

پشت پرده حسابرسی هوشمند اینترنت؛ راهکاری برای دسترسی عادلانه یا محدودیت های طبقاتی



تحول دیجیتال در توسعه
کسب و کار:
فرصت یا چالش؟



تهدیدات امنیت سایبری
در عصر تحول دیجیتال



انعقاد تفاهم نامه «نشریه زمان تحول»
با «انجمن تحول دیجیتال»

۱۶

آقای آذری جهرمی از
توسعه پدافند غیرعامل
در زمان وزارت تان چه خبر؟

۱۲

روندهای کلیدی در حسابرسی فناوری اطلاعات در سال ۲۰۲۵:
آمادگی برای آینده ای دیجیتال

۶

حسابرسی فناوری
اطلاعات؛ ضرورت پنهان
حکمرانی دیجیتال



گفت و گو با
مدیرعامل شرکت
«مهندسی اندیشه پردازان
مبتکر»





زمان تحول

سال هجدهم - شماره ۱۹۷ - مرداد ۱۴۰۳

۲

مقاله

اول دقر

تحول دیجیتال در ایران:
گامی بلند به سوی فردا

قدرت تاب‌آوری، توسعه امن، سرعت بازیابی، تداوم کسب‌وکار همه از شاخص‌های کلیدی تحول دیجیتال امن و پایدار است. اگر این شاخص‌ها در زیرساخت‌های توسعه‌ای تحول دیجیتال مورد توجه قرار نگیرد ممکن است خروجی آن‌ها پایدار نباشد و ضمن کاهش اعتماد دیجیتال، باعث کاهش سرعت توسعه تحول دیجیتال در آینده شود. برای توسعه امن زیرساخت‌ها بویژه در حوزه سایبری و دیجیتال، چند سالی است که سازمان پدافند غیرعامل کشور به عنوان ناظر بر استانداردها، قوانین و مقررات عالی در این حوزه، اسناد بالادستی و رویه‌های اجرایی و تخصصی را در دستگاه‌های اجرایی تدوین و به آن‌ها ابلاغ کرده است. معاونت‌های مختلف سازمان و قرارگاه‌های عملیاتی تمام تلاش خود را می‌کنند تا بتوانند پارادایم توسعه پدافند غیرعامل را در سازمان‌ها توسعه دهند. اما متأسفانه با درک ناصحیح از اهمیت توسعه پدافند غیرعامل، زحمات تلاشگران این عرصه نادیده انگاشته شد.

آنچه در حوادث اخیر دیده شد حاصل کم‌کاری سازمان پدافند غیرعامل نیست؛ بلکه نتیجه تفکر غلط وزیران و مدیران و دولتمردانی است که هیچوقت فکر نمی‌کردند روزی جنگ شود و زیرساخت‌ها اینگونه مورد حمله قرار گیرد. خسارات گسترده به کسب‌وکارها، کاهش اعتماد دیجیتال، از دست دادن فرصت‌های توسعه و نیروهای متخصص همه ماحصل این تفکر غلط دولتمردان و مدیرانی است که گاهی با سُخره گرفتن ابلاغیه‌های سازمان، با هوچی‌گری و همراه کردن منتقدان ناخرد اینگونه بر اعتماد و پایداری ملی ضربه زده، و باعث خسارات گسترده به کسب‌وکارها شده‌اند. نشانه رفتن مدیران عالی سازمان پدافند غیرعامل در رسانه‌ها، شگرد فرار رو به جلوی این افراد و برخی نابخردانه و خیا‌نتکارانی است که هرگز نمی‌خواهند ایران امن به منبع ظهور برسد. اکنون بر همه اصحاب رسانه و اندیشمندان فهمیم است که وارد میدان شده و با نقد صحیح و عالمانه دستگاه‌های اجرایی، مطالبه‌گری ایران امن را از دولتمردان بر دستورکار خود قرار دهند. باشد که با همت اندیشمندان شاهد اعتلای امن ایران عزیز باشیم.

