خبرنامه هفتگی پادیوم
سال اول / شماره سی و چهارم
دوشنبه ۲۵ اسفند ماه ۱۳۹۹

پیشاپیش آغاز بهار یکهزار و چهارصد را تبریک می‌گوییم.

PODIUM.IR

#مصاحبه

دست بالای دست بسیار است!

سامانه باگ‌بانتی «راورو» در الکام‌استارز ششم، برنده جایزه «نگاه پلتفرمی» شد. راورو سامانه‌ای است که با ایجاد بستری مناسب، زمینه فعالیت علاقمندان به حوزه امنیت، هک و نفوذ را در خصوص شناسایی آسیب‌پذیری برای وب‌سایت‌ها و سامانه‌های داخل کشور فراهم کرده است. راورو علاوه بر تسهیل فرآیند کسب درآمد از طریق گزارش آسیب‌پذیری‌ها به‌صورت قانونی برای متخصصان امنیتی، به کسب‌وکارهای دولتی و شرکت‌ها در جهت افزایش امنیت و کاهش آثار مخرب حملات کمک می‌کند.

تجربه موفق جهانی در این زمینه حاکی از آن است که هزینه‌ی تمام شده برای این راهکار، به نسبت میزان کاهش آثار حملات مخرب سایبری، بسیار مناسب است. تیم راورو با استفاده از ظرفیت فنی متخصصان سایبری، در راستای افزایش امنیت در فضای سایبری، گام مثبتی برداشته است.

عصر سه‌شنبه ۱۲ اسفندماه، گپی با مدیرعامل و راهبر کسب‌وکار راورو داشتیم و از زبان خود آن‌ها درباره تجربه راورو در راستای افزایش امنیت در فضای سایبری کسب‌وکارها و نهادهای کشور شنیدیم. محمدامین کریمان و مرضیه لکزایی، مدیرعامل و راهبر کسب‌وکار راورو در این مصاحبه با ما همراه بودند.

در ابتدای صحبت از تجربیاتتان بگویید و اینکه چطور تصمیم به راه‌اندازی سامانه راورو گرفتید؟

محمدامین کریمان: داستان شکل‌گیری راورو به سال ۱۳۹۷ برمی‌گردد. من و کاظم فلاحی که جزو موسسهای اصلی راورو است، از سال ۱۳۹۰ در پروژه‌های مختلف امنیت سایبری (Cyber Security) درگیر بودیم. با توجه به تجربه‌ای که داشتیم، هم به‌صورت کارفرما و هم به‌صورت پیمان‌کار کار کرده بودیم و به نوعی هر دو سمت میز امنیت نشسته بودیم و با تمام چالش‌ها آشنایی کامل داشتیم.

سال ۱۳۹۷ در اثر هک و افشای اطلاعاتی که برای یکی از کسب‌وکارها پیش آمد و رسانه‌ای شد، همراه با یکی دیگر از محققین امنیتی، تجربه ارائه گزارش آسیب‌پذیری به یکی از آن کسب‌وکارها را داشتیم؛ اما متاسفانه آن کسب‌وکار راهکاری برای ارائه پاداش و «باگ‌بانتی» نداشت و همان‌جا جرقه راورو برایمان زده شد.

در سال ۲۰۱۲، باگ‌بانتی در سراسر جهان جا افتاده بود؛ اما در ایران شرکت‌های بسیار کمی بودند که به این مسئله اهمیت می‌دادند. به طور مثال، مجموعه کافه بازار، ابرآروان و ... به باگ‌بانتی توجه داشتند؛ اما به جز این چند مورد، این مسئله موردتوجه شرکت‌های دیگر قرار نگرفته بود. به همین دلیل، ایده راه‌اندازی پلتفرم باگ‌بانتی بومی به ذهنمان رسید و کار را از آن‌جا شروع کردیم.

