**تأثير الذكاء الاصطناعي على الأمن السيبراني**

يوجد حاليًا نقاش كبير يدور حول ما إذا كان الذكاء الاصطناعي أمرًا جيدًا أو سيئًا من حيث تأثيره على حياة الإنسان. مع تزايد عدد الشركات التي تستخدم الذكاء الاصطناعي لتلبية احتياجاتها ، فقد حان الوقت لتحليل الآثار المحتملة لتنفيذ الذكاء الاصطناعي في مجال الأمن السيبراني .

**الاستخدامات الإيجابية للذكاء الاصطناعي في الأمن السيبراني**

يتم استخدام عمليات تسجيل الدخول بالبصمات بشكل متزايد لإنشاء عمليات تسجيل دخول آمنة إما عن طريق مسح بصمات الأصابع أو شبكية العين. يمكن استخدام هذا بمفرده أو مع كلمة مرور ويتم استخدامه بالفعل في معظم الهواتف الذكية الجديدة. كانت الشركات الكبيرة ضحية لانتهاكات الأمان التي أدت إلى تهديد عناوين البريد الإلكتروني والمعلومات الشخصية وكلمات المرور. كرر خبراء الأمن السيبراني في مناسبات متعددة أن كلمات المرور معرضة بشدة للهجمات السيبرانية ، مما يهدد المعلومات الشخصية ومعلومات بطاقة الائتمان وأرقام الضمان الاجتماعي. هذه كلها أسباب تجعل تسجيلات الهوية الحيوية مساهمة إيجابية من الذكاء الاصطناعي في الأمن السيبراني .

يمكن أيضًا استخدام الذكاء الاصطناعي للكشف عن التهديدات وغيرها من الأنشطة الضارة المحتملة. لا يمكن للأنظمة التقليدية ببساطة مواكبة العدد الهائل من البرامج الضارة التي يتم إنشاؤها كل شهر ، لذلك هذا مجال محتمل للذكاء الاصطناعي للتدخل ومعالجة هذه المشكلة . تقوم شركات الأمن السيبراني بتدريس أنظمة الذكاء الاصطناعي للكشف عن الفيروسات والبرامج الضارة باستخدام خوارزميات معقدة حتى تتمكن الذكاء الاصطناعي من تشغيل التعرف على الأنماط في البرامج . يمكن تدريب أنظمة الذكاء الاصطناعي على تحديد حتى أصغر سلوكيات هجمات الفدية والبرمجيات الخبيثة قبل أن تدخل النظام ثم تعزلهم عن هذا النظام. يمكنهم أيضًا استخدام الوظائف التنبؤية التي تتجاوز سرعة الأساليب التقليدية.

تفتح الأنظمة التي تعمل على الذكاء الاصطناعي إمكانية معالجة اللغة الطبيعية التي تجمع المعلومات تلقائيًا عن طريق التصفية من خلال المقالات والأخبار والدراسات حول التهديدات السيبرانية. هذه المعلومات يمكن أن تعطي نظرة على بعض المفارقات ، والهجمات الإلكترونية ، واستراتيجيات الوقاية. يسمح ذلك لشركات الأمن السيبراني بالبقاء على إطلاع دائم على أحدث المخاطر والأطر الزمنية وبناء استراتيجيات سريعة الاستجابة للحفاظ على حماية المؤسسات .

يمكن أيضًا استخدام أنظمة الذكاء الاصطناعي في حالات المصادقة متعددة العوامل لتوفير الوصول إلى مستخدميها. يتمتع مختلف مستخدمي الشركة بمستويات مختلفة من امتيازات المصادقة التي تعتمد أيضًا على الموقع الذي يصلون منه إلى البيانات. عند استخدام الذكاء الاصطناعي ، يمكن أن يكون إطار المصادقة أكثر ديناميكية وفي الوقت الفعلي ، ويمكنه تعديل امتيازات الوصول استنادًا إلى شبكة المستخدم وموقعه. تقوم المصادقة متعددة العوامل بجمع معلومات المستخدم لفهم سلوك هذا الشخص واتخاذ قرار بشأن امتيازات وصول المستخدم .

لاستخدام الذكاء الاصطناعي بأقصى قدراتها ، من المهم أن يتم تنفيذه بواسطة شركات الأمن السيبراني المناسبة التي لديها دراية بوظائفها. بينما في الماضي ، يمكن أن تحدث هجمات البرمجيات الخبيثة دون ترك أي مؤشر على الضعف الذي تستغله ، يمكن أن الذكاء الاصطناعي يتدخل لحماية شركات الأمن السيبراني وعملائها من العديد من الهجمات الماهرة التي تحدث .