مدیر مسئول

پشت پرده «حسابرسی هوشمند اینترنت»: راهکاری برای دسترسی عادلانه یا محدودیت‌های طبقاتی

.....محمدرضا قلعه‌نوی



در جهانی که اینترنت به ستون فقرات اقتصاد دیجیتال و ارتباطات اجتماعی تبدیل شده، مدیریت و نظارت بر آن به یکی از چالش‌های کلیدی سازمان‌ها و دولت‌ها بدل گشته است. در ایران، وقایع اخیر مانند جنگ ۱۲ روزه با اسرائیل و قطعی گسترده اینترنت، بحث‌هایی درباره مفاهیمی چون «اینترنت طبقاتی»، «اینترنت اضطراری»، «شبکه ملی اطلاعات» و «اینترنت آزاد و آزادتر» را به صدر توجهات آورد. این محدودیت‌ها، که به بهانه امنیت سایبری اعمال شدند، نه‌تنها دسترسی عمومی را مختل کردند، بلکه نابرابری‌هایی در دسترسی به اینترنت ایجاد کردند که انتقادات گسترده‌ای را برانگیخت. این مقاله با نگاهی فنی و به دور از مسائل سیاسی، مزایا، معایب و راهکارهای پیاده‌سازی اینترنت حسابرسی‌شده را در سطح جهانی و ایران بررسی می‌کند.

در تعریف فنی اینترنت حسابرسی‌شده آورده شده: «سیستمی است که در آن ترافیک، داده‌ها و فعالیت‌های دیجیتال کاربران با استفاده از ابزارهای حسابرسی فناوری اطلاعات (مانند استانداردها و به روش های COBIT، ITAF، 27001 ISO/IEC و NIST) به صورت شفاف، استاندارد و عادلانه نظارت و مدیریت می‌شود. برخلاف مدل‌های فیلترینگ یا اینترنت طبقاتی که دسترسی را محدود یا اولویت‌بندی می‌کنند، این رویکرد بر سه اصل کلیدی استوار است:

- امنیت سایبری: شناسایی و خنثی‌سازی تهدیدات دیجیتال با ابزارهای تحلیلی پیشرفته؛
- دسترسی عادلانه: تضمین دسترسی یکسان برای همه کاربران، بدون تبعیض؛
- شفافیت و انطباق: رعایت استانداردهای بین‌المللی و اطلاع‌رسانی واضح به کاربران؛

این تعریف، پاسخی فنی به محدودیت‌های اخیر اینترنت در ایران است، که به جای قطعی، می‌تواند از حسابرسی فناوری اطلاعات برای مدیریت هوشمند استفاده کند.

مزایای اینترنت حسابرسی‌شده در سطح جهانی

- تقویت امنیت سایبری: ابزارهای حسابرسی مبتنی بر هوش مصنوعی (AI) می‌توانند ترافیک شبکه را تحلیل کرده و تهدیداتی مانند بدافزارها یا حملات فیشینگ را شناسایی کنند. برای مثال، سنگاپور با استفاده از سیستم‌های نظارتی مبتنی بر AI، حملات سایبری را در سال ۲۰۲۴ تا ۳۰ درصد کاهش داد.
- انطباق با استانداردها: حسابرسی اینترنت براساس استانداردهایی مانند GDPR یا 27001 ISO/IEC، حریم خصوصی و انطباق با قوانین را تضمین می‌کند.
- بهینه‌سازی زیرساخت‌ها: تحلیل داده‌های ترافیکی می‌تواند به تخصیص بهتر پهنای باند و بهبود عملکرد شبکه کمک کند. کره جنوبی با این روش، سرعت اینترنت را در سال ۲۰۲۴ بهینه کرد.

اگر اینترنت حسابرسی‌شده به درستی پیاده‌سازی شود، می‌تواند ایران را به سوی یک اکوسیستم دیجیتال امن، عادلانه و کارآمد هدایت کند. تجربه جنگ اخیر نشان داد که قطعی اینترنت نه‌تنها امنیت را تضمین نکرد، بلکه خسارات اقتصادی و اجتماعی سنگینی به بار آورد.

- مدیریت بحران دیجیتال: در شرایط بحرانی، مانند حملات سایبری، حسابرسی هوشمند می‌تواند بدون قطعی کامل، جریان داده‌ها را مدیریت کند.
- حمایت از اقتصاد دیجیتال: با تقویت زیرساخت‌های بومی و نظارت هوشمند، کشورها می‌توانند خدمات دیجیتال داخلی را بدون حذف دسترسی جهانی رشد دهند.
- محافظت از زیرساخت‌های حیاتی: در جنگ اخیر، حسابرسی هوشمند می‌توانست

بدون قطع کامل اینترنت، از شبکه‌های بانکی و زیرساخت‌های حیاتی در برابر حملات سایبری محافظت کند.

