پنج مزیت هوش مصنوعی برای کسب‌وکارها

کیوان نقره‌کار
کارآفرین ملی
در حوزه آموزش و فناوری

استفاده از هوش مصنوعی می‌تواند به شرکت‌ها کمک کند تا به بهبود عملکرد، کاهش هزینه‌ها، افزایش سودآوری و افزایش رضایت مشتریان خود دست یابند.
در مسیر تحول دیجیتال هفته گذشته به ورود فناوری از تغییر ساختار نرم‌افزاری و سخت‌افزاری تا توسعه و ارتقای دانش و فرهنگ سازمان پرداخته شد که باید با چابکی لازم انجام شود اما تا زمانی که باور کارایی استفاده از هوش مصنوعی برای مدیران مسجل نشود پس عملا این اتفاق نمی‌افتد.
در اینجا ۵ مزیت هوش مصنوعی در کسب‌وکارها را برای شما بازگو می‌کنم، شما می‌توانید یکی از اینها یا هر پنج تای آن را در کسب‌وکار خودتان به کار ببرید.

۱. تحلیل داده‌ها: استفاده از الگوریتم‌های یادگیری ماشین و تحلیل داده‌ها در کسب و کار به‌عنوان یک ابزار بسیار قوی برای شناسایی الگوهایی که در داده‌های کسب‌وکار وجود دارند، می‌تواند به شرکت‌ها کمک کند تا خطاها را کاهش دهند و فرصت‌های جدید را شناسایی کنند.

۲. سفارشی‌سازی تجربه کاربری: استفاده از هوش مصنوعی برای شناسایی نیازهای مشتریان و سفارشی‌سازی تجربه کاربری، می‌تواند باعث بهبود رضایت مشتریان و افزایش فروش شود.

۳. خودکارسازی فرآیندها: استفاده از هوش مصنوعی برای خودکارسازی فرآیندهای کسب‌وکار، می‌تواند به شرکت‌ها کمک کند تا هزینه‌ها و زمان را کاهش داده و کارایی را افزایش دهند.

۴. پیش‌بینی بازار: استفاده از هوش مصنوعی برای پیش‌بینی بازار و شناسایی روندهای جدید، می‌تواند به شرکت‌ها کمک کند تا بهترین تصمیمات را در زمان مناسب بگیرند و به سرعت به تغییرات بازار واکنش نشان دهند.

۵. امنیت سایبری: استفاده از هوش مصنوعی در امنیت سایبری، می‌تواند به شرکت‌ها کمک کند تا از حملات سایبری دفاع کرده و اطلاعات محرمانه را محافظت کنند.

بهره‌گیری از هوش مصنوعی مزایای بسیاری برای سازمان‌ها دارد که در بالا به چندتا از آنها اشاره کردیم. آیا شما مزیت دیگری در استفاده از هوش مصنوعی با توجه به نوع سازمان خودتان می‌توانید نام ببرید؟

۳۰ احراز هویت و دسترسی

مدیریت کنید چه کسی و چه چیزی بتواند به سیستم‌ها و داده دسترسی داشته باشد. حتما برای کاربران‌تان سطح دسترسی قرار دهید و به طور فصلی یا ماهانه سطح دسترسی ها را مجددا چک یا بررسی کنید

۲۰ امنیت داده

- از مجموعه داده آسیب پذیر خود محافظت کنید.

حتما فایروال (دیواره آتش) بر روی نرم‌افزارها یا راهکارهایی برای موارد حفاظتی اسناد فیزیکی خود قرار دهید

۷۰ معماری و پیکربندی

نیت خود را طوری بسازید، که نگهداری و شما کاربردی باشد یعنی بتوانید هر لحظه نید و بتوانید دائم آن را به روز رسانی کنید جوابگوی نیازهای فعلی و آتی شما باشد.

۶۰ مدیریت آسیب پذیری

- محافظت از سیستم‌ها باید در تمام طول چرخه عمرشان پیوسته ادامه داشته باشد. یکی از روش‌های رخنه هکرها و بدافزارها به سیستم‌ها قدیمی شدن روش‌های محافظت یا استفاده از نرم‌افزارهای قفل شده یا شیوه‌های اشتباه در نحوه انتقال است.

۱۰ مدیریت حوادث

- برای هر رویداد سایبری واکنش مناسب را از پیش برنامه ریزی کنید. سیستم‌های جایگزین و راهکارهای مختلف به شما کمک می‌کند که اطلاعات شما حفظ شود و در اثر سهل انگاری از بین نرود!

۱۰ امنیت زنجیره تامین

- با تأمین کنندگان و شرکای خود همکاری کنید، حتما از تجهیزات و نرم‌افزارهایی که تهیه می‌کنید از به روز بودن آن با خبر شوید. اگر اشکالی گزارش شد حتما با خبر شوید و اگر پیشنهاد جدیدی به شما داده می‌شود در صورت تایید، بررسی و سریعا اجرا کنید.

منبع: NCSC (مرکز ملی امنیت سایبری)