الأنظمة وكذا مجالات تأمينها، وما هي الإجراءات والتدابير القانونية في الجزائر التي لازالت بعيدة عن مستوى التطلعات، لأن مؤسسات التأمين الحالية والمتواجدة في الجزائر لازالت لم تضطلع بمثل هذا النوع من التأمين فيبقى الحل الإجرائي الوحيد، هو الوقاية وهو أفضل تأمين لأن الوقاية تجنب وقوع الضرر أو الخطر، وبالتالي فعلى كل المسئولين في المكتبات ومراكز المعلومات تبني الإجراء الوقائي كأفضل إجراء من الإجراءات ما بعد وقع الخطر أو الأزمة.

الهوامش

1.نور الدين ،عصام،إدارة المعرفة والتكنولوجيا الحديثة ،دار أسامة للنشر والتوزيع :الأردن،2009.

2.أبو بكر عيد أحمد، وليد اسماعيل السيفو ، إدارة المخاطر والتأمين ،دار اليازوري العلمية للنشر والتوزيع ،عمان 2009.

3.صلاح عباس،إدارة الأزمات في المنشآت التجارية ،القاهرة: مؤسسة شباب الجامعة،2007.

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

5.خالد الغثبر، محمد بن عبدالله القحطاني،أمن المعلومات بلغة ميسرة،الرياض:مركز التميز لأمن المعلومات،2007.

6.حسنين، رجب عبد الحميد،أمن شبكات المعلومات الإلكترونية: المخاطر والحلول -.Cybrarians Journal -.ع 30 (ديسمبر 2012) .- تاريخ الاطلاع 2013/10/10> البحث -. <متاح في

<http://journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=9>

7.أحمد ماهر ، إدارة الأزمات،القاهرة: الدار الجامعية،2006.

8. Institute De L'Audit interne ,Pricewaterhoudecoopers,Landwell&Associes .le management des risques de l'entreprise :cadre de reference- techniques d'application .germain :editions d'organisation ,2006.

9. Alain desroches ,alainleroy ,Frédérique vallée .La gestion de risques :principes et pratiques.Paris :Lavoisier ,2003.

FrédéricMorlaye,Risk Management et assurance, Paris :Economica,2006.