- تقویت شبکه ملی اطلاعات: حسابرسی فناوری اطلاعات می‌تواند شبکه ملی را با نظارت بر کیفیت خدمات و دسترسی عادلانه، پایدارتر کند.
- کاهش جرایم سایبری: تحلیل ترافیک با ابزارهای AI می‌تواند کلاهبرداری‌های آنلاین، که در ایران در سال ۲۰۲۴ رشد ۱۵ درصد داشت، را کاهش دهد.
- افزایش کارایی خدمات دیجیتال: نظارت هوشمند می‌تواند خدمات بومی مانند پیام‌رسان‌ها یا پلتفرم‌های تجارت الکترونیک را بهینه کند.
- چالش‌های اینترنت حسابرسی‌شده در سطح جهانی
- پیچیدگی پیاده‌سازی: استقرار سیستم‌های حسابرسی نیازمند زیرساخت‌های پیشرفته، مانند سرورهای تحلیل داده و GPU، است که هزینه‌بر و پیچیده است.
- خطر نقض حریم خصوصی: بدون پروتکل‌های شفاف، نظارت می‌تواند به جمع‌آوری غیرمجاز داده‌های کاربران منجر شود. همچنانکه چین نیز با این چالش مواجه بوده است.
- نیاز به نیروی متخصص: حسابرسی اینترنت نیازمند حساب‌رسان فناوری اطلاعات با مهارت‌های تحلیل داده و AI است، که در بسیاری از کشورها کمبود آن محسوس است.
- مقاومت کاربران: نظارت، حتی اگر شفاف باشد، ممکن است به‌عنوان محدودیت تلقی شود و اعتماد کاربران را کاهش دهد.
- کاهش رقابت‌پذیری دیجیتال: تأکید بیش‌ازحد بر خدمات داخلی می‌تواند دسترسی به ابزارهای جهانی، مانند پلتفرم‌های توسعه نرم‌افزار، را محدود کند.

چالش‌های اینترنت حسابرسی‌شده در ایران

- ضعف زیرساخت‌ها: کمبود دیتاسنترهای پیشرفته و وابستگی به فناوری‌های خارجی، اجرای حسابرسی هوشمند را دشوار کرده است.
- خطر تبعیض دیجیتال: تجربه قطعی‌های اخیر نشان داد که دسترسی محدود به برخی نهادها، نابرابری را تقویت کرد و اعتماد عمومی را کاهش داد.
- هزینه‌های اقتصادی: قطعی اینترنت در جنگ ۱۲ روزه، هر ساعت ۱.۵ میلیون دلار به اقتصاد دیجیتال زیان وارد کرد.
- کمبود داده‌های بومی: نبود مجموعه داده‌های باکیفیت برای آموزش ابزارهای AI، کارایی حسابرسی را محدود می‌کند.
- چالش‌های استانداردسازی: انطباق با استانداردهای بین‌المللی مانند 27001 ISO/IEC ایران به دلیل تحریم‌ها دشوار است.
- تجارب جهانی: الگوهایی برای ایران
- اتحادیه اروپا: GDPR نشان می‌دهد که حسابرسی داده‌ها می‌تواند بدون قطع اینترنت، حریم خصوصی و انطباق را تضمین کند. این مدل می‌تواند برای ایران الهام‌بخش باشد.
- سنگاپور: نظارت هوشمند با ابزارهای AI، امنیت سایبری را بدون محدودیت دسترسی تقویت کرده است.

- هند: با ترکیب خدمات بومی و دسترسی جهانی، اقتصاد دیجیتال خود را رشد داده، که می‌تواند الگویی برای شبکه ملی اطلاعات ایران باشد.
- استرالیا: گزارش‌های شفاف درباره نظارت سایبری، اعتماد کاربران را افزایش داده و می‌تواند برای ایران درس‌آموز باشد.
- با توجه به تجارب جهانی، ایران می‌تواند با پیاده‌سازی اینترنت حسابرسی‌شده به‌عنوان جایگزینی برای قطعی و فیلترینگ از رویکردهای فنی زیر بهره گیرد:
- استفاده از هوش مصنوعی: ابزارهای AI، مانند مدل‌های زبانی بزرگ (LLMs)، می‌توانند ترافیک شبکه را تحلیل کرده و تهدیدات سایبری را بلادرنگ شناسایی کنند.
- استانداردهای حسابرسی: پیاده‌سازی چارچوب‌های COBIT و 27001 ISO/IEC برای نظارت شفاف و استاندارد بر اینترنت.
- زیرساخت‌های بومی: سرمایه‌گذاری در دیتاسنترهای محلی و سرورهای پیشرفته برای پشتیبانی از شبکه ملی اطلاعات.
- شفافیت در نظارت: انتشار گزارش‌های منظم درباره اقدامات نظارتی برای جلب اعتماد عمومی.
- آموزش حساب‌رسان: توسعه برنامه‌های آموزشی برای حساب‌رسان فناوری اطلاعات جهت کار با ابزارهای AI و تحلیل داده.

