کد خبر: ۱۰۶۹۴۳۶
یکشنبه ۲۸ اردیبهشت ۱۳۹۹ ۱۲:۴۵

ایسکانیوز گزارش می‌دهد؛

هوش مصنوعی؛ امنیت سایبری و مخاطرات سازمان‌های دولتی

مهم‌ترین عامل افزایش مخاطرات سایبری در کشور ما عدم درک درست از فناوری و عدم پذیرش کامل فناوری است. متأسفانه از ابتدای ورود فناوری‌های نوین به کشور تاکنون هیچ رویه مثبتی نسبت به فناوری توسط متولیان کشور صورت نپذیرفته و هرکدام نسبت به جبر فناورانه مجبور به پذیرش ناقصی از آن فناوری شده‌اند.

به گزارش خبرنگار گروه علم و فناوری ایسکانیوز، خطرات امنیت سایبری، پیچیده‌تر از همیشه شده و پیش‌بینی می‌شود که با گسترش استفاده از اینترنت اشیا و هوش مصنوعی، هر شخص تا پایان سال ۲۰۲۰ حدود ۱.۷ مگابایت اطلاعات در هر ثانیه تولید کند. در همین حال، با تکامل این فناوری‌های جدید، مجرمان سایبری نیز به روش‌های جدیدی برای هک کردن داده‌ها دست یافتند و سازمان‌های دولتی یکی از مهم‌ترین کانون‌های هدف آن‌ها است. در این راستا با سینا تفنگ‌چی، متخصص هوش مصنوعی و مدرس علوم ارتباطات دانشگاه پیام نور پیرامون چالش‌ها و راهکارهای برون‌رفت از این مخاطره فناورانه گفتگویی انجام داده‌ایم.

مهم‌ترین عامل برای افزایش مخاطرات سایبری در کشور ما عدم درک درست از فناوری و عدم پذیرش کامل فناوری است. متأسفانه از ابتدای ورود فناوری‌های نوین به کشور ما یعنی از زمان مظفرالدین شاه قاجار تاکنون هیچ رویه مثبتی نسبت به فناوری توسط متولیان کشور صورت نپذیرفته و هرکدام نسبت به جبرفناورانه مجبور به پذیرش ناقصی از آن فناوری شده‌اند.

از همین رو است که می‌بینیم همچنان درگیر مسائل ساده با فناوری هستیم و این مقاومت بیش از حد متولیان کشور نسبت به پذیرش فناوری و ایجاد قانون مطلوب که هم به کاربر آسیب نرساند و هم مانع از بروز خطرات بیشتر نشود سبب افزایش تهدیدهای فناورانه شده است.

مدرس علوم ارتباطات دانشگاه پیام نور تصریح کرد: امروزه بحث فناوری سریع‌تر از هر دانشی در حال پیشرفت است و با توجه به آنکه مهم‌ترین فناوری پیش‌رو، هوش مصنوعی است، کشورهای اروپایی در حال تدوین قوانینی برای ارائه مطلوب این فناوری به مردم خودشان هستند.

با وضع قوانین، پیش از ورود فناوری به کشور، نه تنها فرهنگ استفاده صحیح توسط مردم می‌تواند به حد مطلوبی صورت گیرد، بلکه دولت‌ها نیز، درگیر مسائل روزمره مخاطرات احتمالی نمی‌شوند و به این صورت روند تسلط انسان بر فناوری و نه برعکس آن کماکان ادامه خواهد پیدا کرد. این در حالی است که در ایران دقیقاً برعکس این اتفاق صورت پذیرفته و همواره متولیان کشور، نظر به وقوع شرایطی مجبور به اقداماتی همچون مسدود کردن و قطع کامل دسترسی به آن فناوری می‌شوند.

متخصص هوش مصنوعی در ادامه به دلایل ضعف سازمان‌های دولتی در مواجهه با مخاطرات سایبری اظهار کرد: سازمان‌های دولتی با توجه به اینکه بیش از مراکز خصوصی درگیر تفکرات سنتی متولیان کشور هستند، به همان میزان بیشتر در صدد مقابله با بهره‌مندی از فناوری بر می‌آیند. متأسفانه همواره چالش‌های سه اداره روابط عمومی ،حراست و فناوری اطلاعات در سازمان‌ها سبب می‌شود تا نتوانیم به صورت مطلوبی به توسعه فناورانه یک سازمان دست یابیم. طبق قاعده سازمان‌های دولتی، حراست در تمام زمینه‌ها تمایل به حفظ دیدگاه

امنیتی دارد و تصور می‌کند که در پی هر دسترسی امنیت سازمان به یکباره مورد تهدید قرار می‌گیرد و فناوری اطلاعات نیز همواره در صدد مسدود کردن هرچه بیشتر با تصور حفظ امنیت است.

وی ادامه داد: اساساً هیچکدام از این دو اداره تمایلی به تقویت زیرساخت‌ها ندارند و محدود کردن را عاملی برای تقویت می‌دانند. این درحالی است که در همین هفته گفته شد که شرکت توئیتر این امکان را برای کارمندان خود ایجاد کرده که به صورت کامل بتوانند در خانه به کارهایشان بپردازند و با هیچ مشکلی هم مواجه نشوند؛ امری که سبب کاهش هزینه‌های هرچه بیشتر سازمان و افزایش بهره‌وری کارمندان نیز می‌شود.

