

حماية أنمن الشبكات الإلكترونية

تعد أمراً بالغ الأهمية في عصر التكنولوجيا الحديثة، حيث تزداد التهديدات الإلكترونية تعييناً يوماً بعد يوم.

إليك بعض الخطوات الأساسية التي يمكن اتباعها لتأمين الشبكات الإلكترونية

1*تحديث البرمجيات والأجهزة بانتظام

التتأكد من تثبيت آخر التحديثات الأمنية لأنظمة التشغيل والبرامج المستخدمة على الشبكة

2*استخدام جدران الحماية (Firewalls)

تثبيت جدران الحماية على الشبكة لمراقبة حركة المرور الواردة والصادرة ومنع الوصول غير المصرح به والتتأكد

من تكوين جدار الحماية بشكل صحيح ليكون فعالاً في حماية الشبكة

3*تشغيل البيانات

تشغيل البيانات الحساسة المخزنة على الخوادم أو أثناء نقلها عبر الشبكة

4*إدارة الهويات والوصول

قلل من صلاحيات المستخدمين إلى الأدنى لأداء مهامهم (مبدأ الامتياز الأقل)

5*تقسيم الشبكة

تقسيم الشبكة إلى أجزاء منفصلة لقليل تأثير الهجمات.

6*مراقبة الشبكة باستمرار

استخدم أدوات مراقبة الشبكة لاكتشاف أي نشاط غير عادي أو مشبوه وبنظام لتحديد أي محاولات اختراق أو انتهاكات أمنية.

7*توعية الموظفين

تدريب الموظفين على أفضل الممارسات الأمنية، مثل تجنب فتح رسائل البريد الإلكتروني المشبوهة أو النقر على الروابط غير المعروفة

تشجيع الموظفين على استخدام كلمات مرور قوية وتغييرها بانتظام

8*نسخ احتياطي منتظم

إجراء نسخ احتياطي منتظم للبيانات المهمة وتخزينها في مكان آمن والتتأكد من إمكانية استعادة البيانات بسرعة في حالة حدوث هجوم إلكتروني أو فقدان البيانات

9*استخدام أنظمة منع التسلل (IDS) واستخدام أنظمة كشف التسلل

تثبيت أنظمة كشف التسلل لاكتشاف ومنع الهجمات في الوقت الفعلي

10*تقييم الأمان بشكل دوري

إجراء اختبارات بشكل دوري لتقدير نقاط الضعف في الشبكة.

11*تطبيق سياسات أمنية واضحة

وضع سياسات أمنية واضحة للشبكة وتتأكد من أن جميع المستخدمين يلتزمون بها

12*حماية الأجهزة الطرفية

تثبيت برامج مكافحة الفيروسات وبرامج الحماية من البرامج الضارة على جميع الأجهزة المتصلة بالشبكات التتأكد من تحديث هذه البرامج بانتظام