چشم‌انداز آینده:

اگر اینترنت حسابرسی‌شده به درستی پیاده‌سازی شود، می‌تواند ایران را به سوی یک اکوسیستم دیجیتال امن، عادلانه و کارآمد هدایت کند. تجربه جنگ اخیر نشان داد که قطعی اینترنت نه‌تنها امنیت را تضمین نکرد، بلکه خسارات اقتصادی و اجتماعی سنگینی به بار آورد. با تشکیل «ستاد توسعه فناوری و کاربرد هوش مصنوعی» در ایران، فرصت برای استفاده از فناوری‌های پیشرفته در حسابرسی اینترنت فراهم است. آینده اینترنت در ایران باید بر پایه استانداردهای جهانی، دسترسی عادلانه و بهره‌وری دیجیتال بنا شود.

زمان تحول

سال هجدهم - شماره ۱۹۷ - مرداد ۱۴۰۳

۳

مقاله



نخن سردیر

«هوش مصنوعی»: انقلاب پنهان حسابرسی فناوری اطلاعات

روزگاری حسابرسی فناوری اطلاعات فرایندی پرحمت بود؛ ساعت‌ها غرق شدن در داده‌ها، بررسی دستی لاگ‌های سیستم، و جستجوی خطاها یا تقلب‌ها. حالا هوش مصنوعی مانند یک دستیار ابرقهرمان وارد صحنه شده است! الگوریتم‌های یادگیری ماشین و پردازش زبان طبیعی، میلیون‌ها تراکنش را در کسری از ثانیه کاوش می‌کنند، ناهنجاری‌ها را شکار کرده و ریسک‌های سایبری را پیش‌بینی می‌کنند. مثلاً، یک بانک می‌تواند با AI، تراکنش‌های مشکوک به پولشویی را لحظه‌ای شناسایی، و پیش از فاجعه، واکنش نشان دهد. این فناوری، زمان و هزینه‌های حسابرسی را به شکل خیره‌کننده‌ای کاهش داده و دقت را به اوج رسانده است.

AI همچنین حسابرسی مستمر را به واقعیت بدل کرده است؛ برخلاف روش‌های سنتی که حسابرسی را به دوره‌های خاص محدود می‌کرد، ابزارهای مبتنی بر AI داده‌ها را بلادرنگ تحلیل می‌کنند. این قابلیت، سازمان‌ها را قادر می‌سازد تا مشکلات را در لحظه رفع کنند و انطباق با استانداردهایی مثل GDPR یا ISO/IEC 27001 را تضمین کنند؛ اما AI هرگز جای حساب‌رسان را نگرفته؛ بلکه آن‌ها را به ستاره‌های استراتژیک تبدیل کرده است! حساب‌رسان دیگر درگیر کارهای تکراری نیستند و بر تحلیل‌های عمیق، تفسیر داده‌ها و ارائه راهکارهای بهبود تمرکز دارند. در ایران، با وجود پتانسیل بالای AI، مولعی مثل تحریم‌ها، کمبود زیرساخت‌های ابری و داده‌های باکیفیت، پیشرفت را کند کرده‌اند. اما نشانه‌های امیدبخشی وجود دارد؛ برخی سازمان‌ها از AI برای تحلیل مالیاتی یا بررسی انطباق استفاده می‌کنند. مثلاً، سیستم‌های مبتنی بر AI در سازمان امور مالیاتی، تخلفات را سریع‌تر شناسایی، و کارایی را بالا برده‌اند. با این حال، چالش‌هایی مانند سوء‌گیری الگوریتمی و امنیت داده‌ها همچنان نیازمند توجه‌اند. هوش مصنوعی، حسابرسی فناوری اطلاعات را از فرایندی واکنشی به ابزاری پیش‌بینانه و هوشمند تبدیل کرده است. این نشریه متعهد است با تحلیل‌های عمیق و داستان‌های الهام‌بخش، شما را در این سفر همراهی کند. بیا بید با AI، آینده‌ای هوشمند برای حسابرسی بسازیم!