تفاوت باگ‌بانتی و باگ‌هانتینگ را برای ما توضیح می‌دهید؟

محمدامین کریمان: باگ‌بانتی و باگ‌هانتینگ یک تفاوت عمده دارند. در هر دو مورد، در نهایت گزارش آسیب‌پذیری اعلام می‌شود؛ اما در باگ‌بانتی چارچوب از قبل مشخص شده است و شرکت‌ها با توجه به قوانینشان اعلام می‌کنند که اگر آسیب‌پذیری خاصی گرفته شود برایشان مهم است و حاضرند بابت آن هزینه پرداخت کنند. همچنین عنوان می‌کنند که بعضی از آسیب‌پذیری‌ها برایشان اهمیتی ندارند. در مقابل، در بحث باگ‌هانتینگ، متخصص امنیتی در اینترنت می‌گردد و اگر آسیب‌پذیری را کشف کند، از یک کانال سعی می‌کند اطلاعات را به آن کسب‌وکار ارائه بدهد. در باگ‌هانتینگ چون هیچ چارچوب و زیرساختی برای پذیرش آسیب‌پذیری در کسب‌وکار تعریف نشده، با متخصص به درستی برخورد نمی‌شود. از طرفی چون متخصص دقیقاً نمی‌داند باید چه کاری انجام بدهد، ممکن است خطوط قرمز کسب‌وکار را نقض کند که این ماجرا چالش‌های بسیاری را به وجود می‌آورد.

یعنی به نوعی کسب‌وکار می‌تواند مدعی شود که مورد حمله یا باج‌گیری واقع شده؟ در این زمینه قوانین ایران چه می‌گویند؟

محمدامین کریمیان: عموماً در باگ‌هانتینگ ادبیات مشترک بین کسب‌وکار و فرد شکل نمی‌گیرد. خیلی از کسب‌وکارها ممکن است با دریافت گزارش آسیب‌پذیری از شما تقدیر کنند؛ اما در عین حال ممکن است یک کسب‌وکار به مراجع قضایی شکایت کند؛ چون خلأ قانونی در این مسئله وجود دارد.

عموماً در دنیا در حوزه باگ‌هانتینگ، گزارش‌های آسیب‌پذیری که متخصصین به‌صورت آزاد پیدا می‌کنند، توسط نهادهای ناظر و متولی دریافت می‌شود. ما در کشور سه نهاد ناظر در زمینه امنیت اطلاعات داریم: پلیس فتا، مرکز ماهر و افتا نهاد ریاست جمهوری. این سه نهاد گزارش‌های باگ‌هانتینگ را دریافت می‌کنند و به غیر از این سه نهاد، ورود اشخاص و شرکت‌های خصوصی غیرقانونی است.

در باگ‌بانتی چارچوب کاملاً مشخص است و محدوده پرداخت تعیین شده و متخصص می‌داند کاری که انجام می‌دهد غیرقانونی نیست و کسب‌وکار می‌داند در ازای گزارش‌های آسیب‌پذیری که دریافت می‌کند باید هزینه پرداخت کند.

ارزشی که شما به‌عنوان یک پلتفرم خلق می‌کنید چیست؟ چه نگرانی‌هایی در این زمینه وجود دارد و چه راهکاری دارید؟

مرضیه لکزایی: قبل از ما تلاش‌هایی با هدف ارائه باگ‌بانتی به‌صورت پلتفرم انجام شده بود. اما مهم‌ترین مسئله در پلتفرم این است که شما زبان مشترک برای هر دو سمت پروژه داشته باشید. در واقع ما سعی می‌کنیم در مسیر باگ‌بانتی هم‌قدم و همراه متخصصان امنیت و کسب‌وکارها باشیم تا در صورت وجود چالش، با کمک هم آن را بررسی و حل کنیم.

در سمت کسب‌وکارها چطور؟ وقتی اسم «هکر» به میان می‌آید، کسب‌وکارها نگران نمی‌شوند؟

محمدامین کریمیان: از سال ۹۷ تا ۹۹ ما مشغول کار تحقیق و توسعه بودیم و چون خودمان ۱۰ سال در این حوزه کار کرده بودیم، با اکثر افراد آشنایی و ارتباط داشتیم که این باعث شد به خوبی نیازهای سمت متخصصان را درک کنیم و مسائل مهم برای آن‌ها را با حساسیت پاسخ بدهیم.

