9-المحاضرة التاسعة- مخاطر النظم الآلية وإدارة المكتبات الرقمية

1-مفهوم النظم الآلية وإدارة المكتبات الرقمية:

النظم الآلية لإدارة المكتبات هي البرمجيات والأنظمة التي تدير عمليات المكتبات بشكل رقمي، تشمل:

- نظم إدارة المكتبات المتكاملة (ILS) مثلKoha ، Alma، وEvergreen، التي تدير الفهرسة، الإعارة، الإرجاع، والخدمات الرقمية.
- المستودعات الرقمية التي تحفظ وتنظم الوثائق الرقمية والأرشيفات الإلكترونيةDSpace) ، EPrints).
- البنى التحتية التكنولوجية والسحابة التي تستضيف قواعد البيانات وواجهات المستخدم.

إدارة المكتبات الرقمية تعتمد بشكل كامل على هذه النظم لتقديم خدمات فعالة وسريعة وموثوقة للمستفيدين، مما يجعل المخاطر التكنولوجية تهديداً استراتيجياً يجب التعامل معه بمنهجية صارمة.

2-تصنيف المخاطر التكنولوجية المتعمق:

1-المخاطر الفنية والتشغيلية:

- تعطل النظام :(System Downtime) قد يحدث بسبب أعطال تقنية في الخوادم، انقطاع التيار الكهربائي، أو مشاكل في الشبكة. هذا يوقف الخدمات ويسبب توقف العمل.

- أخطاء البرمجيات :(Software Bugs) تحديثات غير ناجحة، تعارض في الإصدارات، أو عيوب في تصميم النظام تسبب فساد البيانات أو تعطل بعض الوظائف.
- فقدان البيانات :نتيجة حذف بالخطأ، فشل النسخ الاحتياطي، أو تلف وسائط التخزين. وهو من أخطر المخاطر لما له من تأثير دائم قد يعطل البحث ويكلف موارد ضخمة.

2- المخاطر الأمنية السيبرانية:

- الهجمات الخبيثة :مثل هجمات الفدية (Ransomware) التي تشفر البيانات وتطلب فدية لفك التشفير، وهجمات رفض الخدمة الموزعة (DDoS) التي تستهدف شل النظام، واختراق قواعد البيانات للسرقة أو التخريب.
- سرقة البيانات وتسريب الخصوصية :خاصة البيانات الشخصية للمستفيدين، وثائق البحث غير المنشورة، وسجلات الاستخدام التي قد تُسبب أضراراً قانونية وسمعة للمؤسسة.
- الهجمات الداخلية :موظفون أو متعاونون يستخدمون صلاحياتهم بشكل خاطئ، سواء عن قصد أو بسبب نقص التوعية.

3- مخاطر الحفظ الرقمي طويلة الأمد:

- تقادم الصيغ الرقمية وعدم توافق الأنظمة :مع مرور الزمن، قد تصبح صيغ الملفات قديمة وغير مدعومة، مما يشكل خطر فقدان المحتوى أو تدهوره.

- اعتماد مزود خدمة وحيد :الاعتماد على جهة واحدة في الاستضافة أو الخدمات السحابية يزيد من خطر الانقطاع أو تعطل الخدمة.
- غياب استراتيجية لحفظ واسترجاع البيانات :دون وجود خطة واضحة للحفظ الرقمي والاسترجاع، تتحول المخاطر الفنية إلى خسائر نهائية.

4- مخاطر مالية وتنظيمية:

- تكاليف الأعطال والإصلاح :الأعطال التقنية قد تكلف مكتبات رقمية مبالغ ضخمة لإصلاحها أو لاستعادة البيانات.
- تغييرات في الموردين والسياسات :تقلبات السوق أو سياسات شركات البرمجيات تؤثر على استمرارية الخدمات الرقمية.

3-منهجية إدارة المخاطر في النظم الآلية (وفق ISO 31000 مع شرح تفصيلي):

أ. تحديد السياقContext Establishment :

فهم متطلبات البيئة الرقمية للمكتبة، الموارد التقنية، الموظفين، والمستفيدين. يشتمل على:

- تحديد الأصول الرقمية الحيوية (المجموعات الرقمية، قواعد البيانات، الأنظمة).
- فهم التنظيم التشريعي والقانوني (حماية البيانات، حقوق النشر).
- تقييم البنية التحتية التقنية (الأجهزة، الشبكة، السحابة).