حسابرسی فناوری اطلاعات؛ ضرورت پنهان حکمرانی دیجیتال

.....میلاد میغانی

در دنیای امروز، فناوری اطلاعات به بخش جدایی‌ناپذیری از ساختار سازمان‌ها و کسب‌وکارها از سیستم‌های مالی و زنجیره تامین گرفته تا ارتباطات داخلی و خدمات مشتری تبدیل شده است. این نفوذ همه‌جانبه باعث شده است که فناوری اطلاعات نه فقط به عنوان بخشی از عملیات سازمانی، بلکه به عنوان عاملی تعیین‌کننده در موفقیت یا شکست کل سازمان و کسب‌وکار مطرح شود. در چنین شرایطی، حسابرسی فناوری اطلاعات به عنوان ابزاری کلیدی برای شناسایی، ارزیابی و مدیریت ریسک‌های مرتبط با این حوزه، اهمیت فزاینده‌ای یافته است. در این راستا برای آشنایی بیشتر مخاطبان نشریه با مفهوم حسابرسی فناوری اطلاعات در عصر تحول دیجیتال با جناب آقای جواد رحیمی مشاور حسابرسی فناوری اطلاعات و تحول دیجیتال، عضو کمیسیون مشاوران سازمان نظام صنفی رایانه‌ای تهران به گفت‌وگو نشستیم که با هم می‌خوانیم:

لطفاً در ابتدا برای مخاطبان ما توضیح دهید که حسابرسی فناوری اطلاعات چیست و چرا امروز به یکی از موضوعات مهم در حوزه مدیریت سازمان‌ها تبدیل شده است؟

حسابرسی فناوری اطلاعات (IT Audit) فرآیندی سیستماتیک برای ارزیابی اثربخشی، امنیت، صحت عملکرد و انطباق دارایی‌های فناوریانه یک سازمان با استانداردها، سیاست‌ها و الزامات قانونی است. در دنیای امروز که تحول دیجیتال و اتوماسیون فرایندها در تمامی صنایع نفوذ کرده، ریسک‌های مرتبط با فناوری اطلاعات نیز افزایش یافته‌اند. حسابرسی فناوری اطلاعات ابزار مهمی است برای سنجش سطح بلوغ فناوریانه سازمان و محافظت از دارایی‌های اطلاعاتی، که اغلب حیاتی‌تر از دارایی‌های فیزیکی هستند.

چه ضرورت‌هایی باعث شده تا سازمان‌ها به سمت اجرای حسابرسی فناوری اطلاعات حرکت کنند؟

اولین و مهم‌ترین ضرورت، مدیریت ریسک است. تهدیدات سایبری، نشت اطلاعات، خرابکاری داخلی، و اشکالات سیستمی می‌توانند صدمات جبران‌ناپذیری وارد کنند. دوم، الزامات قانونی و انطباق با مقررات داخلی و بین‌المللی است که حسابرسی را الزام‌آور می‌کند. سوم، شفافیت و پاسخ‌گویی سازمانی که در ارزیابی عملکرد و کارآمدی واحدهای فناوری اطلاعات نقش مهمی ایفا می‌کند. چهارم، شناسایی گلوگاه‌های فناوریانه، ناکارآمدی‌ها و فرصت‌های بهبود در ساختار IT از طریق حسابرسی قابل دستیابی است. **رویکردهای نوین در حسابرسی فناوری اطلاعات کدام‌اند و چگونه می‌توان آن‌ها را در ایران پیاده‌سازی کرد؟**



رویکردهای نوین به‌جای نگاه ایستا، نگاهی پویا، داده‌محور و پیوسته دارند. مثلاً در رویکرد Continuous Auditing

داده‌ها به‌صورت بلادرنگ تحلیل و پایش می‌شوند. Audit Analytics با استفاده از تکنیک‌های داده‌کاوی، تقلب یا رفتارهای غیرعادی را شناسایی می‌کند. همچنین مدل‌های کنترل داخلی مبتنی بر Frameworkهایی مانند COBIT 2019 ، NIST CSF و ISO/IEC 27005 از ابزارهای روزآمد در این حوزه هستند. در ایران، برای پیاده‌سازی این رویکردها باید زیرساخت تحلیلی، فرهنگ نظارت‌پذیری و تخصص حرفه‌ای هم‌زمان رشد پیدا کنند.