از طرف دیگر، تا اسم هکر آورده می‌شد با واکنش‌های منفی مواجه می‌شدیم. همین قضیه باعث شد ایده مفهوم ارزیابی امنیتی را با ادبیات و کلمات جدید ارائه کنیم. مثلاً به جای هکر از کلمه «شکارچی آسیب‌پذیری» استفاده کرده‌ایم یا به جای کسب‌وکار از «میدان» استفاده می‌کنیم و اسکوپ را «هدف» تعریف کردیم. هدف از به‌کارگیری ادبیات و واژه‌های جدید این بود که بتوانیم تصورات ذهنی منفی را از بین ببریم و به اعتماد و تعامل برسیم.

البته در ابتدا شرکت‌ها خیلی مقاومت داشتند؛ اما چون ما در گذشته تجربه اجرای طرح‌های امنیتی را داشتیم، دغدغه کسب‌وکارها را هم می‌فهمیدیم. سعی کردیم این دغدغه‌ها را در پلتفرم به‌طور کامل پاسخ بدهیم. خیلی از کسب‌وکارها در شروع کار نگران هستند و احساس خطر می‌کنند؛ اما بعد از گذشت یک هفته و ارسال گزارش‌ها، رضایتشان جلب می‌شود و بسیاری از مشتریانمان از طرف مشتریان اولیه ما معرفی شده‌اند.

شناخت نیاز هر دو سمت و وصل کردن نیازها در یک نقطه مشترک کار بسیار مشکلی است. حساسیت‌های زیادی در حوزه امنیت وجود دارد و پول درآوردن از این راه بسیار سخت است. برای همین ما سعی کردیم با مدل باگ‌بانتی یک منبع درآمد فریلنسری برای محققین داشته باشیم، از سمتی دیگر با هدف امن‌تر کردن کسب‌وکارها، هزینه‌های آن‌ها را در این حوزه و با روش پرداخت به ازای هر گزارش آسیب‌پذیری کاهش بدهیم.

مرضیه لکزایی :در حال حاضر، در سطح جهانی به مسئله امنیت بیش از قبل توجه می‌شود؛ چون به اصطلاح در آینده به جای جنگ فیزیکی، جنگ سایبری خواهیم داشت. برای همین باگ‌بانتی جایگاه بسیار ویژه‌تری پیدا کرده است. در سطح جهانی، در سال ۲۰۱۲ هکروان و باگ‌کرود کار را شروع کردند و امسال هم در ایران این مسئله مورد توجه زیادی قرار گرفته است و علت این است که امنیت، دغدغه شناخته شده است. راورو نیز به عنوان یکی از پلتفرم‌های باگ بانتی در کنار سایر پلتفرم‌ها برای بحث اعتمادسازی بین کسب‌وکارها و متخصصین امنیت است. همچنین بحث اعتمادسازی بین پلتفرم‌هایی مثل راورو و باگدشت در کسب‌وکارها شکل گرفته است.

چه تضمینی وجود دارد که یک کسب‌وکار، در فرآیند شناسایی آسیب، خود آسیب نبیند؟

محمدامین کریمان: اتفاقاً این نکته چالش بسیاری از کسب‌وکارها است. حقیقت این است که ما در راورو به هیچ عنوان امنیت را صددرصد تضمین نمی‌کنیم و با مشتریانمان صادقانه برخورد می‌کنیم؛ اما نکته اصلی که گفته می‌شود این است که ما یک معامله انجام می‌دهیم. یک کسب‌وکار یک سری آسیب‌پذیری‌ها دارد که خودش هم از آن‌ها خبر ندارد ما بر اساس توافقی که از قبل کردیم، با ارائه گزارشی که مناسب باشد، هزینه را دریافت می‌کنیم ولی اگر آن سند به کار کسب‌وکار نیاید هیچ هزینه‌ای پرداخت نمی‌کند.

