مخاطر نظم المعلومات المحوسبة

د. أحمودة وفاء

أصبحت نظم المعلومات المحوسبة جزءا لا يتجزأ من المؤسسات الحديثة، ولكنها ترتبط بالعديد من المخاطر التي قد تهدد سرية البيانات وسلامتها وتوافرها. يمكن أن تكون لهذه المخاطر عواقب وخيمة، بما في ذلك الخسائر المالية والأضرار التي تلحق بالسمعة وتعطيل العمليات.

أنواع مخاطر نظم المعلومات المحوسبة

- **المخاطر المتعلقة بالموظفين**

تشمل بعض المخاطر الرئيسية المتعلقة بالموظفين ما يلي:

1. أخطاء إدخال البيانات المتعمدة
2. الوصول غير المصرح به إلى مخرجات النظام
3. مشاركة كلمات المرور
4. إساءة استخدام موارد الحاسوب لأغراض شخصية

- غالبا ما تنشأ هذه المخاطر من نقص التدريب المناسب، أو عدم كفاية الوعي الأمني، أو في بعض الأحيان متعمدة.

أنواع مخاطر نظم المعلومات المحوسبة

- **المخاطر التكنولوجية**

المخاطر التكنولوجية متأصلة في الأنظمة نفسها وتشمل:

1. الإصابة بالفيروسات
2. الوصول غير المصرح به إلى النظام
3. تلف البيانات أو فقدانها
4. فشل النظام

أنواع مخاطر نظم المعلومات المحوسبة

- **مخاطر الرقابة الداخلية**

يمكن أن تؤدي نقاط الضعف في أنظمة الرقابة الداخلية إلى:

1. العرض غير المصرح به للمخرجات
2. التعامل غير السليم مع الوثائق
3. سرقة البيانات أو التلاعب بها

الاتجاهات الناشئة في مخاطر نظم المعلومات المحوسبة

مع تطور التكنولوجيا، تطورت أيضا المخاطر المرتبطة بها. تشمل بعض مجالات الاهتمام الناشئة ما يلي:

1. الحوسبة السحابية: مع انتقال المزيد من المؤسسات إلى السحابة، تظهر تحديات أمنية جديدة.
2. الذكاء الاصطناعي والتعلم الآلي: تقدم هذه التقنيات نقاط ضعف جديدة، خاصة فيما يتعلق بتحيز البيانات والاعتبارات الأخلاقية.
3. إنترنت الأشياء (:(IOTيوسع انتشار الأجهزة المترابطة سطح الهجوم للاختراقات المحتملة.
4. تقنية البلوكتشين: بينما توفر تقنية البلوكتشين أمانًا معززًا في بعض الجوانب، إلا أنها تقدم أيضًا أنواعًا جديدة من المخاطر التي يجب فهمها وإدارتها.

إدارة مخاطر نظم المعلومات المحوسبة

تعد الإدارة الفعالة للمخاطر جد مهمة للمؤسسات لحماية أصول المعلومات الخاصة بها. تتضمن العملية عادة:

1. تحديد المخاطر: التعرف على التهديدات ونقاط الضعف المحتملة.
2. تحليل المخاطر: تقييم احتمالية والتأثير المحتمل للمخاطر المحددة.
3. تقييم المخاطر: ترتيب أولويات المخاطر بناءً على شدتها وقابلية المؤسسة لتحمل المخاطر.
4. معالجة المخاطر: تنفيذ ضوابط للتخفيف من المخاطر أو نقلها أو قبولها.

