الاستراتيجية لحماية جامعة الكتاب من الهجمات السيبرانية ...

- **الهدف**

تهدف هذه الاستراتيجية إلى حماية جامعة الكتاب من الهجمات السيبرانية من خلال نهج شامل يجمع بين الحلول التقنية والإدارية والبشرية

- **المخاطر**

تواجه الجامعات العديد من المخاطر السيبرانية، بما في ذلك

الاختراقات: يمكن للمهاجمين اختراق أنظمة الجامعة وسرقة البيانات الحساسة أو تعطيل العمليات

البرامج الضارة: يمكن للبرامج الضارة، مثل الفيروسات وبرامج الفدية، إتلاف الأنظمة والبيانات

الهجمات الإلكترونية: يمكن للمهاجمين شن هجمات إلكترونية على أنظمة الجامعة، مثل هجمات الحرمان أو هجمات الهندسة الاجتماعية (DoS) من الخدمة

- **الخطوات الرئيسية**

1. تقييم المخاطر

- إجراء تقييم شامل للمخاطر لتحديد الأصول الأكثر عرضة للخطر، والتهديدات المحتملة، والثغرات الأمنية الموجودة.
- تحديد مستوى المخاطر لكل تهديد وتحديد تأثيره على الجامعة.

2. التخطيط والوقاية

- وضع خطة شاملة للأمن السيبراني تحدد الأدوار والمسؤوليات والإجراءات للتعامل مع الهجمات السيبرانية.
- تطبيق حلول تقنية مناسبة، مثل جدران الحماية، وبرامج مكافحة الفيروسات، وبرامج التشفير، وأنظمة الكشف عن التسلل.

- نشر ثقافة الأمن السيبراني بين موظفي الجامعة والطلاب من خلال برامج التوعية والتدريب.

3. الاستجابة والتعافي

- وضع خطة استجابة لحالات الطوارئ تحدد الإجراءات التي يجب اتخاذها في حال وقوع هجوم سيبراني.
- اختبار خطة الاستجابة لحالات الطوارئ بانتظام للتأكد من فعاليتها.
- الاحتفاظ بنسخ احتياطية من البيانات الهامة لضمان استعادتها في حال وقوع هجوم سيبراني.

برامج الحماية المناسبة :

برامج مكافحة الفيروسات :

- حماية الأنظمة من البرامج الضارة، مثل الفيروسات وبرامج الفدية.
- تحديث برامج مكافحة الفيروسات بانتظام للحصول على أحدث تعريفات البرامج الضارة.

جدران الحماية :

- منع الوصول غير المصرح به إلى أنظمة الجامعة.
- تقييد حركة البيانات بين الشبكات الداخلية والخارجية.

أنظمة الكشف عن التسلل :

- رصد الأنشطة المشبوهة على أنظمة الجامعة.
- تنبيه المسؤولين عن الأمن السيبراني إلى التهديدات المحتملة.

برامج التشفير :

- حماية البيانات الحساسة من السرقة أو الاستخدام غير المصرح به.
- ضمان استمرارية عمل الجامعة في حال وقوع هجوم سيبراني.

حلول التوعية والتدريب :

- نشر ثقافة الأمن السيبراني بين موظفي الجامعة والطلاب.
- تعليمهم كيفية التعرف على التهديدات السيبرانية وكيفية التصرف في حال واجهوها.

➢ **ملاحظة**

- يجب مراجعة الاستراتيجية بانتظام وتحديثها لتواكب التطورات في مجال الأمن السيبراني.
- يجب أن تتناسب برامج الحماية مع احتياجات الجامعة وميزانيتها.

بالإضافة إلى ما سبق، إليك بعض النصائح الإضافية لحماية جامعة الكتاب من الهجمات السيبرانية

- استخدام كلمات مرور قوية وفريدة من نوعها لكل حساب.
- تحديث البرامج والتطبيقات بانتظام.
- توخي الحذر عند فتح رسائل البريد الإلكتروني والمرفقات غير المعروفة.
- عدم مشاركة المعلومات الشخصية أو الحساسة مع أي شخص.
- إبلاغ إدارة الجامعة عن أي نشاط مشبوه.

المقترحات:

1. برامج مكافحة الفيروسات
   Kaspersky
2. جدران الحماية
   Check Point
3. برامج التشفير
   Microsoft BitLocker
4. توعية و تدريبات

من خلال اتباع هذه الخطوات، يمكننا حماية جامعة الكتاب و نقلل من مخاطر الهجمات السيبرانية ونحمي بياناتها وأنظمتها من التهديدات.