نقاط مهمة عن تهديدات أمن مواقع التجارة الإلكترونية (1)

د. هيا عبدالرحمن الشهري

في الوقت الحالي أصبح إنشاء مواقع للتجارة الإلكترونية أسهل بكثير من اي وقت مضى وذلك لوجود المصادر المفتوحة المتاحة مما ادى الى إزدهار التجارة الإلكترونية بشكل كبير جداً. ولكن ذلك اتاح بشكل اكبر ازدياد تهديدات التجارة الإلكترونية. هناك إعتبارات مختلفة لقضايا أمن التجارة الإلكترونية ومن أهمها ان مواقع الشركات الصغيرة تكون في الغالب هي الأضعف من بين مستويات الشركات الاخرى لانها لاتملك الموارد المتخصصة الكافيه لتدافع عن مواقعها وذلك بسبب تطور تلك التهديدات سريعا. يتمكن المتسللون الى حلول متوسطة والتصيد لمواقع الشركات بإستخدام شركائهم الإعلانيين. تمثل مشكلات الأمان التي تواجة الشركات التي تعمل في التجارة الإلكترونية تحديات كبيرة اكثر من السابق وذلك باسباب تدفق الاختراقات الامنية المستمرة والبيانات الضخمة والي زيادة تطور وإحترافية المهاجمين بالإضافة الى عالم اكثر إتصالا يعمل على توسيع نطاق الهجمات الأمنية. لذلك يجب تطوير الخطط الأمنية لمواقع الشركات بإستمرار لمواكبة التطور السريع في جميع التقنيات على كافة المستويات بالأدوات المناسبة لحل كل مشكلة امنية بما يناسبها.

هناك تساؤل: هل هناك علامات توضح ان مواقع التجارة الإلكترونية مخترقه؟

نعم هناك إشارات تبين إختراق الموقع

عندما تشهد مبيعات الموقع نسبة هبوط مفاجئة او سوء أداء الموقع قد يكون هذا بسبب تهديدات أمان لموقع الشركة الإلكتروني بالاضافة الى انه غالبا مايكون المحتالون على الشبكة العنكبوتية متاخرين للغاية ويستطيعون تجنب اكتشافة لفترات اطول ومع ذلك في بعض الحالات ، يميل المتسللون إلىإختراق شيء ما "مثل مكون إضافي غير وظيفي" أثناء المساس بالموقع الذي يعطي الهجوم بعيدًا. تتضمن التلميحات التاليه أساسية تهدد الانظمة:

- تحميل عالي على الخادم بسبب الطلبات المتكررة من نفس عناوينIP
- روبوتات تجريف المحتوى التي تخنق النطاق الترددي, بمعنى زيادة تحميله اكثر من طاقته
- عند ما تظهر المنتجات التي لم تقم الشركة بتسجيلها في المتجر على الموقع إذا كان الموقع ضعيف امنيا
- الإعلانات الضارة التي تطلب من العملاء تثبيت البرامج الضارة التي يتم عرضها على العملاء
- عندما يشكو المستخدمون من عمليات إعادة التوجيه الضارة التي تتسبب في ارتفاع معدل الارتداد الذي ياخذ المستخدم الى موقع اخر
- عنما يشكو العملاء من معلومات بطاقة الائتمان المسروقة على الرغم من أن الموقع متوافق مع Payment Card Industry(PCI) وهي مجموعة من معايير الأمان المصممة لضمان أن جميع الشركات التي تقبل أو تعالج أو تخزن أو ترسل معلومات بطاقة الائتمان تحافظ على بيئة آمنة.
- عندما يشكو المستخدمون من الدفع مقابل طلب لم يستلم
- تظهر سجلات الخادم أيضًا هجمات أخرى مثل محاولات DoS(رفض الخدمة) وهي منع الوصول الى الخدمة عند ارسال كم هائل من الأوامر الى الخادم الخاص بمزود الخدمة.

Source: magenticians.com