شکارچی‌ها با هکرهای کلاه سیاه تفاوت زیادی دارند. شکارچیان، محققان امنیتی هستند، قصد کمک دارند و مشکلی برای چارچوب‌های کسب‌وکارها به وجود نمی‌آورند. ما به هر دو طرف این اطمینان را داده‌ایم. اگر شکارچی بر اساس قوانین گزارش را کامل کند، مطمئناً به پولش می‌رسد. همچنین کسب‌وکار هم، زمانی پول را پرداخت می‌کند که متخصص بر اساس قوانین رفتار کرده باشد. در نهایت این یک اتفاق برد-برد است.

ما پارامترهای مختلفی تعریف کرده‌ایم تا فرآیند کاملاً شفاف باشد. روند ارزش‌گذاری کاملاً در سایت توضیح داده شده است و راورو به عنوان واسط و شخص ثالث کار ارزیابی را انجام می‌دهد. با این روش، هر دو طرف اعتماد بیشتری می‌کنند. تمام این‌ها باعث شده تا میزان خطر احتمالی به حداقل برسد و این قضیه برای کسب‌وکار و متخصص امنیتی یک نقطه برد محسوب شود.

طبقه‌بندی شکارچیان به چه صورت انجام می‌گیرد؟ چون احراز هویت شکارچیان قطعاً اطمینان بیشتری به کسب‌وکارها می‌دهد.

مرضیه لکزایی: ما در حالت ایده‌آل دوست داریم طبقه‌بندی شکارچیان بدون سطح‌بندی انجام شود؛ اما چون پلتفرم هستیم، باید به نیازها پاسخ بدهیم. معمولاً در اوایل کار، چون کسب‌وکارها آسیب‌پذیری زیادی دارند، نیاز دارند با متخصصینی که یک درجه ماهرتر هستند کار ارزیابی را انجام دهند.

ما در سامانه، متخصصین را در سه سطح از نظر تخصص طبقه‌بندی می‌کنیم. با توجه به سابقه فعالیتی که داشتند آن‌ها را دسته‌بندی می‌کنیم و از جهتی هم آن‌ها را تایید هویت می‌کنیم. در کسب‌وکارهای دولتی حساسیت زیاد است که افراد حتماً شناخته شده باشند. متخصصانی هم که دوست داشته باشند با این کسب‌وکارها کار کنند، مدارک هویتی خودشان را برای ما ارسال می‌کنند و با آن‌ها جلسه مصاحبه هماهنگ می‌شود و بعد از اینکه تایید شدند، به‌عنوان متخصص تایید هویت شده به کسب‌وکارهایی که دوست دارند با آن‌ها کار کنند معرفی می‌شوند.

رمزنگاری تمام اطلاعات در راورو چه منفعتی برای کسب‌وکارها دارد؟

محمدامین کریمان: دست بالای دست بسیار است! ما با اینکه خودمان محقق امنیتی هستیم، می‌دانیم که یک یا چند متخصص پیدا می‌شوند که آسیب‌پذیری خود ما را کشف کنند. در سامانه ما اطلاعات آسیب‌پذیر و اطلاعات خیلی حساس از سامانه‌های دیگر تجمیع شده است. برای همین راورو هدف بسیار خوبی برای حمله است و اگر کسی به اطلاعات دیتابیس راورو دسترسی پیدا کند، مطمئناً به آسیب‌پذیری بسیاری از مشتریان راورو دسترسی پیدا کرده است.

این دغدغه را از همان ابتدا داشتیم و راه‌حل این بود که تمام اطلاعات حساس، شامل اطلاعات حیاتی کسب‌وکارها یا اطلاعات هویتی متخصصان امنیتی را به صورت استاندارد رمز کنیم و رمزنگاری شده در دیتابیس ذخیره کنیم. کسب‌وکارها یا میدان‌هایی که بخواهند از این سرویس استفاده کنند، اطلاعاتشان به شکل کاملاً رمزنگاری شده بارگذاری می‌شود. و این به عنوان شرط و مزیت اصلی پلتفرم ماست که به آن بسیار اهمیت می‌دهیم.

