امنیت، بزرگترین دستاورد استفاده هوش مصنوعی در مرکز داده است

مدتی است هوش مصنوعی برای مدیریت راحت‌تر و تأمین امنیت در مراکز داده استفاده می‌شود. ابزارهای هوش مصنوعی می‌توانند داده‌ها را مورد بررسی قرار داده و آنومالی‌هایی را تشخیص دهند که از دید انسان خارج است.

یک مثال خوب در مورد پیشرفت هوش مصنوعی، خودروهای بدون سرنشین هستند که تمام توجهات را به خود جلب کرده‌اند. اما برای سازمان‌ها بیشترین تأثیر هوش مصنوعی(AI) و یادگیری ماشینی(ML) مربوط به مباحث امنیتی بخصوص امنیت مرکز داده است. با بررسی‌هایی که در سال‌های اخیر انجام شده است خطرات بوالقوه‌ای مراکز داده را تهدید می‌کند و نگرانی‌هایی برای شرکت‌ها بوجود آورده است. در مطالب گذشته در مورد تأثیر هوش مصنوعی در مدیریت مراکز داده صحبت کردیم و اکنون اهمیت آن در تأمین امنیت را بیان می‌کنیم.

بر اساس تحقیقات شرکت Webroot و Walefield Research از بین 400 کارشناس در شرکت‌ها، 99 درصد از آنها معتقد هستند که در مجموع هوش مصنوعی باعث افزایش امنیت شرکتشان خواهد شد. همچنین 87 درصد از آنها در حال حاظر از هوش مصنوعی استفاده می‌کنند و 74 درصد اعتقاد دارند تا سه سال آینده سازمان‌ها نمی‌توانند امنیت دیجیتالی را بدون استفاده از هوش مصنوعی فراهم کنند.

AI و ML حتی می‌تواند در جاهایی استفاده شود که هنوز بدافزاری دیده نشده است و قرار است رفتار مشکوک کاربران و آنومالی در ترافیک شبکه، کشف شود. آنومالی به رفتارهای نابهنجاری گفته می‌شود که با قوانین از پیش تعیین شده مطابقت ندارد. هوش مصنوعی همچنان می‌تواند داده‌ها را تحلیل کند، خطاهای احتمالی پیکربندی و نقاط ضعف را تشخیص دهد، کد و زیرساخت را برای آسیب‌پذیری‌ها اسکن کند، استفاده از ابزارهای امنیتی را ساده‌تر کند و با توجه به تجارب گذشته یاد بگیرد که خودش را با شرایط تطبیق دهد.

یکی از نقاط قوت هوش مصنوعی و یادگیری ماشینی توانایی آن در بررسی سریع حجم زیادی از داده است. بر اساس گفته Manoj Asnani معاون تولید و طراحی شرکت Balbix انسان‌ها نمی‌توانند همه اطلاعات را مدیریت کنند و به موقع اقدام مناسب را در برابر خطرات انجام دهند. او می‌گوید: «سرمایه‌گذاری‌های مجازی و فیزیکی در دیتاسنترها در حال رشد است. بدون هوش مصنوعی سازمان‌ها نمی‌توانند در برابر حملات مقاومت کنند؛ حملاتی که همواره بیشتر و پیشرفته‌تر می‌شوند.»

فرض کنید تغییراتی در مرکز داده ایجاد می‌شود و به تبع آن قوانین فایروال باید به صورت دستی تغییر کنند. AI و ML مسئول این کار هستند. آنها معنی اتفاقاتی که در مرکز داده می‌افتد را می‌فهمند و اپلیکیشن‌هایی را که برای امن‌سازی، مناسب آن شرایط هستند را انتخاب و سپس قوانین جدید فایروال را به کمک اپلیکیشن‌ها بازنویسی می‌کنند. سیستم‌های هوشمند همچنین می‌توانند بر روی رفتارهایی که اهمیت زیادی برای انسان دارد، بیشتر تمرکز کنند. برای مثال میزان حرارت سخت‌افزار مدل‌سازی و با فعالیت‌های عادی مقایسه شود یا اینکه زمان‌های دسترسی انفرادی کاربران به سیستم با همتاهایشان مقایسه و آنومالی‌ها کشف شوند.

شرکت‌های آینده‌نگر توجه زیادی به هوش مصنوعی خواهند داشت و سرمایه‌گذاری زیادی در این بخش می‌کنند تا از مزایای آن بهره‌مند شوند. با این وجود اپراتورهای مرکز داده کوچکتر نیز سود می‌برند. زیرا اکثر شرکت‌های مرتبط با امنیت در حال اضافه کردن هوش مصنوعی به محصولاتشان هستند. اگر شرکت‌های تأمین‌کننده امنیت نتوانند خود را با شکلی از هوش مصنوعی وفق دهند، احتمالاً عقب‌تر از سایر رقبا قرار می‌گیرند.

مطالب گفته شده نتایجی از جاسازی هوش مصنوعی و یادگیری ماشینی در فناوری‌های امنیتی است که در مراکز داده استفاده می‌شود و رشد اپلیکیشن‌های فناوری اطلاعات را سریع‌تر کرده است.

منبع:
دیتاسنترنالج
تاریخ انتشار:
10 بهمن 1396

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/11655/%D8%A7%D9%85%D9%86%DB%8C%D8%AA%D8%8C-%D8%A8%D8%B2%D8%B1%DA%AF%D8%AA%D8%B1%DB%8C%D9%86-%D8%AF%D8%B3%D8%AA%D8%A7%D9%88%D8%B1%D8%AF-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%87%D9%88%D8%B4-%D9%85%D8%B5%D9%86%D9%88%D8%B9%DB%8C-%D8%AF%D8%B1-%D9%85%D8%B1%DA%A9%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87-%D8%A7%D8%B3%D8%AA