**الذكاء الاصطناعي مساعد للبشرية ام مهدد لها**

 **تهديدات الامن السيبراني والذكاء الاصطناعي**

الذكاء الاصطناعي (AI) قد يكون أحد أكبر التطورات التكنولوجية في القرن الحالي، إلا أنه يمكن أن يشكل تهديدًا كبيرًا على الأمن السيبراني. فالأنظمة الذكية المدعومة بالذكاء الاصطناعي يمكن أن تتعرض للاختراق من قبل الهاكرز والمخترقين السيبرانيين، ويمكن أن يؤثر ذلك على الأمن السيبراني للمؤسسات والحكومات

تتعرض المؤسسات الحكومية للعديد من التهديدات في مجال الأمن السيبراني بسبب استخدام التقنيات الذكاء الاصطناعي. ومن بين هذه التهديدات:

1- هجمات القرصنة الإلكترونية: يمكن للمهاجمين استخدام تقنيات الذكاء الاصطناعي في تطوير هجمات القرصنة الإلكترونية المتطورة، والتي تستهدف سرقة البيانات الحكومية وتعطيل الأنظمة الحيوية.

2- هجمات الاحتيال الإلكتروني: يمكن استخدام التعلم الآلي في تطوير برامج الاحتيال الإلكتروني المتطورة، والتي تستهدف اختراق الأنظمة الحكومية وسرقة البيانات.

3- التلاعب بالبيانات: يمكن استخدام التقنيات الذكاء الاصطناعي في تلاعب البيانات الحكومية، وتغييرها بطريقة تسبب ضرراً للحكومة أو المواطنين.

4- الاختراق الذاتي: يمكن للتعلم الآلي المستخدم في الذكاء الاصطناعي أن يتعلم من تصرفات المستخدمين الحكوميين، ويستخدم هذه المعلومات لتطوير هجمات الاختراق الذاتي، والتي تتسم بالتعقيد والصعوبة في الكشف عنها.

**تعتبر الحكومات من أكثر الجهات تعرضًا للهجمات السيبرانية، ومن المهام الأساسية لها في التصدي لتلك الهجمات:**

* وضع استراتيجيات وسياسات سيبرانية قوية وفعالة، تحتوي على إجراءات وآليات تحديثية للحماية والوقاية من الهجمات السيبرانية

**كيف**

1. تحديث البرامج والأنظمة المستخدمة بشكل دوري: يجب تحديث البرامج والأنظمة بشكل دوري للتأكد من تغطية الثغرات الأمنية المعروفة وتحديث الأمان.
2. تعزيز الحماية بالأدوات الأمنية: يتضمن ذلك استخدام الحواجز النارية (Firewalls) ونظام كشف التسلل (Intrusion Detection System) والتشفير (Encryption) وأدوات الحماية من البرامج الضارة (Antivirus).
3. إنشاء أماكن لتخزين البيانات الحساسة: يجب وضع معايير وإجراءات واضحة لحماية البيانات الحساسة، مثل إنشاء أماكن خاصة لتخزينها وتقييد الوصول إليها.
4. التدريب الدوري للموظفين: يجب توفير التدريب الدوري للموظفين لتعزيز الوعي الأمني وتعليمهم السلوكيات الصحيحة للحماية من الهجمات السيبرانية.
* تشجيع المؤسسات والشركات والمواطنين على اتخاذ التدابير اللازمة للوقاية من الهجمات السيبرانية، مثل استخدام برامج الحماية الجيدة والتحديث الدوري للبرامج والأنظمة الأساسية.
* إنشاء فرق متخصصة في مجال الأمن السيبراني، للتحقق من تطبيق السياسات والإجراءات المعتمدة، وتحليل ومراقبة النشاطات السيبرانية المشبوهة.

كيف :

1. فريق الاستجابة للحوادث الأمنية في الشركة (CSIRT): وهو فريق يتم إنشاؤه داخل المؤسسة أو الشركة ويتم تعيينه للتحقق من تطبيق السياسات والإجراءات المعتمدة وتحليل ومراقبة النشاطات السيبرانية المشبوهة.
2. الفرق المختصة بالأمن السيبراني في الجيش: وهي فرق تابعة للجيش تعمل على حماية النظام السيبراني للدولة، وتحليل التهديدات السيبرانية المتعلقة بالدفاع العسكري والأمن القومي.
3. فريق التحقق من الأمان السيبراني (Security Assurance Team): وهو فريق متخصص في تقييم النظام السيبراني والتأكد من تطبيق الإجراءات الأمنية اللازمة، والتحقق من عدم وجود ثغرات أمنية
* التعاون والتنسيق مع الجهات المعنية الأخرى، سواء على المستوى المحلي أو الدولي، لتبادل المعلومات والخبرات وتحديد النهج والاستراتيجيات الفعالة في مكافحة الهجمات السيبرانية.
* الاستثمار في التدريب والتطوير المستمر للكوادر البشرية المختصة في الأمن السيبراني، لتمكينهم من مواكبة التحديات الجديدة في هذا المجال المتطور والمتغير باستمرار.

كيف :

يمكن إعطاء بعض الأمثلة على الاستثمار في التدريب والتطوير المستمر في مجال الأمن السيبراني كالتالي:

* 1. تدريب الكوادر الأمنية الحكومية على مختلف التقنيات الحديثة في مجال الأمن السيبراني، مثل الحماية من البرامج الخبيثة والتصيد الالكتروني والتشفير وغيرها.
	2. تطوير وتحسين مهارات العاملين في مجال الأمن السيبراني من خلال الحصول على دورات تدريبية وشهادات معتمدة في مجال الأمن السيبراني، وذلك لتحسين مهاراتهم ومعرفتهم بأحدث التقنيات والأدوات الأمنية.
	3. تعزيز التدريب الداخلي في الشركات والمؤسسات والحكومات عن طريق تنظيم دورات تدريبية دورية وورش عمل للتوعية بالمخاطر السيبرانية وتدريب الموظفين على كيفية التصرف في حالة وجود هجوم سيبراني.

المصادر:

* <https://www.csoonline.com/article/3277717/cybersecurity-skills-shortage-in-2021.html>
* <https://www.forbes.com/sites/forbestechcouncil/2020/02/07/the-importance-of-continuous-training-for-cybersecurity-professionals/?sh=3d35a29a3242>
* <https://www.cisco.com/c/en/us/products/security/cybersecurity-training.html>
* "Cybersecurity Strategies for Government Agencies"، Forcepoint.
* "5 Essential Strategies for Government Cybersecurity"، Symantec.