أمن نظم المعلومات المحوسبة

د. أحمودة وفاء

التحديات الرئيسية في أمن نظم المعلومات المحوسبة

- **اكتشاف التهديدات والتحكم في الوصول**

أحد التحديات الرئيسية في أمن نظم المعلومات هو الكشف الفعال عن التهديدات وتنفيذ تدابير قوية للتحكم في الوصول. سلطت الأبحاث الحديثة الضوء على أهمية تطوير آليات متقدمة للكشف عن التهديدات وأنظمة التحكم في الوصول لحماية البيانات الحساسة ومنع الوصول غير المصرح به.

التحديات الرئيسية في أمن نظم المعلومات المحوسبة

- **تقنيات الحفاظ على الخصوصية**

مع تزايد المخاوف بشأن خصوصية البيانات، هناك تركيز متزايد على تطوير وتنفيذ تقنيات تحافظ على الخصوصية. تهدف هذه التقنيات إلى حماية خصوصية المستخدم مع السماح في الوقت نفسه بمعالجة البيانات وتحليلها بالشكل الضروري.

.

التحديات الرئيسية في أمن نظم المعلومات المحوسبة

- **أمن الذكاء الاصطناعي**
- مع الاعتماد الواسع على أنظمة الذكاء الاصطناعي، أصبح ضمان أمنها مجالا حيويا للتركيز. يجري البحث حاليا في مجال أمن الذكاء الاصطناعي لنظم المعلومات، مع التطرق إلى قضايا مثل الهجمات الخصومية والدفاعات في نظم المعلومات القائمة على التعلم العميق.

تقنيات تعزيز أمن نظم المعلومات المحوسبة

- التوعية والتدريب الأمني
- أكدت الدراسات على أهمية تنفيذ برامج التوعية والتدريب الأمني للتخفيف من التهديدات الداخلية. إن تطوير ثقافة تنظيمية تعزز الوعي بأمن البيانات أمر بالغ الأهمية للتنفيذ الفعال للأمن.السياسات والإجراءات التنظيمية
- تعد السياسات والإجراءات الأمنية التنظيمية المتسقة ضرورية للحفاظ على بيئة معلومات آمنة. أظهرت الأبحاث أن المبادئ التوجيهية والبروتوكولات الواضحة يمكن أن تحسن بشكل كبير الوضع الأمني للمؤسسة.تبني التقنيات الجديدة
- يجب أن تلتزم المؤسسات بتبني التقنيات الجديدة والعمليات المبتكرة للبقاء في المقدمة أمام التهديدات الأمنية المتطورة. يشمل ذلك مواكبة أحدث التطورات في تقنيات ومنهجيات الأمن.

تقنيات تعزيز أمن نظم المعلومات المحوسبة

- **التشفير والاتصالات الآمنة**CRYPTOGRAPHY AND SECURE COMMUNICATION

لا تزال التطورات في مجال التشفير تلعب دورا هاما في تأمين نظم المعلومات. ركزت الدراسات الحديثة على تطوير تقنيات تشفير جديدة وبروتوكولات اتصال آمنة لحماية البيانات أثناء النقل والتخزين.

- **تحليل الوعي بالموقف** SITUATION AWARENESS ANALYSIS

تحسين الوعي بالموقف في نظم المعلومات هو مجال آخر للبحث النشط. يتضمن ذلك تطوير تقنيات لفهم التهديدات الأمنية المحتملة والاستجابة لها في الوقت الفعلي بشكل أفضل.

- **التحقيق الجنائي الرقمي** DIGITAL FORENSICS

مع تزايد تعقيد الهجمات الإلكترونية، اكتسب مجال التحقيق الجنائي الرقمي أهمية كبيرة. ركزت الأبحاث الحديثة على تطوير تقنيات متقدمة للتحقيق في الحوادث الأمنية وتحليلها.

المراجع

- ADAMS, A., & SASSE, M. A. (1999). USERS ARE NOT THE ENEMY. COMMUNICATIONS OF THE ACM, 42(12), 40-46.
- ALOTAIBI, M., FURNELL, S., & CLARKE, N. (2016). INFORMATION SECURITY POLICIES: A REVIEW OF CHALLENGES AND INFLUENCING FACTORS. IN 2016 11TH INTERNATIONAL CONFERENCE FOR INTERNET TECHNOLOGY AND SECURED TRANSACTIONS (ICITST) (PP. 352-358). IEEE
- BASKERVILLE, R., & SIPONEN, M. (2002). AN INFORMATION SECURITY META-POLICY FOR EMERGENT ORGANIZATIONS. LOGISTICS INFORMATION MANAGEMENT, 15(5/6), 337-346.
- D'ARCY, J., & HERATH, T. (2011). A REVIEW AND ANALYSIS OF DETERRENCE THEORY IN THE IS SECURITY LITERATURE: MAKING SENSE OF THE DISPARATE FINDINGS. EUROPEAN JOURNAL OF INFORMATION SYSTEMS, 20(6), 643-658.
- ENISA. (2014). ENISA THREAT LANDSCAPE 2014: OVERVIEW OF CURRENT AND EMERGING CYBER-THREATS. EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY.ERNST & YOUNG. (2008). GLOBAL INFORMATION SECURITY SURVEY 2008. ERNST & YOUNG.
- ERNST & YOUNG. (2010). BORDERLESS SECURITY: ERNST & YOUNG'S 2010 GLOBAL INFORMATION SECURITY SURVEY. ERNST & YOUNG.
- FLOWERDAY, S. V., & TUYIKEZE, T. (2016). INFORMATION SECURITY POLICY DEVELOPMENT AND IMPLEMENTATION: THE WHAT, HOW AND WHO. COMPUTERS & SECURITY, 61, 169-183.