ب. تحديد المخاطر Risk Identification :

- استخدام تقنيات وأدوات متعددة مثل العصف الذهني، مراجعة الحوادث السابقة، وفحص نقاط الضعف في النظام.(Vulnerability Assessment)
- الاستعانة ببرمجيات الكشف المبكر عن التهديدات والأخطار الأمنية.(IDS/IPS)
- إعداد قوائم تفصيلية لمخاطر تتراوح بين الفشل الفني، الهجمات الإلكترونية، فقدان البيانات، أو الأعطال التشغيلية.

ج. تحليل المخاطر Risk Analysis :

- تقييم الاحتمال: تحليل البيانات التاريخية، اختبارات تحمل النظام، ومستويات الأمان.
- تقييم التأثير: مدى الضرر على البيانات، الخدمات، سمعة المكتبة، والتكاليف المالية.
- بناء مصفوفات احتمالية/أثر مع درجات تفصيلية (مثلاً: من 1 إلى 5 لكل محور).
- استخدام مقاييس كمية عند الإمكان (مثل معدلات انقطاعات الشبكة، أوقات استرجاع النظام).

د. تقييم المخاطر Risk Evaluation :

- مقارنة النتائج مع معايير قبول المخاطر المؤسسية.
- تصنيف المخاطر إلى: حرجة، عالية، متوسطة، منخفضة.
- تركيز الموارد على المخاطر التي تتطلب معالجة عاجلة، مع توثيق أسباب قبول المخاطر المتبقية.

هـ. معالجة المخاطر Risk Treatment :

- التخفيف :تحسين صيانة الأجهزة، تحديث البرمجيات بانتظام، تنفيذ سياسات أمنيّة صارمة، تصميم خطط نسخ احتياطية متعددة وتكرارية، اعتماد بروتوكولات تشفير متقدمة.
- النقل :التأمين على الخسائر السيبرانية، التعاقد مع مزودي خدمات آمنة، والاستعانة بمزودي سحاب متعددين لضمان استمرارية الخدمة.
- التجنب :إيقاف الخدمات أو التطبيقات ذات المخاطر غير المقبولة بدون حلول فنية مناسبة.
- القبول :توثيق المخاطر المقبولة مع إجراءات مراقبة مستمرة وتقييم دوري.

و. المتابعة والمراجعة Monitoring and Review :

- وضع مؤشرات أداء لمراقبة سلامة النظام والتقارير الأمنية.
- تحديث سجل المخاطر وفق التغيرات التقنية أو البيئية.
- مراجعة وتحديث خطط الاستجابة للطوارئ بناء على دروس مستفادة وحوادث فعلية.

ز. التواصل والتدريب Communication and Consultation :

- بناء ثقافة أمنيّة داخل المكتبة الرقمية عبر ورش تدريب ورفع وعي الموظفين.
- تحديث المستفيدين حول سياسات الخصوصية والمخاطر المحتملة.
- التنسيق مع فرق تقنية المعلومات، فرق الأمن السيبراني، ومزودي الخدمات الرقمية خارج المؤسسة.

4-تقنيات وأدوات مساعدة لإدارة المخاطر في النظم الآلية:

- أنظمة النسخ الاحتياطيRsync :، Bacula، Veeamلضمان تكرار البيانات وتوزيعها في مواقع متعددة.
- أدوات أمنية: جدران نارية(pfSense) ، أنظمة كشف التسلل(Snort) IDS ، حلول مكافحة الفيروسات المتقدمة، وأنظمة مراقبة السجلات.(SolarWinds) SIEM
- أدوات فحص الثغراتNessus :، OpenVASلاكتشاف نقاط الضعف بشكل دوري.
- أدوات إدارة الحوادث Incident Response Platforms :مثلTheHive ، مع رصد وتنبيه تلقائي للحوادث الأمنية.

5-الخطط والتدريب العملي:

- إعداد خطة مشابهة لخطة استمرارية الأعمال (Business Continuity Plan) تغطي سيناريوهات عدة تخيلتها المؤسسة للمخاطر التقنية.
- إجراء تمارين محاكاة دورية (مثل اختراق وهمي، حادثة فقدان بيانات) مع تقييم أداء فريق تقنية المعلومات والإدارة.
- تقييم الأداء والقدرة على سرعة الاستجابة والاسترجاع في ضوء مؤشرات KPIs محددة.

مخاطر النظم الآلية وإدارة المكتبات الرقمية تشكل تحدياً متصاعداً مع توسع رقمنة الخدمات. الاعتماد على إطار إدارة المخاطر القائم على منهجية ISO 31000 يسمح بتحليل دقيق وتنظيم استجابات

فعالة مستندة إلى فهم عميق للمخاطر التقنية، مما يضمن استمرارية خدمات المكتبة الرقمية وحماية بياناتها ومجموعاتها القيمة.