العوامل التي تؤثر على تبني ممارسات أمنة اثناء تطوير البرنامج

اعداد الطالبة: فاطمة عبدالله صالح الغامدي

اشراف: د.نرمين حمزة

المستخلص

تقترح هذه الدراسة إطار عمل لتعزيز مبادئ الأمان والمعايير والمقاييس والممارسات الامنة اثناء تطوير البرمجيات للمشاريع المخصصة في شركات التطوير الصغيرة والمتوسطة الداخلية.

تلعب المؤسسات الصغيرة والمتوسطة (SME) دورًا رئيسيًا في العديد من الصناعات وفي الاقتصادات الوطنية. ومع ذلك ، يمكن أن تكون الشركات المستقلة هي الشركات الأكثر انتشارًا والأكثر نفوذاً في العديد من المجالات الصناعية والاقتصادية. يتمثل التحدي الذي يواجه هذه الأنواع من الشركات في تقديم منتج عالي الجودة في فترة زمنية قصيرة وضمن ميزانيات صغيرة. لذلك ، لا تكون هذه المنتجات في العادة خالية من مشكلات الأمان الناتجة عن الفشل في إجراء اختبارات الأمان خلال دورة حياتها وبعد نشرها بسبب ضيق الوقت والموارد. أيضا ، هناك مطالب كبيرة من العملاء على شركات تطوير البرمجيات لضمان أمن البرمجيات في أنظمتها. بعض المنظمات قد عالجت القضايا الأمنية وطورت العديد من المعايير والنماذج. ومع ذلك ، فإن هذه المعايير والنماذج ليست دائما ممكنة للشركات الصغيرة والمتوسطة الحجم.

استخدمت هذه الرسالة طرق البحث التجريبي (ERM) للتحقق من صحة إطار الاستراتيجية المقترحة. تم تكييف العديد من ممارسات الأمان لتكون مناسبة للبرامج المخصصة في الشركات الصغيرة والمتوسطة. ومع ذلك ، فإن قدرة الشركات على التكيف مع ممارسات الأمان أثناء تطوير البرمجيات تختلف وفقًا لخصائص الشركة ، مثل حجم الشركة والعمر والميدان والتاريخ السابق للشركة في اعتماد ممارسات الأمان. أحد التحديات الرئيسية التي تم تحديدها في هذا العمل هو نقص خبراء أمن البرمجيات. علاوة على ذلك ، كان عدد مطوري البرمجيات المدربين غير كافٍ.

Factors That Influence Adoption of Security Practices During Software Development

By Fatimah Abduallah Saleh Alghamdi

Supervised by: Dr. Nermin Hamza

ABSTRACT

Small and medium enterprises (SME) play a key role in many industries and in national economies. However, independent companies can be the most prevalent and most influential companies in many industries and economic settings. The challenge for these types of companies is to deliver a high-quality product in a short amount of time and within small budgets. Therefore, these products are not usually free of security problems resulting from a failure to perform security tests during its life cycle and after its deployment due to a lack of time and resources. Also, there are high demands from the customer on software development companies to ensure software security in their systems. Some organizations have addressed security issues and have developed many standards and models,. These include the security techniques in ISO/IEC 17799 (as an information security management standard), control objectives for information and related technology (COBIT), and the best practices promoted by the National Institute of Standards and Technology (NIST). However, these standards and models are not always feasible for small and medium-sized companies. This study proposes a framework to enhance the security principles, criteria, measurement, and practices for software development of custom-made projects at in-house SME development companies. This thesis used Empirical Research Methods (ERM) to validate the proposed strategy framework. Many security practices have been adapted to be suitable for custom-made software at SME. However, the companies' adaptability to security practices during software development varied according to company characteristics, such as company size, age, field, and previous history of the company in adopting security practices. One of the main challenges identified in this work was the shortage of software security experts. Moreover, the number of trained software developers was insufficient.