الأمن السيبراني درع الحماية لبنوك الدم

المدونة :كوثر عدنان الهاجوج

الأمن السيبراني:

الحصن الحديث لحماية البيانات
في عصر تتدفق فيه البيانات كالأنهار الجارية في الفضاء الإلكتروني، يبرز الأمن السيبراني كسد منيع لحماية هذه البيانات من الاختراقات والهجمات الإلكترونية١. يُعرف الأمن السيبراني بأنه مجموعة من التقنيات والعمليات والضوابط التي تهدف إلى حماية الأنظمة والشبكات والبرامج والأجهزة من التهديدات الإلكترونية

عناصر الأمن السيبراني:

الأشخاص: العنصر البشري القادر على التعرف على التهديدات ومعالجتها.

السلطة: تعيين مسؤولين بصلاحيات لتنفيذ وإدارة برنامج الأمن السيبراني.

الدعم الإداري: الحصول على دعم الإدارة العليا لضمان نجاح البرنامج.

الميزانية: تخصيص ميزانية كافية لدعم البرنامج

التقنيات المناسبة: استخدام تقنيات قادرة على مواجهة التهديدات.

العملية الفعّالة: نهج فعّال لإدارة الأمن ومواجهة المخاطر.

تقنيات الأمن السيبراني:

01

أمن المعلومات: تأمين البيانات وخصوصيتها

03

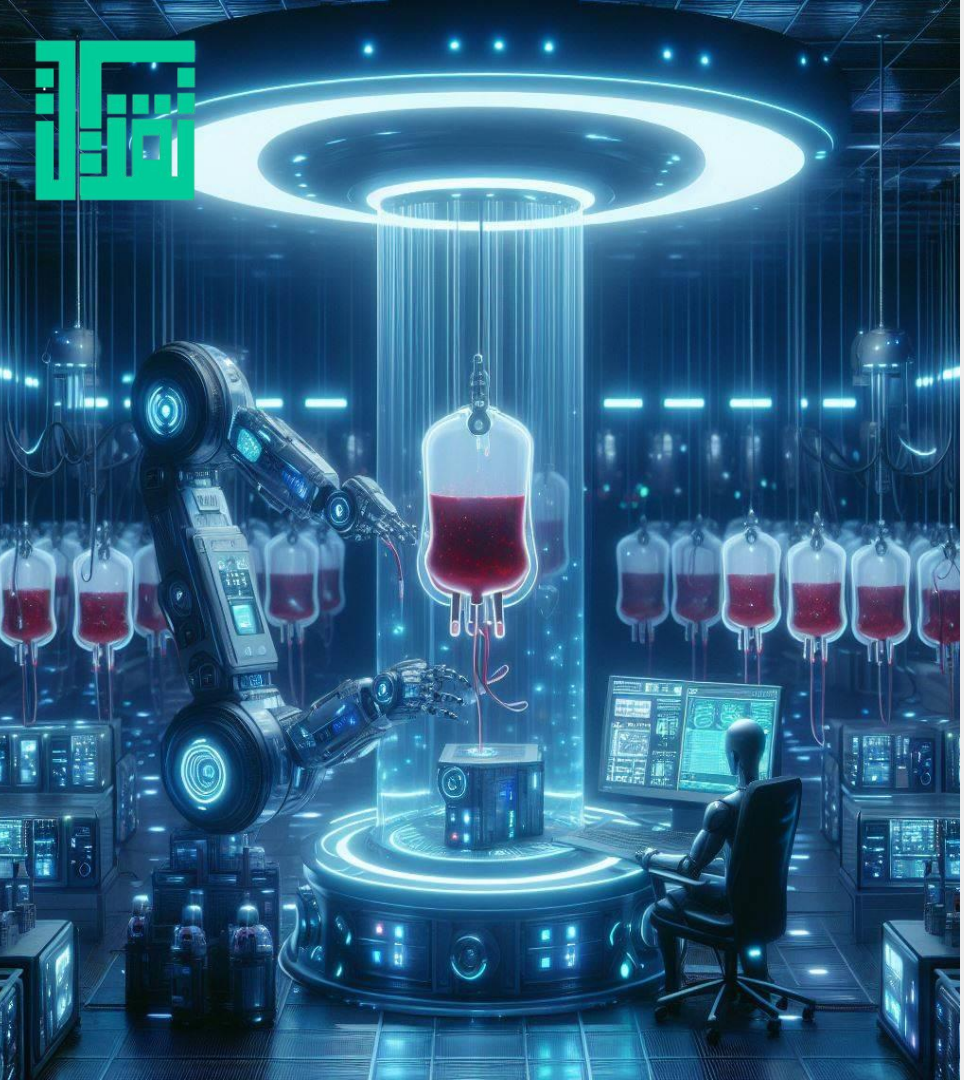
أمن التطبيقات: الحفاظ على سلامة البرمجيات والأجهزة.

04

أمن الشبكة: حماية الشبكة من المتطفلين والبرامج الضارة.

الأمن السيبراني: درع الحماية لبنوك الدم

في الوقت الذي تتزايد فيه الاعتمادية على التكنولوجيا في جميع جوانب الحياة، تبرز أهمية الأمن السيبراني كعامل حاسم في حماية المؤسسات الحيوية مثل بنوك الدم، حيث تعد بنوك الدم مراكز حيوية تقوم بجمع وتخزين ومعالجة وتوزيع الدم ومشتقاته للمرضى المحتاجين، وبالتالي، فإن أي تهديد لأمنها السيبراني قد يعرض حياة الأفراد للخطر



تحتوي بنوك الدم كمية هائلة من
البيانات الشخصية والطبية من
المتبرعين والمرضى مثل العناوين و
فصائل الدم والتواريخ والتفاصيل الاخرى
وتعتبر هذه البيانات موضع للخطر ومن
الأسباب التي تجعل أمن بنك الدم مهم ،
ومن خلال الأمن السيبراني يمكن تنفيذ
أنظمة التبرع الالكترونية ويتم خلال
لها التواصل بين المستشفيات وبنوك
الدم ويشكل مستوى من الأمان
لخصوصية المرضى والمتبرعين و تنفذ
تدابير أمنية قوية بحيث تمنع وصول
غير المصرح بهم الى البيانات.

استراتيجيات الأمن السيبراني في بنوك الدم:

- **سياسات الأمن السيبراني**: تطوير وثائق تحدد الأهداف والأدوار والمسؤوليات والإجراءات لضمان أمن المعلومات.
- **تدابير الحماية**: تنفيذ تدابير أمنية قوية لمنع الوصول غير المصرح به إلى البيانات والأنظمة
- **التأمين السيبراني**: الاستثمار في بوليصات التأمين السيبراني لتغطية الخسائر المحتملة نتيجة الهجمات السيبرانية.

الخلاصة:

يُعد الأمن السيبراني جزءاً لا يتجزأ من البنية التحتية لبنوك الدم، حيث يوفر الحماية اللازمة للبيانات الحساسة ويضمن استمرارية الخدمات الحيوية. من خلال تبني سياسات وتدابير أمنية متقدمة، تستطيع بنوك الدم مواجهة التحديات السيبرانية والحفاظ على سلامة الدم المخزن والموزع، مما يضمن الأمان للمتبرعين والمتلقين على حد سواء.

المراجع

Chandra, sekhar., Rajesh, Kumar. (2023). An Overview of Cyber Security in Digital Banking Sector. East

https://short-link.me/Egt-