استاندارد ارزش‌گذاری به چه شکل بوده و چطور توسط طرفین پذیرفته می‌شود؟

محمدامین کریمان: فرمول ارزش‌گذاری ما بر اساس استانداردهای جهانی است. با استفاده از استانداردهای جهانی CVSS و VRT کار بومی‌سازی را انجام دادیم و این استانداردها را با یک فرمول ترکیب کردیم. در این فرمول از یک طرف قیمت پایه آسیب‌پذیری قرار می‌گیرد و از جهات دیگر شدت آسیب‌پذیری و اندازه کسب‌وکار وارد معادله می‌شوند. هرکدام از این اجزا پارامترهای مشخص و جداول مختص به خودشان را دارند. به ازای هرکدام، اعداد را قرار می‌دهیم و طبق فرمول محاسبه می‌کنیم و ارزش هر باگ به ازای هر کسب‌وکار محاسبه می‌شود.

در فرآیند طراحی این فرمول از متخصص‌های مختلف از جامعه هکری، جامعه شکارچیان و مدیران کسب‌وکاری نظرسنجی شده و این مدل ارزش‌گذاری، عدد نزدیکی را به دو سمت ارائه می‌کند.

اتوماسیون در راورو در چه سطحی است؟ چقدر از فرآیند خودکار انجام می‌شود؟

مرضیه لکزایی: ما در پلتفرم راورو از همان ابتدا صفر تا صد را به شکلی طراحی کردیم که کار را به‌طور خودکار جلو ببریم. البته بخش‌هایی هست که در نهایت نیاز به بحث داوری و ارزش‌گذاری دارد و برای آن قسمت‌ها از نیروی انسانی استفاده می‌کنیم.

اگر بخواهیم جریان ثبت گزارش را در نظر بگیریم، از لحظه‌ای که گزارش ثبت می‌شود تا لحظه‌ای که نهایی می‌شود، تمام مراحل تا جایی که امکان دارد به شکل خودکار انجام می‌شوند. در این فرآیند نقش نیروی انسانی را به حداقل رسانده‌ایم.

در سال‌های آتی نیز در خصوص استفاده از هوش مصنوعی و ربات‌ها بیشتر خواهید شنید. ابزارهایی که به‌صورت خودکار می‌توانند نقش‌های مختلفی را به عهده بگیرند. نقش‌هایی مثل ارزیابی امنیتی خودکار، شناسایی آسیب‌پذیری‌های جدید با استفاده از تکنیک‌های گذشته و ...

از اینکه وقت خود را به این مصاحبه اختصاص دادید، متشکریم.

#اخبار_جهان

حمله سایبری؛ بحرانی جدید برای بیمارستان‌ها

حملات سایبری علیه مراقبت‌های بهداشتی، بیماران را در معرض خطر جدی قرار داده است. موسسه CyberPeace هشدار می‌دهد که دولت‌ها باید برای کمک به مبارزه با حملات، اقدامات بیشتری انجام دهند.

صنعت مراقبت‌های بهداشتی در سال گذشته، تحت‌تاثیر همه‌گیری کرونا، تحت فشار زیادی قرار داشته است و همین امر موجب شده است تا حملات سایبری به تاسیسات مراقبتی بیشتر شود. موسسه CyberPeace، در مقاله‌ای تحت عنوان «بازی با زندگی»، استدلال می‌کند که حملات سایبری به مراقبت‌های بهداشتی، به ویژه در شرایط همه‌گیری کرونا، حمله به کل جامعه است و به طور بالقوه تهدیدهایی برای زندگی بشر ایجاد می‌کند.