با این‌حال در کشورمان، شاهد مسدود شدن سایت‌ها، کاهش سطح دسترسی کارکنان، مسدود کردن دسترسی آن‌ها به اینترنت و قابلیت‌هایی همچون استفاده از و... هستیم. اگر سازمان‌ها تلاش به تقویت زیرساخت‌های خود کنند، بی‌نیاز از بسیاری از این محدودیت‌ها می‌توانند نه تنها امنیت سازمان خود را تأمین کنند بلکه به توسعه سازمان خود نیز بپردازند.

تفنگ‌چی در پاسخ به این سوال که با توجه به نقش هوش مصنوعی هر روز رنگ بیشتری در حوزه امنیت سایبری پیدا می‌کند، چه تأثیری در کاهش مخاطرات امنیتی سازمان‌های دولتی می‌تواند ایفا کند؛ اظهار داشت: سال‌ها پیش وینتون سرف یکی از متخصصان بسیار شناخته شده در حوزه امنیت سایبری گفته بود که برای جلوگیری از مخاطرات امنیت سایبری نیازمند برنامه نویس قوی نیستیم، بلکه ابزار قوی نیاز داریم و امروز آن ابزار در دسترس ما قرار گرفته است. با استفاده از هوش مصنوعی می‌توان امنیت سایبری را به حداکثر و نفوذپذیری را به حداقل رسانید.

وی تصریح کرد: با استفاده از هوش مصنوعی می‌توان مانع از اسکن‌های پیشرفته، ویدئوهای جعل عمیق، هک اثر انگشت و رمزگشایی شد هرچند که باید توجه داشت که خود همین موارد حاصل از هوش مصنوعی بوده است.

مدرس علوم ارتباطات دانشگاه پیام نور تصریح کرد: به صورت غیرانتزاعی بخواهیم بگوییم تنها راه حل ممکن تقویت همیشگی زیرساخت ها برای مقابله با نفوذ سایبری است؛ چراکه به همان موازات که متخصصان امنیت پیشرفت می کنند؛ هکرها نیز پیشرفت کرده و با استفاده از نفوذ به سیستم های و نیز اسکن سریع شبکه ها با استفاده از هوش مصنوعی، راه هایی برای نفوذ پیدا می کنند.

متخصص هوش مصنوعی تأکید کرد: با این‌حال در سال‌های اخیر تلاش برای تحدید هرچه بیشتر فضای نفوذپذیری ایجاد شده که عمدتاً بر بستر بلاکچین که بیشتر کاربردهای حوزه مالی دارد متمرکز بوده است؛ ولی دستیابی به ایده بسیار قدیمی رایانه‌های کوانتومی در گام‌های خوبی قرار گرفته که در پی آن هم اکنون مراحل ارائه آن در پایان ۲۰۲۰ در حال طی شدن است. با استفاده از رایانه‌های کوانتومی به فضای اینترنتی غیرقابل هک می‌توان دست یافت. این فناوری که سال‌های بسیاری برای دستیابی به آن تلاش شده سبب درهم تنیدگی در شبکه شده که با این اتفاق امنیت تضمین شده و استراق سمع غیرقابل امکان می‌شود.

تفنگ چی همچنین به سایر راه‌های ممکن برای تقویت امنیت سایبری با استفاده از هوش مصنوعی اشاره کرد و گفت: با استفاده از یادگیری ماشینی ( ) که هم اکنون در استفاده از اسکن‌های شناسایی ویروس کرونا نیز مورد استفاده قرار گرفت، می‌توان ضمن ایزوله کردن هرچه بیشتر سیستم، به شناسایی رفتار هکرها پرداخت و بدین طریق در هنگام تلاش های آنان برای نفوذ، اقدامات لازم برای مقابله صورت پذیرد.

مدرس علوم ارتباطات دانشگاه پیام نور افزود: همچنین دیگر ابزار در دسترس و کارآمد در زمینه مقابله با هک و نفوذ به سیستم دستگاه‌ها نام دارد که از سال ۲۰۱۹ به بازار آمده و بر بستر اینترنت اشیا و بلاکچین خدمت رسانی می‌کند. این فناوری که هم اکنون مورد استفاده بسیاری از شرکت‌های بزرگ خدماتی نیز قرار گرفته در مقیاس وسیع و برای سازمان‌هایی که ورود کاربران زیادی دارند مناسب است.

متخصص هوش مصنوعی ادامه داد: یکی دیگر از راه‌هایی که می‌توان به آن برای کاهش نفوذپذیری به سازمان‌ها اشاره داشت، بهره مندی از ارکستراسیون امنیتی اتوماسیون و پاسخ () است که ضمن تقویت مدیریت امنیت، امکان خنثی‌سازی و تجزیه و تحلیل نفوذ را هم فراهم کرده و اجازه می‌دهد تا تعریف، اولویت‌بندی و هدایت پاسخ به نفوذ از طریق یک گردش کاری استاندارد صورت گیرد.

تفنگ‌چی ادامه داد: این فناوری نیز در بستر هوش مصنوعی بوده و ضمن بهبود کیفیت هشداردهی، زمان مورد نیاز برای در دسترس بودن تحلیلگران سایبری را کاهش می‌دهد و مدیریت امنیتی را بهبود می‌بخشد.

می توان چنین برداشت کرد که پذیرش فناوری، تهدید نکردن بستر داخلی و تقویت زیرساخت‌ها، آشنایی با فناوری‌های روز و هزینه کردن برای دستیابی به این ابزارها سبب می‌شود تا ضمن جلوگیری از نفوذ به سیستم ها به پیشرفت سازمان نیز کمک کنیم. دیگر باید از لجبازی‌های دیدگاه‌های امنیتی و مقابله جویانه با فناوری گذر کنیم، در غیر اینصورت جبر فناورانه ما و سازمان‌مان را به برده‌های فناوری بدل می‌کند.

انتهای پیام/