آیا میان حسابرسی فناوری اطلاعات و امنیت سایبری تفکیکی وجود دارد؟ و چگونه این دو حوزه در عمل هم‌پوشانی پیدا می‌کنند؟

بله، این دو حوزه با وجود اشتراک زیاد، از نظر ماهیت مأموریت تفاوت دارند. امنیت سایبری بیشتر بر روی پیشگیری، شناسایی، پاسخ و بازپایی تمرکز دارد؛ در حالی که حسابرسی فناوری اطلاعات به ارزیابی اثربخشی این اقدامات و کنترل‌ها می‌پردازد. حسابرس بررسی می‌کند آیا چارچوب امنیتی تدوین‌شده اجرا شده و آیا مستندات، شواهد و فرآیندهای مربوطه قابل اتکا هستند یا خیر. در عمل، حسابرسی می‌تواند نقش ناظر مستقل بر واحد امنیت سایبری ایفا کند و نقاط کور یا خلأهای اجرایی را شناسایی نماید.

در حوزه حسابرسی فناوری اطلاعات چه تفاوتی میان حسابرسی سازمان‌های دولتی، بانک‌ها، شرکت‌های پتروشیمی یا شرکت‌های استارت‌آپی وجود دارد؟

تفاوت‌ها قابل‌توجه‌اند. در سازمان‌های دولتی بیشتر با انطباق قانونی، رعایت ضوابط افتا، سامانه‌های دولتی و

معماری سازمانی مواجه هستیم. در بانک‌ها و بیمه‌ها، ملاحظات مربوط به حریم خصوصی، ریسک عملیاتی و تطابق با مقررات نهادهای ناظر مانند بانک مرکزی و بیمه مرکزی پررنگ است. در صنایع نفت، گاز و پتروشیمی، تأکید روی دسترس‌پذیری، تاب‌آوری سیستم‌ها و امنیت عملیاتی است. در استارت‌آپ‌ها، چالش بیشتر مربوط به بلوغ پایین کنترل‌های داخلی، عدم مستندسازی مناسب و مقیاس‌پذیری زیرساخت‌هاست. بنابراین، حسابرس باید درک درستی از صنعت هدف، فرآیندهای حیاتی آن و الزامات قانونی و عملیاتی آن داشته باشد.

با توجه به گسترش فناوری‌های نوظهور مانند هوش مصنوعی، بلاک‌چین و اینترنت اشیا، حسابرسی فناوری اطلاعات چگونه باید خود را با این تحولات وفق دهد؟

ساز و کارهای سنتی حسابرسی پاسخگوی چالش‌های فناوری‌های نوین نیستند. به عنوان مثال، در سیستم‌های مبتنی بر هوش مصنوعی، باید حسابرسی مدل‌ها شفافیت تصمیم‌گیری الگوریتم‌ها بررسی شود. در حوزه بلاک‌چین، صحت قراردادهای هوشمند اهمیت دارد. در اینترنت اشیا نیز، اطمینان از صحت داده‌های ورودی، حریم خصوصی و امنیت فیزیکی-دیجیتال چالش‌برانگیز است. بنابراین، ما نیازمند توسعه چارچوب‌های نوین حسابرسی، بازتعریف نقش حسابرس در اکوسیستم دیجیتال، و ارتقای مهارت‌های تخصصی هستیم.

جایگاه حاکمیت فناوری اطلاعات (IT Governance) در فرآیند حسابرسی فناوری اطلاعات چیست و چه رابطه‌ای میان این دو برقرار است؟

حاکمیت فناوری اطلاعات ستون فقرات مدیریت منابع،

ریسک‌ها و عملکرد IT در سازمان است. چارچوب‌هایی مانند COBIT دقیقاً به تبیین این ارتباط می‌پردازند. در واقع، حسابرسی فناوری اطلاعات یک ابزار قدرتمند برای سنجش میزان اثربخشی و استقرار IT Governance است. اگر سازمانی فاقد نظام حاکمیتی شفاف باشد، حسابرسی آن صرفاً به کشف اشکالات تکنیکی محدود می‌شود. اما در سازمان‌هایی که حاکمیت قوی دارند، حسابرسی ابزاری برای بهبود راهبری، تصمیم‌گیری و شفافیت عملکرد فناوری اطلاعات خواهد بود.