یکی از مهم‌ترین دلایلی که مجرمان اینترنتی خدمات بهداشتی را هدف قرار می‌دهند، زیرساخت‌های قدیمی تاسیسات خدمات بهداشتی است. همچنین شبکه‌های بهداشتی به دلیل تنوع دستگاه‌های تخصصی متصل، از پیچیدگی بیشتری برخوردار هستند. برای مثال، استفاده از زیرساخت‌های قدیمی در سراسر شبکه باعث شد که سرویس بهداشتی ملی انگلستان (NHS) در معرض حمله باج‌افزار WannaCry قرار گیرد. هر چند قبل از این سانحه فایل patch در دسترس بود، اما با توجه به شرایط خاص مراقبت‌های پزشکی، خاموش کردن بخشی از شبکه برای اعمال به‌روزرسانی کار دشواری بود. محافظت کامل از سخت‌افزار و نرم‌افزارهای شبکه به دلیل کم بودن بودجه بخش امنیت سایبری کار دشواری است و همین امر باعث می‌شود که مجرمان سایبری به دنبال به دست آوردن پول آسان، اقدام به اخاذی از بیمارستان‌هایی کنند که شبکه آن‌ها در معرض خطر است.

SOURCE: WFMZ.COM

#اخبار_جهان

بدافزار غیرقابل‌شناسایی؛ چالش جدی امنیت سایبری

بدافزار NimzaLoader به خاطر استفاده از یک زبان برنامه‌نویسی که به ندرت توسط مجرمان اینترنتی استفاده شده، بدافزاری غیرمعمول به شمار می‌رود و این موضوع شناسایی و مقابله با این بدافزار را سخت‌تر می‌کند.

این بدافزار که توسط موسسه تحقیقاتی امنیت سایبری Proofpoint شناسایی شده، به زبان Nim نوشته شده و گمان می‌رود افرادی که این بدافزار را نوشته‌اند، امیدوار بوده‌اند که با انتخاب این زبان برنامه‌نویسی غیر معمول، کار شناسایی و تحلیل بدافزار را سخت‌تر کنند.

بدافزار NimzaLoader با هدف نفوذ به رایانه‌های مبتنی بر ویندوز طراحی شده و قابلیت اجرای دستورات را دارد. به این ترتیب افرادی که با استفاده از این بدافزار به رایانه دیگران نفوذ می‌کنند، می‌توانند کنترل سیستم را در دست بگیرند، اطلاعات حساس را به سرقت ببرند یا از آن به عنوان سکویی برای نصب بدافزارهای بیشتر استفاده کنند.

گمان می‌رود این بدافزار کار تیمی باشد که با نام TA800 شناخته می‌شوند. این گروه، صنایع مختلفی در آمریکای شمالی را هدف حملات خود قرار می‌دهد.

این احتمال وجود دارد که مجرمان اینترنتی از NimzaLoader به عنوان ابزاری برای بارگذاری بدافزارهای مخرب خود استفاده کنند.

با وجود بدافزارهای مخربی مانند NimzaLoader، توصیه می‌شود که شرکت‌ها و سازمان‌ها از ابزارهایی استفاده کنند که از رسیدن ایمیل‌های مخرب و مشکوک جلوگیری می‌کنند.

همچنین توصیه می‌شود شرکت‌ها کارکنان خود را برای شناسایی و مقابله با ایمیل‌های فیشینگ، به خصوص ایمیل‌هایی که از اطلاعات شخصی افراد برای جلب اعتماد آن‌ها استفاده می‌کنند، آموزش دهند.

SOURCE: ZDNET.COM

#اخبار_جهان

دسترسی تمامی جوانان به اینترنت؛ دغدغه بنیان‌گذاران وب

سازنده‌ی شبکه‌ی جهانی اینترنت، تیم برنرز لی، از رهبران این صنعت خواسته است تا با تضمین اینکه هر فرد جوان به شبکه وب دسترسی دارد، روی آینده سرمایه‌گذاری کنند.

در روزهای گذشته تیم برنرز لی به همراه رزماری لیث، از دیگر بنیان‌گذاران شبکه وب، در سی و دومین سالگرد ایجاد شدن این شبکه جهانی، در نامه‌ای سرگشاده به این موضوع پرداختند که یک سوم جوانان در سراسر جهان به اینترنت دسترسی ندارند و بسیاری دیگر از کمبود داده، ابزارها و ارتباط پایداری که برای استفاده‌ی حداکثری از وب موردنیاز است، رنج می‌برند.