استراتيجيات معالجة المخاطر

لمعالجة المخاطر المرتبطة بنظم المعلومات المحوسبة، يمكن للمؤسسات تنفيذ عدة استراتيجيات:

1. التدريب المنتظم للموظفين: تثقيف الموظفين حول أفضل ممارسات الأمان وأهمية حماية البيانات.
2. ضوابط وصول قوية: تنفيذ آليات مصادقة قوية ومبدأ الامتياز الأدنى.
3. المراقبة المستمرة: استخدام أنظمة متقدمة للكشف عن التهديدات لتحديد الحوادث الأمنية والاستجابة لها بسرعة.
4. تشفير البيانات: حماية المعلومات الحساسة أثناء التخزين والنقل.
5. التحديثات المنتظمة للنظام: الحفاظ على تحديث جميع البرامج والأنظمة لمعالجة نقاط الضعف المعروفة.
6. تخطيط الاستجابة للحوادث: تطوير واختبار خطط الاستجابة للحوادث بانتظام لضمان اتخاذ إجراءات سريعة وفعالة في حالة حدوث خرق أمني

دور الامتثال والمعايير لإدارة مخاطر نظم المعلومات المحوسبة

تشمل بعض الأطر المهمة في إدارة مخاطر نظم المعلومات المحوسبة ما يلي:

1. ISO/IEC 27001: يوفر مسارا منهجيا لإدارة معلومات الشركة الحساسة.
2. إطار عمل الأمن السيبراني NIST: يقدم إرشادات لتحسين الموقف الأمني السيبراني.
3. COBIT: يركز على حوكمة وإدارة تكنولوجيا المعلومات.

- يجب على المؤسسات اختيار الإطار الذي يناسب احتياجاتها ومتطلبات نشاطها بشكل أفضل.

المراجع

1. BOHEISI, & SHAREF. (2008). [NO TITLE PROVIDED IN THE SEARCH RESULTS]
2. ABO-MOUSA. (2006). EXAMINING THE THREATS REGARDING THE COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS IN THE DEVELOPING COUNTRIES: A FIELD STUDY ON THE SAUDI ORGANIZATIONS.
3. CEBULA, J. L., POPECK, M. E., & YOUNG, L. R. (2014). A TAXONOMY OF OPERATIONAL CYBER SECURITY RISKS VERSION 2. CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE.
4. AGRAFIOTIS, I., NURSE, J. R., GOLDSMITH, M., CREESE, S., & UPTON, D. (2018). A TAXONOMY OF CYBER-HARMS: DEFINING THE IMPACTS OF CYBER-ATTACKS AND UNDERSTANDING HOW THEY PROPAGATE. JOURNAL OF CYBERSECURITY,
5. ALLIANZ. (2021). ALLIANZ RISK BAROMETER 2021
6. .WORLD ECONOMIC FORUM. (2020). THE GLOBAL RISKS REPORT 2020.
7. LOUKAS, G., GAN, D., & VUONG, T. (2013). A REVIEW OF CYBER THREATS AND DEFENSE APPROACHES IN EMERGENCY MANAGEMENT. FUTURE INTERNET, 5(2), 205-236.
8. ULVEN, J. B., & WANGEN, G. (2021). A SYSTEMATIC REVIEW OF CYBERSECURITY RISKS IN HIGHER EDUCATION. FUTURE INTERNET, 13(2), 39.
9. LEE, I., & LEE, K. (2020). THE INTERNET OF THINGS (IOT): APPLICATIONS, INVESTMENTS, AND CHALLENGES FOR ENTERPRISES. BUSINESS HORIZONS, 58(4), 431-440
10. .ILHAN FIRAT, A., FIRAT, S., ABDULHAMIT KAYA, M., & ALTUN, H. (2021). A REVIEW OF CYBERSECURITY DATASETS FOR MACHINE LEARNING ALGORITHMS. IN 2021 INTERNATIONAL CONGRESS OF HUMAN-COMPUTER INTERACTION, OPTIMIZATION AND ROBOTIC APPLICATIONS (HORA) (PP. 1-6). IEEE.
11. KHRAISAT, A., GONDAL, I., VAMPLEW, P., & KAMRUZZAMAN, J. (2019). SURVEY OF INTRUSION DETECTION SYSTEMS: TECHNIQUES, DATASETS AND CHALLENGES. CYBERSECURITY, 2(1), 1-22.