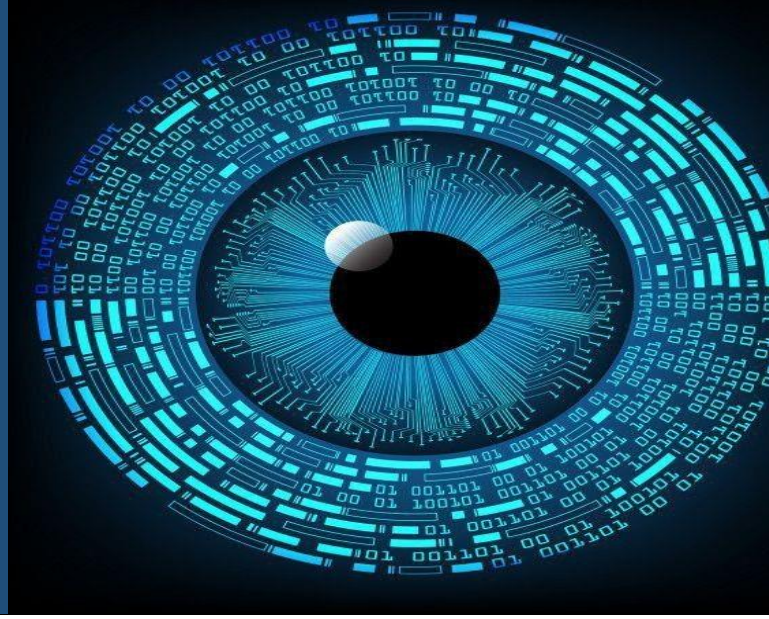
تقرير سنوي
Anuual

2026

المحتويات

قائمة المحتويات
contents

يهدف هذا التقرير الى تحليل ابرز الهجمات السيبرانية في عام 2026 واستعراض نقاط الضعف الشائعة في الأنظمة مع تقديم استراتيجيات عملية للاستجابة للحوادث وتوصيات فعالة لتعزيز الامن السيبراني في المؤسسات



الهجمات Cyber Attacks

هجمات الفدية

هجمات التصيد المتقدمة

هجمات سلسلة التوريد

هجمات الفدية تستهدف المؤسسات الكبرى والمستشفيات وتعتمد على تشفير البيانات وطلب فدية مالية

هجمات التصيد المتقدمة تستهدف المسؤوليين التنفيذيين

وتستخدم رسائل مخصصة تبدو رسمية لسرقة بيانات حساسة

هجمات سلسلة التوريد تخترق مزودي الخدمات السحابية او البرمجيات

وتؤثر على الاف الشركات عبر برمجيات موثوقة

تحليل نقاط الضعف الشائعة

نقطة الضعف	التاثير
ضعف كلمات المرور	تسهل اختراق الحسابات
عدم تحديث البرامج	يترك ثغرات امنية قابلة للاستغلال
نقص التوعية الامنية	يزيد من مخاطر التصيد
غياب التشفير	يعرض البيانات للسرقة
ضعف إدارة الصلاحيات	يسمح بانتشار الهجمات داخليا

استراتيجيات الاستجابة للحوادث

الاكتشاف المبكر

- استخدام أنظمة كشف الاختراق
- مراقبة الشبكات بشكل مستمر

الاحتواء

- عزل الأجهزة المخترقة فورا
- قطع الاتصال بالشبكة الداخلية

التحقيق والتحليل

- تحليل السجلات لتحديد مصدر الاختراق
- التعاون مع فرق السحابة للحوادث

التعافي

- استعادة البيانات من النسخ الاحتياطية
- تحديث الأنظمة واغلاق الثغرات

اهم التوصيات

١. تفعيل المصادقة متعددة العوامل لجميع الموظفين
٢. تحديث الأنظمة والبرامج بشكل دوري لاغلاق الثغرات
٣. عقد دورات توعوية امنية للموظفين
٤. عمل نسخ احتياطية منتظمة للبيانات المهمة
٥. تطوير خطة استجابة للحوادث وتحديثها باستمرار