



مدیر آنتروپیک می‌گوید کارمندان هوش مصنوعی سال آینده از راه می‌رسند

به گفته «جیسون کلینتون»، مدیر ارشد امنیت اطلاعات آنتروپیک (Anthropic)، این شرکت انتظار دارد..

به گفته «جیسون کلینتون»، مدیر ارشد امنیت اطلاعات آنتروپیک (Anthropic)، این شرکت انتظار دارد کارمندان مجازی مبتنی بر هوش مصنوعی ظرف یک سال آینده در شبکه‌های سازمانی حضور یابند و باید از نظر امنیتی برای آنها آماده شویم. اظهارات مدیر آنتروپیک از آن جهت اهمیت دارد که مدیریت نیروهای مبتنی بر هوش مصنوعی شرکت‌ها را ناگزیر می‌کند تا استراتژی‌های امنیت سایبری خود را بازبینی کنند، در غیر این صورت ممکن است در معرض نقض‌های جدی امنیتی قرار بگیرند. پایگاه خبری تحلیلی انتخاب: به گفته «جیسون کلینتون»، مدیر ارشد امنیت اطلاعات آنتروپیک (Anthropic)، این شرکت انتظار دارد کارمندان مجازی مبتنی بر هوش مصنوعی ظرف یک سال آینده در شبکه‌های سازمانی حضور یابند و باید از نظر امنیتی برای آنها آماده شویم.

اظهارات مدیر آنتروپیک از آن جهت اهمیت دارد که مدیریت نیروهای مبتنی بر هوش مصنوعی شرکت‌ها را ناگزیر می‌کند تا استراتژی‌های امنیت سایبری خود را بازبینی کنند، در غیر این صورت ممکن است در معرض نقض‌های جدی امنیتی قرار بگیرند.

کلینتون در گفتگو با Axios می‌گوید کارمندان مجازی می‌توانند به یکی از حوزه‌های داغ نوآوری در هوش مصنوعی تبدیل شوند. برخلاف عامل‌های خودکار فعلی که روی وظایف خاصی متمرکزند، این هویت‌های مجازی حافظه مستقل، نقش‌های مشخص در سازمان، حساب‌های کاربری و حتی رمز عبور اختصاصی خواهند داشت. سطح خودمختاری آنها بسیار فراتر از عامل‌های امروزی است.

کلینتون مدعی است در این جهان جدید، چالش‌های امنیتی زیادی وجود دارد که هنوز برایشان راه حل مناسبی پیدا نکرده ایم. ازجمله این چالش‌ها می‌توان به چگونگی تأمین امنیت حساب‌های کاربری کارمندان مجازی، میزان دسترسی مناسب به شبکه و تعیین مسئول مدیریت عملکرد آنها اشاره کرد.

کلینتون توضیح داد آنتروپیک ۲ مسئولیت اصلی در این مسیر دارد: اول آزمایش گسترده مدل‌های کلود (Claude) برای مقاوم سازی آنها در برابر حملات سایبری. دوم نظارت بر مسائل ایمنی و کاهش راه‌های سوءاستفاده از مدل‌های کلود توسط عوامل مخرب.

هشدار آنتروپیک درباره تهدیدات امنیتی در دنیای کارمندان مجازی

درحال حاضر، مدیران شبکه می‌کوشند برای کنترل حساب‌های کاربری متعدد و مقابله با هک‌هایی هستند که از رمزهای عبور فاش شده در دارک وب سوءاستفاده می‌کنند. در این شرایط، ظهور کارمندان مجازی، خطرات تازه‌ای ایجاد می‌کند؛ برای مثال، کارمند مجازی ممکن است به سیستم‌های حساس مانند سامانه‌های تست و ادغام کد شرکت نفوذ کند، بدون اینکه مسئولیتی متوجه شخص خاصی شود.

کلینتون تأکید می‌کند امنیت کارمندان مجازی یکی از مهم‌ترین حوزه‌هایی است که شرکت‌های هوش مصنوعی باید در آن سرمایه‌گذاری کنند. او به ویژه بر اهمیت راهکارهایی اصرار کرد که شفافیت بیشتری درباره عملکرد حساب‌های کاربری مجازی ایجاد کرده و دسته‌بندی جدیدی برای این هویت‌ها ارائه می‌دهند.

چندین شرکت امنیت سایبری هم اکنون محصولات جدیدی برای مدیریت «هویت‌های غیرانسانی» معرفی کرده‌اند؛ برای نمونه، شرکت «Okta» در فوریه پلتفرم کنترل یکپارچه‌ای برای محافظت از این هویت‌ها و نظارت بر رفتار آنها عرضه کرد.

منبع: دیجیاتو