در ایجاد امنیت سایبری بهبودیافته، نقش هوش مصنوعی بسیار پررنگ است

امنیت بیشتر با هوش‌مصنوعی پیشرفته‌تر

هوش مصنوعی شاید تازه به دایره واژگانی عامه مردم اضافه شده باشد، اما عقبه آن به دهه ۱۹۵۰ بازمی‌گردد که تبدیل به بخش مهمی از فناوری شده بود؛ زمانی که یک موش روباتیک یاد گرفت که چگونه خود را از فضایی پر پیچ و خم خارج کند. در دهه ۱۹۹۰، نرم‌افزار هوشمند یاد گرفت که چگونه انسان‌ها را در شطرنج شکست دهد. اوایل دهه ۲۰۰۰، تولید عکس واقعی، ترجمه متن در مقیاس بزرگ، زیرنویس‌های خودکار و کدهای کپچا (CAPTCHA) را به ارمغان آورد که امیدوار بود انسان‌ها را از ماشین‌ها متمایز کند. اکنون هوش مصنوعی می‌تواند پروازها را برنامه‌ریزی کند، مردمک چشم و اثر انگشت انسان‌ها را ردیابی کند و حتی ماشین‌های خودران را براند. پشت این نوآوری‌های هیجان‌انگیز تیم‌هایی از مهندسان نرم‌افزار، دانشمندان داده، برنامه‌نویسان کامپیوتر و متخصصان یادگیری ماشین قرار دارند که با ارائه مقادیر زیادی داده به یادگیری هوش مصنوعی کمک می‌کنند.

هوش مصنوعی و امنیت

متخصصان امنیت سایبری مسئول حفاظت از داده‌ها، اطلاعات و شبکه‌های مورد استفاده برای تقویت هوش مصنوعی هستند. آنها حتی می‌توانند به هوش مصنوعی یاد دهند که چگونه از خود در برابر تهدیدات احتمالی و فعالیت‌های مخرب محافظت کند. این پیشرفت‌های هوش مصنوعی باعث شده افراد زیادی به این فکر بیفتند که مشاغل امنیت سایبری در نهایت منسوخ می‌شوند، اما به جای جایگزینی پرسنل آموزش‌دیده، شرکت‌ها و سازمان‌ها از هوش مصنوعی برای تکمیل و بهینه‌سازی کادر امنیت سایبری خود استفاده می‌کنند.

هوش مصنوعی چگونه در امنیت سایبری استفاده می‌شود؟

برخی از راه‌های ساده‌تر استفاده از هوش مصنوعی در امنیت سایبری شامل محافظت از رمز عبور، تشخیص فیشینگ و به‌روزرسانی خودکار نرم‌افزار است. در طول چند سال گذشته، در این حوزه کاربردهای پیشرفته دیگری کشف شده است. شناسایی خودکار تهدید و فرایندهای امنیتی مولد ۲نمونه از مهم‌ترین نمونه‌های استفاده از هوش مصنوعی در امنیت سایبری امروزی هستند.

تشخیص تهدید هوش مصنوعی و امنیت هوش مصنوعی مولد

یکی از بزرگ‌ترین کمک‌های هوش مصنوعی به امنیت سایبری تشخیص تهدید است؛ اینکه چگونه هوش مصنوعی می‌تواند تهدیدات سایبری را شناسایی و گزارش کند. با آموزش و ارائه مجموعه‌داده‌های مناسب، هوش مصنوعی می‌تواند از خود در برابر دسترسی ناخواسته کاربر، نقض داده‌ها و نرم‌افزارهای مخرب محافظت کند. طبق گفته فورتی‌نت که شرکت راه‌حل‌های امنیت سایبری است، هوش مصنوعی می‌تواند با نظارت مستمر تلاش‌های دسترسی، شناسایی رشته‌های جدید بدافزار و ایجاد هشدارهای امنیتی، لایه‌های امنیتی بیشتری به داده‌های حساس اضافه کند. هنگامی که هوش مصنوعی یاد گرفت که چگونه تهدیدات را شناسایی و پاسخ‌های مناسب ایجاد کند، سازمان‌ها می‌توانند در زمان و منابع ارزشمند خود صرفه‌جویی کنند. هوش مصنوعی در این موارد سریع‌تر تصمیم می‌گیرد، مجموعه‌داده‌های متعدد را همزمان تجزیه و تحلیل می‌کند و از داده‌های تاریخی بسته به تقاضا استفاده می‌کند. با قابلیت‌های قابل اعتماد شناسایی و گزارش‌دهی تهدید، متخصصان امنیت سایبری می‌توانند با کمک هوش مصنوعی تقریبا بلافاصله در برابر تهدیدات عکس‌العمل نشان دهند.

نمونه‌های بیشتر هوش مصنوعی و امنیت سایبری

هوش مصنوعی علاوه بر تشخیص تهدید و امنیت مولد، چندین مزیت دیگر نیز به این حوزه ارائه می‌کند.

یادگیری مستمر: هوش مصنوعی هر گز یادگیری از داده‌هایی را که با آنها در تعامل است متوقف نمی‌کند و بنابراین در لبه پیشروی با ترندها، تکنیک‌ها و آسیب‌پذیری‌های امنیت سایبری باقی می‌ماند. هوش مصنوعی می‌تواند این رویکردهای حیاتی را مستقیما به کارکنان ارائه دهد، از جمله داده‌های خام و تجزیه و تحلیل دقیق. هنگامی که تیم‌های امنیتی تصمیم می‌گیرند کدام داده ارزشمندتر است، می‌توانند بازخورد خود را به هوش مصنوعی ارائه دهند و یک حلقه یادگیری مداوم ایجاد کنند.