به گفته آقای برنرز لی: «در سراسر جهان، به طور خاص افراد جوان از شبکه وب کمک می‌گیرند تا آینده‌ی بهتر و عادلانه‌تری را خلق کنند. این رهبران جوان شبکه وب را به عنوان ابزاری برای جنگیدن برای عدالت، افزایش فرصت‌ها و یافتن پاسخ‌ها برای مشکلات جدی می‌بینند.»

او عقیده دارد که سرمایه‌گذاری روی آسان‌تر کردن دسترسی به شبکه اینترنت، نوعی سرمایه‌گذاری بلندمدت برای رشد و پیشرفت نسل بعدی است و تبعات چشم‌گیر مختلفی مانند رشد اقتصادی و تقویت اجتماعی در پی خواهد داشت. با این حال، فقط دسترسی داشتن به اینترنت یا تکنولوژی کفایت نمی‌کند. بلکه این نکته باید در نظر گرفته شود که این امکانات کمک‌کننده و عادلانه باشند.

SOURCE: ZDNET.COM

#اخبار_اکوسیستم_ایران

احراز هویت از طریق هوش مصنوعی؛ از ایده تا اجرا

قوه قضاییه ایران قصد دارد با شرکت‌های دانش‌بنیان برای راه‌اندازی سیستم احراز هویت از طریق هوش مصنوعی همکاری کند. در رویداد «ارائه نیازهای فناورانه سازمان پزشکی قانونی» که در روزهای اخیر به شکل مجازی برگزار شد، توضیحات بیشتری درباره این طرح ارائه شد.

سید محمد صاحبکار، معاون برنامه‌ریزی قوه قضاییه، در این رویداد درباره طرح استفاده از هوش مصنوعی برای احراز هویت بیان کرد: «احراز هویت قوه قضاییه یکی از مواردی است که قابلیت ایجاد کسب‌وکار دارد. تا پیش از این، احراز هویت آنلاین وجود نداشت و تنها از طریق حضور فرد در دفاتر خدمات الکترونیک قوه قضائیه صورت می‌گرفت، اما با همکاری برخی از شرکت‌های دانش‌بنیان، فرآیند احراز هویت به صورت غیرحضوری و از طریق موبایل و تکنیک هوش مصنوعی انجام می‌شود، ضمن آنکه در کنار آن نیز اشتغال نیز ایجاد شده است.»

به عقیده آقای صاحبکار، شرکت‌های دانش‌بنیان می‌توانند با توان خود به قوه قضاییه در راستای این طرح کمک کنند. از سوی دیگر ارائه این پروژه به بخش دانش‌بنیان کشور نیز برای رشد این بخش سودمند خواهد بود. علاوه بر رفع نقص‌های احراز هویت بدون نیاز به سرمایه‌گذاری‌های دولتی کلان، کسب‌وکارهای دیجیتال رونق بیشتری پیدا می‌کنند و فرصت‌های شغلی مختلفی برای افراد ایجاد خواهد شد.

SOURCE: ISNA.IR

پادیوم، یک بازارچه API و خدمات دیجیتال است که می‌کوشد با ارائه خدمات و راهکارهای دیجیتال در محیطی شفاف و چابک، گامی در راستای توانمندسازی اکوسیستم دیجیتال ایران بردارد. این هفته‌نامه با هدف توسعه گفتمان دیجیتال و بانکداری باز منتشر می‌شود.

شناسنامه

تولیدشده در گروه کسب‌وکار پادیوم، تهران، اسفند ۹۹

پست الکترونیک: Info@podium.ir
تلفن تماس: ۰۲۱۸۹۵۱۸۹۸۹
نشانی: تهران، پردیس، پارک فناوری پردیس، بلوار نوآوری ۱۲، پلاک ۱۲۳
کد پستی: ۱۶۵۴۱۲۰۸۴۰

مدیر خبرنامه: ندا خراسانی
هیات تحریریه: مهدی ملکی‌فر، ثمین رادفر، رضا دهقان، نیلوفر نجیب‌نیا، ریحانه احمدی
صفحه‌آرایی: سعیده شیخ‌الاسلام