الرياض
جريدة يومية تصدر عن مؤسسة اليمامة الصحفية
الثلاثاء 18 من ذي القعدة 1426هـ - 20 ديسمبر 2005م - العدد 13693

أمن المعلومات و تقنيتها

لقد تعثر مرور مكالمتك...نرجو محاولة الاتصال مرة أخرى!

د. خالد بن سليمان الغثبر ❖

لن أتكلم عن الاتصالات الهاتفية و لا عن خدمات شركات الاتصالات و لكن سيدور المقال حول ركن أساس من مفاهيم أمن المعلومات الثلاث و هو الوجود الدائم. يرتكز مفهوم أمن المعلومات على ثلاثة محاور أساسية:

أولا: توفير السرية، و يقصد به حماية المعلومات في حال انتقالها أو تخزينها من التعرض للقراءة غير المشروعة، و يمكن استخدام التشفير لتوفير السرية.

ثانياً: تأمين صحة المعلومة و تكاملها، و يقصد بها المحافظة على حال المعلومة عند انتقالها أو تخزينها من التغيير غير المشروع. و لتيسير هذا المفهوم لنفترض أن شخصاً قام بتحويل مبلغ قدره ألف ريال و في حالة انتقال طلب التحويل قام احد المخربين (أو لوجود خلل في النظام) بزيادة صفرين للمبلغ فأصبح المبلغ المحول مائة ألف ريال!

ثالثاً: الوجود المستمر، و يقصد به المحافظة على بقاء الأنظمة المعلوماتية متوافرة لمستخدميها و المستفيدين منها. و كمثال على ذلك متابعة مواقع التداول الالكتروني للبنوك و الحرص على عدم تعطلها.

يتفق معي كثير من الناس في المحورين الأولين و لكن عندما يُطرح المحور الثالث فالأذهان قد لا تتقبله نظراً لما يعتقدونه من بعده عن مفهوم أمن المعلومات. دعوني أحاول توضيح علاقة الوجود بأمن المعلومات.

ماذا لو تم سرقة معلومات سرية لمنظمة؟... طبعاً المنظمة قد تتضرر بفقدان إيراداتها جراء تفشي أسرار تفوّقها من خلطات أو معادلات كيمائية أو جراء تفشي أسرار مضرة بسمعة الشركة و مكانتها بين العملاء. هذا فيما يخص المحور الأول (توفير السرية)

حسناً، ماذا لو تم التلاعب عبثاً في المعلومات المحاسبية لمنظمة؟... بالتأكيد سوف تضر بقرارات عديدة فضلاً عن وضع الشركة المالي و دقته. و ماذا لو تم التلاعب في حسابات عملاء البنوك؟...النتيجة باختصار: كارثة. هذا فيما يختص بالمحور الثاني (تأمين صحة المعلومة و تكاملها)

الآن، ماذا لو تم تعطيل بعض خدمات حساسة كنظام تداول الأسهم السعودية أو موقع متجر شركة أمزون الالكتروني (Amazon.com)؟ بلا شك أن هذا الفعل سوف يترتب عليه ضرر واضح بالإيرادات و غير واضح لصورة و سمعة المنظمة أمام العملاء و المستفيدين. و هذا فيما يختص بالمحور الثالث (الوجود المستمر).

لاحظ كيف تشاركت المحاور الثلاث في الاهتمام بتقليل الضرر. و لزيادة توضيح أهمية المحور الثالث و علاقته بأمن المعلومات يمكنني القول أن الضرر لا يقتصر على تعطيل خدمة ما بل يتعدى ذلك إلى المساس بالمحورين الأولين. لنأخذ مثالاً يوضح ذلك. لنفرض أني مشترك في خدمة تداول بنك التجار الالكترونية لتداول الأسهم عن طريق الانترنت، و عند تمام الساعة الرابعة و النصف عصراً (موعد تداول الفترة المسائية) قمت بالدخول للموقع لبدء التداول، لكني فوجئت بأني لا استطيع الوصول للصفحة الرئيسية للبنك على الموقع المعتاد و هو www.togaar.com.sa، مع العلم أني استطيع الوصول لأي صفحة على الانترنت و منها موقع منتدى الأسهم الذي أزوره خلال مدة التداول. بالطبع هذا الوضع غير مقبول لدي بتاتاً. و أنا أحاول الوصول للموقع بشكل مستمر عله يستجيب و

في الوقت نفسه أتابع المنتدى و أقرأ مواضيعه، لفت نظري موضوع كُتب فيه أن الكاتب من عملاء بنك التجار و انه كذلك وجد صعوبة في فتح موقع البنك، و بعد الاتصال بموظف البنك أفاده الموظف باستخدام عنواناً آخر يمكن للعملاء من استخدامه حتى يتم إصلاح الموقع الرئيسي و هو www.tojaar.com. بسرعة و بدون تردد قمت بكتابة العنوان الجديد و فعلاً أوصلني لموقع البنك، قمت بإدخال اسم المستخدم و كلمة المرور و بعدها ظهرت لي رسالة تفيد بأن الموقع الجديد سيتم إصلاحه خلال خمس دقائق و يرجى الانتظار... بعدها بمدة وجيزة تم إحالتي للموقع الأول و سجلت و تداولت الأسهم كالعادة و لم يكن في بالي إلا أن خدمات بنك التجار ضعيفة و غير منسقة.

ما تم فعلاً في هذا المثال هو أن احد المهاجمين عطل الموقع الرئيس للبنك و عمل موقعاً آخر و بنفس المظهر الرئيس لموقع البنك مع إمكانية تقبل اسم المستخدم و كلمة المرور و بدون أن يقدم أي شيء آخر غير ذلك و بمعاونة من احد الكتاب في ذلك المنتدى استطاع و في ذروة افتتاح التداول و توجه العملاء لفتح حاسباتهم أن يحصل على أسماء و كلمات مرورهم التي من خلالها يمكنه تحقيق الضرر بالعملاء و بالبنك.

أرأيتم كيف كان أثر تعطيل الخدمة و عدم تواجدها؟ إذا، أتوقع الآن أن كل الناس متفقون معي في ضرورة التفكير في مفهوم الوجود الدائم عند التفكير في تطبيق أمن المعلومات و الحرص على تطبيق المحور و عدم تجاهله.

و على فكرة، تعثر مرور المكالمات هي إحدى أمثلة عدم الوجود و تعطل الخدمات و التي قد ينتج عنها مشاكل أمنية.

استشاري أمن المعلومات - جامعة الملك سعود

CISSP, CISM, MCSE:Security, PMP, BS7799 LA
KSAKSU@GMAIL.COM