**هيكلة وتصميم البرمجيات الآمنة**

هيكلة البرمجيات وتصميمها هو المكان الذي يتم فيه ترجمة الأفكار وتحويلها إلى واقع ، حيث تصبح المتطلبات وماذا ولماذا هي من ومتى وأين وكيف ستكون البرمجيات. من منظور أمني ، يعتبر العديد من الخبراء الهندسة المعمارية والتصميم أهم مرحلة منفردة في دورة حياة تطوير البرمجيات .هناك عدة اهداف امنية متعلقة بهندسة وتصميم البرمجيات، أولها هو تمكين ميزات وامكانيات الأمان بشكل كامل، ومقاومة الهجوم أي يجب ان يحتوي البرنامج على الحد الأدنى من نقاط الضعف الأمنية التي يمكن استغلالها ، ثانيا التسامح مع الهجوم ، أي اثناء مقاومة الهجوم يجب ان لا تتأثر وظيفة البرنامج وقدرته بشكل كبير، وكذلك يجب ان يتم تقليل التأثيرات على البرنامج عند مواجهة هجوم تم بنجاح . نريد التفريق بين اهم المفردات المتعلقة بالبنية والأمان التي قد يتم الخلط بينهم ، حين نشير الى برامج الأمان، فنحن نقصد هنا جدران حماية التطبيقات، وحزم التشفير ، اما امان البرامج فهو ممارسة تجعل البرامج اكثر امانا. هندسة الامن هي هندسة مكونات الامن اما الهندسة الامنة فتطلق على الهندسة المرنة والمقاومة للهجوم. تحليل المخاطر المعمارية تعتبر ممارسة ذات أهمية قصوى لتكوين تصور عن المخاوف الأمنية في هندسة البرمجيات ومرحلة التصميم، يهدف الى توفير ضمان بأن الاهتمامات الأمنية على مستوى التصميم والهيكلة يتم تحديدها ومعالجتها في اسرع وقت ممكن في دورة حياة تطوير البرامج ، مما يؤدي الى تحسين مستويات مقاومة الهجوم والتسامح والمرونة مع الهجوم. يساعد كذلك تحليل المخاطر في تحديد الضوابط الأمنية المناسبة او المراجعات او الإجراءات لتقليل المخاطر او القضاء عليها. الخطوة الأولى المطلوبة في تحليل أي برنامج، بالنسبة للمخاطر هي تحقيق فهم كامل لماهية البرنامج وكيف يعمل ، وعادة ما يتضمن جمع المعلومات لهذا التوصيف للبرنامج مراجعة مجموعة واسعة من أدوات النظام واجراء مقابلات متعمقة مع أصحاب المصلحة الرئيسيين مثل مدراء الإنتاج او مدراء البرنامج، العديد من المخرجات يجب ان تراجعها في هذه الخطوة لتوصيف البرامج ، مثل المتطلبات الوظيفية وغير الوظيفية ومستندات حالات الاستخدام ومستندات حالات سوء الاستخدام، ووثائق التصميم التفصيلية مثل مخططاتUML التي توضح الجوانب السلوكية والهيكلية للنظام. ثاني مرحلة من تحليل المخاطر المعمارية هي تحليل التهديدات ، التهديدات هي عوامل تنتهك حماية أصول المعلومات وسياسة امان المواقع ، خلال هذا التحليل يتك استخدام التهديدات لفهم كيفية استغلال البرنامج . تتكون خطة التخفيف من الإجراءات من الإجراءات المضادة التي تعتبر فعالة ضد نقاط الضعف التي تستغلها هذه التهديدات. قد توجد مصادر تهديدات داخلية وخارجية ويجب ان يأخذ تصنيف الهجوم في الاعتبار الدافع والقدرة على كلا النوعين من التهديدات. يمكن تنفيذ الهجمات الداخلية من قبل أفراد مثل الموظفين الساخطين والمتعاقدين، الدوافع لذلك على سبيل المثال ؛ الفضول ، الأنانية، الذكاء ، الأخطاء غير المقصودة (على سبيل المثال ، أخطاء إدخال البيانات ، أخطاء البرمجة) أو نقص الإجراءات أو التدريب، إجراءات التهديد الداخلي: على سبيل المثال: الابتزاز وهو طلب مال أو منفعة أخرى مقابل عدم الكشف عن معلومات عنها. و إساءة استخدام الكمبيوتر مثل استخدام جهاز كمبيوتر بطريقة غير نزيهة مثل استخدام الكمبيوتر الشخصي للعمل.

الاسم: بيان مسفر عيظه النهدي عدد الكلمات476:كلمة

نسبة الاقتباس: 0%