

حماية أمن الشبكات الإلكترونية

تُعدُّ أمرًا بالغ الأهمية في عصر التكنولوجيا الحديثة، حيث تزداد التهديدات الإلكترونية تعقيدًا يوميًا بعد يوم.

إليك بعض الخطوات الأساسية التي يمكن اتباعها لتأمين الشبكات الإلكترونية

1*تحديث البرمجيات والأجهزة بانتظام

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

2* (Firewalls) استخدام جدران الحماية

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

من تكوين جدار الحماية بشكل صحيح ليكون فعالاً في حماية الشبكة

3*تشفير البيانات

تشفير البيانات الحساسة المخزنة على الخوادم أو أثناء نقلها عبر الشبكة

4* إدارة الهويات والوصول

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

5* تقسيم الشبكة

تقسيم الشبكة إلى أجزاء منفصلة لتقليل تأثير الهجمات.

6*مراقبة الشبكة باستمرار

استخدم أدوات مراقبة الشبكة لاكتشاف أي نشاط غير عادي أو مشبوه وبانتظام 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 والتأكد 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 الأمن بشكل دوري

إجراء اختبارات بشكل دوري لتقييم نقاط الضعف في الشبكة.

11*تطبيق سياسات أمنية واضحة

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

12* حماية الأجهزة الطرفية

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