کارایی: از آنجا که هوش مصنوعی می‌تواند به کارهای معمول تجاری کمک کند، تحلیلگران و کارکنان امنیت سایبری می‌توانند تمرکز بیشتری روی عملیات‌های دارای تأثیر بیشتر داشته باشند. برخی از کارهای روزانه‌ای که هوش مصنوعی می‌تواند به آنها کمک کند شامل به‌روزرسانی وضعیت شبکه، جمع‌آوری دوره‌ای داده‌ها و نظارت بر فایروال (دیوار دفاعی) است. با توجه به وظایفی مانند این، متخصصان امنیت سایبری می‌توانند زمان بیشتری را به تجزیه و تحلیل داده‌های پیچیده، ارتقای سیستم و تحقیقات مربوط به تقلب اختصاص دهند.

احراز هویت رفتاری: هوش مصنوعی می‌تواند داده‌های متنی و ظریف کاربران را تجزیه و تحلیل کند، مانند زمان‌ها و مکان‌های ورود به سیستم، سبک‌های تایپ و انحرافات صوتی. شناسایی این الگوها به آن کمک می‌کند تشخیص دهد که چه زمانی تغییرات ممکن است نشان‌دهنده خطر امنیتی باشد. برای مثال، اگر کارمندی که از خانه کار می‌کند با یک آدرس IP متفاوت به شبکه شرکت وارد شود، هوش مصنوعی می‌تواند بلافاصله تیم امنیتی شرکت را خبردار کند. سپس ممکن است شخصی با کارمند تماس بگیرد و مطمئن شود که دستگاه او دزدیده نشده یا به خطر نیفتاده است.

خطرات امنیتی هوش مصنوعی

نوآوری‌های هوش مصنوعی و امنیت سایبری یک جنبه منفی دارد؛ مهاجمان سایبری از همان فناوری استفاده می‌کنند و تکنیک‌های خود را ارتقا می‌دهند. برخی از این خطرات در حال ظهور عبارتند از:

- **فیشینگ:** ابزار هوش مصنوعی ChatGPT و ابزارهای زبانی مشابه به مهاجمان کمک می‌کند تا کلاهبرداری‌های فیشینگ واقعی‌تر و متقاعدکننده‌تر را نسبت به گذشته بنویسند. هکرها ممکن است هوش مصنوعی را برای شناسایی اهداف بالقوه آموزش دهند و از مجموعه داده‌های شرکت و حتی اطلاعات ارائه شده در رسانه‌های اجتماعی استفاده کنند.
- **یادگیری ماشینی متخاصم:** هکرها تلاش می‌کنند تا نقاط ضعف الگوریتم‌های هوش مصنوعی را پیدا و سپس رفتار الگوریتم را به نفع خود مختل کنند. به‌عنوان مثال، آژانس امنیت سایبری و امنیت زیرساخت آمریکا (CISA) توضیح می‌دهد که هکرها می‌توانند داده‌های آموزشی را دستکاری کنند، مدل‌های پیش‌بینی‌کننده را تنظیم و داده‌ها را سرقت کنند و موارد دیگر.
- **دیپ فیک:** ترکیبی از «یادگیری عمیق» و «جعلی». دیپ فیک محتوای رسانه‌ای بسیار واقع‌گرایانه‌ای را توصیف می‌کند که کاملا با هوش مصنوعی ایجاد شده‌است. دیپ‌فیک‌ها به حجم عظیمی از داده‌ها در مورد محتوایی که ایجاد می‌کنند نیاز دارند. برای مثال، اگر تصویری مشابه یک فرد ایجاد شود، مجموعه داده به عکس‌ها و ویدئوهای باکیفیت آن شخص نیاز دارد. اگر نمونه‌هایی از نوشتن و صحبت کردن یک فرد ارائه شود، هوش مصنوعی حتی می‌تواند الگوهای گفتار و زبان را تقلید کند.

آیا هوش مصنوعی جایگزین مشاغل امنیت سایبری خواهد شد؟

کارمندان برای هدایت مسیرهای یادگیری هوش مصنوعی، تأیید تجزیه و تحلیل داده‌ها و محافظت از نرم‌افزارها، شبکه‌ها و مجموعه داده‌ها به مهارت‌های تخصصی نیاز دارند. این مهارت‌ها تقاضاهای زیادی دارند. گزارش رسمی ۲۰۲۳ در مورد مشاغل امنیت سایبری جهانی، ۳٫۵میلیون شغل خالی در صنعت را تا سال ۲۰۲۵ پیش‌بینی کرده است. طبق گزارش Cybersecurity Ventures، انتظار می‌رود هزینه جرائم سایبری تا سال ۲۰۲۵ به ۱۰٫۵ تریلیون دلار برسد. ۷ جرم سایبری تقریباً هر صنعت را تحت تأثیر قرار می‌دهد، بنابراین متخصصان رایانه و فناوری اطلاعات که به هوش مصنوعی تسلط دارند می‌توانند بدون توجه به مسیر شغلی مورد علاقه‌شان برای پیشرفت تلاش کنند.