نظم تكنولوجيا المعلومات إدارة حساب المستخدم وتسجيل الدخول

لمحة عامة

- نحن نعيش في عصر انترنت الأشياء (IoT) الذي يوفر التكامل السلس وسهولة الدخول بين الأشياء بغض النظر عن مكانها الفعلي. ينتشر انترنت الأشياء (IoT) بين نطاقات مختلفة مثل أنظمة الرعاية الصحية والخدمات الحكومية والبنوك والاتصالات على سبيل المثال لا الحصر. لم نعد عرضة فقط لهجمات الالكترونية بل عرضة لهجمات تهدد الحياة كالهجمات الإرهابية وهجمات التجسس وبالتالي أصبح هناك حاجة إلى توفير ضمانات الهوية الشخصية ومراقبة صارمة.
- تتناول هذه الدورة المبادئ الأساسية والإطار الهندسي لنظام الهوية التكنولوجي وإدارة الدخول كما يشمل ضمان الهوية والتصديق والتفويض والإذن والمساءلة وإمكانية مراجعة حسابات الدخول الموحدة (SSO) وهوية الاتحاد. كما تناقش هذه الدورة حالات عملية مثل جواز السفر الإلكتروني والخدمات المصرفية عبر الهاتف النقال وخدمات الحكومة الإلكترونية ونظم EMV وحالات مختارة أخرى .

المنهجية

- هذه الدورة على درجة عالية من التفاعلية وتتضمن مناقشات جماعية ودراسات الحالة والتمارين المصممة خصيصا، كما تتضمن أيضا تمارين عملية ولعب الأدوار.

أهداف الدورة

سيتمكن المشاركون في نهاية الدورة من:

- توضيح إطار إدارة الهوية والدخول ومناقشة المخاطر الأمنية المرتبطة بخيارات النشر المختلفة
- مناقشة آليات مختلفة لإقامة مصادقة قوية (مثل مكتب المدعي العام، والمصادقة القائمة على الشهادات، مصادقة OTP)
- شرح مبادئ البنية التحتية الرئيسية العامة وسلطات المصادقة وإظهار قيمتها في تقليل المخاطر الأمنية التي تواجه المجتمعات الحديثة
- شرح آليات التحكم الأكثر شيوعا في الدخول وأدوار أوث، OATH، SAMLومعايير الهويات المفتوحة في نطاق IAM وتطبيق مفاهيمSSO الموحدة
- إظهار هيكلة IAM باستخدام أدوات صناعية ودراسات الحالة (مثل جواز السفر الإلكتروني وحدود البوابة والأعمال المصرفية المتنقلة ونظام EMV والخدمات الإلكترونية المتحركة

الفئات المستهدفة

- تم تصميم هذه الدورة لاخصائيي تكنولوجيا المعلومات والمخططين الاستراتيجيين ومدراء المشاريع ومدراء الأمن والمهندسين المعماريين ومدراء المخاطر.

المحاور العلمية

- إدارة أمن المعلومات
- تنفيذ بنية تحتية رئيسية للعامة
- تحديد وتوثيق الإدارة
- إدارة الدخول للهوية(IAM)

مقدمة ومبادئ أمن المعلومات:

- لمحة عامة عن إدارة الهوية والدخول(IAM)
- سمات أمن المعلومات:
- السرية
- النزاهة
- التوفر
- عدم انكار التواصل
- المساءلة
- القابلية للتدقيق
- التشفير المتناظر وغير المتناظر
- التجزئة والتوقيع الرقمي
- الادارة الرئيسية

البنية التحتية للمفاتيح العامة(PKI)

- العمارة: الشهادة وسلطة التسجيل
- إدارة دورة الحياة
- أنواع الشهادات وأنماط الاستخدام
- التشفير
- التوقيع إلكتروني
- شهادة العميل
- شهادة الخادمSSL
- الشهادة المعتمدة على الصفة
- دراسات الحالة (مثل حماية البريد الإلكتروني والخدمات المصرفية عبر الهاتف النقال وتوقيع الوثيقة(

التحديد والتوثيق

- نظرة عامة عن التحديد والتحقق والتوثيق
- آليات لتحديد الهوية والتوثيق
- كلمة السر لمرة واحدة
- البصمة الحيوية
- التوقيع الالكتروني
- البطاقة الذكية
- القطع المعدنية الصلبة والاليكترونية
- أجهزة المحمول
- المصادقة القائمة على المخاطر
- المصادقة على الزيادة
- تسجيل الدخول المفرد وتسجيل الدخول الموحد
- القسم والتعريف الشخصي الجديد وتعريف الدخول للمتصفح وSAML
- الإطار العماري والأدوات الصناعية
- دور الحوسبة الموثوقة في ضمان الهوية
- المخاطر الأمنية المرتبطة بالآليات التي نوقشت

صلاحية التحكم

- مبادئ التفويض
- أنظمة التحكم في الدخول
- بروتوكولOath
- إدارة حقوق المشاريع وإدارة الحقوق الرقمية
- إدارة الحسابات المميزة
- الحوكمة والامتثال

إطار(IAM التعريف الشخصي وإدارة الدخول) وحالات استخدامه

- إطار IAM
- نظام IAM للصدى
- IAM والحوسبة السحابية
- توضيح حالات الاستخدام
- أمن الحدود
- الجواز السفر الالكتروني
- الهوية الوطنية
- البنوك الإلكترونية
- النظام الصحي الالكتروني
- نظام EMV