امنیت

لزوم به‌روزرسانی امنیتی با آمدن هوش مصنوعی

حمیدرضا خاتونی
سردبیر کلیک

یکی از موارد مهمی که کسب و کارها باید به آن توجه ویژه داشته باشند ایجاد راهکار مناسبی برای بهبود هر لحظه در امنیت اطلاعات و داده هاست.

همیشه هکرها از رخنه امنیتی سوءاستفاده کرده و داده‌های یک سازمان، شرکت و ... را از بین می‌برند یا با ایجاد بدافزارها، سازمان‌ها را دچار اختلال می‌کنند.

با توجه به پیشرفت‌های تکنولوژی و هوش مصنوعی سازمان‌ها و شرکت‌های بزرگ باید به گوش باشند چون آمدن هوش مصنوعی مانند چاقویی دو لبه است از طرفی می‌تواند به سازمان‌ها کمک کند تا بهترین نتایج را از این تکنولوژی ببرند و هم از طرفی باید ترسید چون هوش مصنوعی با آمدنش راهکارهای جدیدی برای هکرها ایجاد کرده است و حتی دسترسی هوش مصنوعی برای افراد می‌تواند رخنه‌های امنیتی گسترده‌ای ایجاد کند.

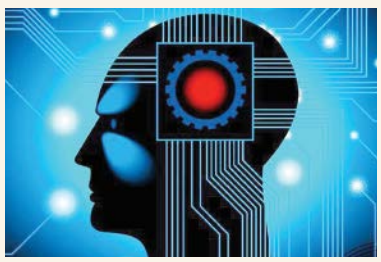
همان‌طور که می‌دانید بعضی از هوش‌های مصنوعی نیازمند استفاده از فیلترشکن است که برخی افراد سازمان برای استفاده از این موارد با روش‌های مختلف سطوح امنیتی سیستم‌ها را دور می‌زنند و باعث ایجاد شکاف‌های امنیتی در سیستم شده و راه را برای هکرها و دزدان اطلاعات باز می‌کنند.

از طرفی هوش مصنوعی یک شیوه جدید است که هنوز توسط خیلی از کارشناسان و مهندسان شناخته شده نیست و ما نمی دانیم پشت دادن امکانات رایگان و خدمات رایگان چیست؟

همان‌طور که می‌دانید خیلی از سایت‌ها به شما امکانات رایگان می‌دهند ولی بعد از ثبت نام و گرفتن اطلاعات داده‌های شما را جمع آوری و شما را در شبکه جهانی اطلاعاتی که مشخص نیست سوق می‌دهند. از طرفی دارک وب «محیطی که مخصوص هکرهاست» جایی است که اطلاعات به شیوه‌های مختلف شکار می‌شود و محتویات شما به هر شکلی مورد پژوهش و بررسی قرار می‌گیرد.

این نکته امنیتی بسیار مهم است که بدانید داده‌ها و عکس‌هایی که داخل اینترنت قرار می‌دهید با خود حاوی اطلاعاتی است که می‌تواند در ردیابی اطلاعات مشابه شما مورد توجه قرار گیرد.

با توجه به دشمنانی که هر لحظه از حمله‌های سایبری نرم استفاده می‌کنند باید در استفاده از فناوری‌های روز بیشتر به هوش باشیم و داده‌های اصلی خود را در معرض این سایت‌ها یا روش‌های هوشمند ناشناخته قرار ندهیم. پیشنهاد می‌شود سازمان‌ها بیشتر به فکر اطلاعات و خروجی‌هایی که قرار می‌دهند باشند این نکته مهم است که فقط با نصب یک آنتی‌ویروس و دیواره آتش داده‌ها، امنیت پیدا نمی‌کنند و حتما باید از راهکارهای جدید امنیتی در سراسر دنیا استفاده کرد و مدیران سایبری و شبکه دائما اطلاعاتشان باید به روز شود.



ده راه رسیدن به امنیت سایبری مناسب

این ۱۰ راه توصیه‌های NCSC (مرکز ملی امنیت سایبری) که برای کارشناسان و کارمندان فنی سازمانهای متوسط تا بزرگ فراهم شده است. با انجام این توصیه‌ها امنیت سایبری و اطلاعاتی خود را بالاتر برده و می‌توانید با دید بهتری نسبت به سیستم‌ها و سازمان خود ایجاد کنید.

۱

مدیریت ریسک

برای ایمن سازی داده و سیستمها رویکردی به کار ببرید که ریسک محور باشد اگر سیستم‌ها دچار باگ امنیتی شد بتوان از شیوه‌های دیگر کنترل روی سیستم‌ها داشته باشیم و راهکارهای دیگر را دائما بررسی کنید.

۲

مشارکت و آموزش

کارکنان را در ایجاد امنیتی مشارکت دهید تا نتیجه‌ای متناسب سازمان خودتان به دست آورید. بعضی اوقات با مشارکت کارمندان مواردی را می‌یابید که خلاهای نادیدنی امنیتی را بهتر درک می‌کنید

۳

مدیریت دارایی

■ بدانید چه داده‌ها و سیستم‌هایی دارید و بدانید چه کسب و کارهایی به آنها نیاز دارند.

یکی از مواردی که باعث باگ امنیتی می‌شود نداشتن اطلاعات درست از این موارد است و همیشه تجهیزات نرم و سخت درست با کار خود تهیه کنید.

۴

■ سیستم ام
مدیریت آن برای ش
موارد را بررسی ک
و

۸

ثبت وقایع (لاگ برداری) و پایش

■ رویدادها را شناسایی و بررسی کند.

نکته مهم این است که برای این وقایع حتما برنامه ریزی داشته باشید و تجهیزات مورد نظر را تهیه کنید. بیشتر مواقع بررسی این وقایع به شما روزنه‌ها و رخنه‌های امنیتی را خبر می‌دهد.

۹