**عيوب وقيود استخدام الذكاء الاصطناعي لأمن الإنترنت**

الفوائد الموضحة أعلاه ليست سوى جزء بسيط من إمكانات الذكاء الاصطناعي في مساعدة الأمن السيبراني ، ولكن هناك أيضًا قيودًا تمنع الذكاء الاصطناعي من أن تصبح أداة سائدة تستخدم في هذا المجال. من أجل بناء وصيانة نظام الذكاء الاصطناعي ، تحتاج الشركات إلى قدر هائل من الموارد بما في ذلك الذاكرة والبيانات وقوة الحوسبة. بالإضافة إلى ذلك ، نظرًا لأن أنظمة الذكاء الاصطناعي يتم تدريبها من خلال مجموعات بيانات التعلم ، فإن شركات الأمن السيبراني تحتاج إلى الحصول على أيديها على العديد من مجموعات البيانات المختلفة من أكواد البرمجيات الخبيثة ، الرموز غير الخبيثة. يمكن أن يستغرق الحصول على كل مجموعات البيانات الدقيقة هذه وقتًا طويلاً وموارد لا تستطيع بعض الشركات تحملها.

عيب آخر هو أن المتسللين يمكنهم أيضًا استخدام الذكاء الاصطناعي بأنفسهم لاختبار البرمجيات الخبيثة وتحسينها ليصبحوا دليلًا على الذكاء الاصطناعي. في الواقع ، يمكن أن تكون البرامج الضارة المقاومة للذكاء الاصطناعي مدمرة للغاية لأنها يمكن أن تتعلم من أدوات الذكاء الاصطناعي الموجودة وتطوير هجمات أكثر تقدماً لتكون قادرة على اختراق برامج الأمن السيبراني التقليدية أو حتى الأنظمة التي تدعم الذكاء الاصطناعي.

**حلول لقيود الذكاء الاصطناعي**

مع العلم بهذه القيود والعيوب ، من الواضح أن الذكاء الاصطناعي هو طريق طويل من أن يصبح الحل الأمني السيبراني الوحيد. تتمثل الطريقة الأفضل في الوقت الحالي في الجمع بين التقنيات التقليدية وأدوات الذكاء الاصطناعي ، لذلك ينبغي للمنظمات أن تضع هذه الحلول في الاعتبار عند تطوير استراتيجية الأمن السيبراني الخاصة بها:

* قم بتوظيف شركة للأمن السيبراني مع محترفين لديهم خبرة ومهارات في العديد من الجوانب المختلفة للأمن السيبراني
* اطلب من فريق الأمن السيبراني اختبار أنظمتك وشبكاتك بحثًا عن أي ثغرات محتملة وإصلاحها على الفور
* استخدم عوامل تصفية لعناوين URL لمنع الارتباطات الضارة التي قد تحتوي على فيروس أو برامج ضارة
* قم بتثبيت جدران الحماية وغيرها من ماسحات البرامج الضارة لحماية أنظمتك وتحديثها باستمرار لمطابقة البرامج الضارة التي أعيد تصميمها
* راقب حركة المرور الصادرة وتطبيق عوامل تصفية الخروج لتقييد هذا النوع من حركة المرور
* راجع باستمرار أحدث تهديدات الإنترنت وبروتوكولات الأمان للحصول على معلومات حول المخاطر التي يجب عليك إدارتها أولاً وتطوير بروتوكول الأمان وفقًا لذلك
* قم بإجراء عمليات تدقيق منتظمة لكل من الأجهزة والبرامج للتأكد من صحة أنظمتك

يمكن أن يساعد اتباع هذه الخطوات في التخفيف من العديد من المخاطر المرتبطة بالهجمات الإلكترونية ، ولكن من المهم معرفة أن منظمتك لا تزال عرضة لخطر الهجوم. لهذا السبب ، لا تكون الوقاية كافية ويجب عليك أيضًا العمل مع فريق الأمان عبر الإنترنت لتطوير استراتيجية استرداد.

نظرًا لاستكشاف إمكانات الذكاء الاصطناعي لتعزيز صورة الأمان الإلكتروني لشركة ما ، يتم تطويرها أيضًا من قبل المتسللين. نظرًا لأنه لا يزال قيد التطوير وإمكاناته بعيدة المنال ، فلا يمكننا بعد معرفة ما إذا كان سيكون مفيدًا أو ضارًا للأمن السيبراني يومًا ما. في غضون ذلك ، من المهم أن تفعل المنظمات ما تستطيع بقدر الإمكان مع مزيج من الأساليب التقليدية والذكاء الاصطناعي للبقاء على رأس إستراتيجية الأمن السيبراني.

المرجع :

<https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/>