شنیده‌ایم که برای نخستین بار در کشور، یک دوره DBA تخصصی در حوزه حسابرسی فناوری اطلاعات برگزار می‌شود. در این خصوص بیشتر توضیح دهید؟

بله، برای نخستین بار در کشور، دوره DBA حسابرسی

فناوری اطلاعات توسط دانشگاه صنعتی امیرکبیر و با همکاری سازمان نظام صنفی رایانه‌ای کشور برگزار می‌شود. این دوره با مشارکت اساتید برجسته حوزه IT Governance ، امنیت اطلاعات، تحلیل داده‌ها و حسابرسی طراحی شده و تمرکز آن بر توسعه مهارت‌های حرفه‌ای، کاربرد استانداردهای بین‌المللی، و تربیت حسابرسان فناوری اطلاعات در سطح استراتژیک است. این دوره نه تنها برای مدیران فناوری و کارشناسان امنیت، بلکه برای مدیران ریسک، حسابرسان داخلی، و مشاوران تحول دیجیتال نیز طراحی شده تا بتوانند با نگاهی جامع، زیرساخت‌های IT سازمان را در ابعاد مختلف ارزیابی کنند. در اولین دوره برگزاری این دوره جمعی از مشاوران سازمان نظام صنفی و مدیران و متخصصان شرکت‌های دولتی و خصوصی از صنایع مختلف بعنوان دانش‌پذیر حضور دارند.

آینده شغلی حوزه حسابرسی فناوری اطلاعات را در ایران چگونه ارزیابی می‌کنید و چه توصیه‌ای به علاقه‌مندان این حوزه دارید؟

حسابرسی IT یکی از مشاغل رو به رشد در دنیاست و در ایران نیز با افزایش ضریب نفوذ فناوری و الزاماتی همچون قانون حفاظت از داده‌ها، نیاز به حسابرسان حرفه‌ای بیشتر احساس می‌شود. شرکت‌های مالی، بانکی، بیمه و دولتی به دنبال جذب متخصصانی هستند

که هم با فناوری آشنا باشند و هم زبان حسابرسی و ریسک را بفهمند. توصیه من به علاقه‌مندان این حوزه، ترکیب دانش فنی با مهارت‌های حسابرسی و کسب دانش تخصصی

است؛ چراکه مسیر شغلی در این حوزه، پتانسیل رشد و اثرگذاری بالایی دارد.

در پایان، چه پیامی برای مدیران و تصمیم‌گیران حوزه فناوری اطلاعات دارید؟

حسابرسی فناوری اطلاعات، آینده‌نگران‌ترین ابزار برای حفاظت از دارایی‌های دیجیتال، ارتقای پاسخ‌گویی، و بهبود مستمر ساختار IT است.

سازمان‌هایی که امروز سرمایه‌گذاری در این حوزه را آغاز کنند، نه‌تنها در برابر ریسک‌ها مقاوم‌ترند، بلکه در مسیر تحول دیجیتال نیز موفق‌تر خواهند بود.

پیشنهاد من این است که مدیران، آموزش کارشناسان از طریق آموزش‌های تخصصی را در اولویت قرار دهند و با نهادهای سازشی رویکرد حسابرسی مستمر، بلوغ دیجیتال سازمان را به سطح بالاتری برسانند.

.....را حله جمعه زاده بهابادی

در دنیای امروز که فناوری با سرعتی بی‌سابقه در حال پیشرفت است، حسابرسی فناوری اطلاعات (IT Audit) نیز دستخوش تحولات عمیقی شده است. سال ۲۰۲۵ نقطه عطفی برای این حوزه به شمار می‌رود؛ چرا که پیشرفت‌های فناورانه، الزامات نظارتی پیچیده‌تر و افزایش تهدیدات سایبری، نقش حسابرسان فناوری اطلاعات را بیش از پیش حیاتی و چالش‌برانگیز کرده است. براساس گزارش‌های معتبر از مؤسسات پیشرو مانند Deloitte، KPMG، Gartner و AuditBoard، پنج روند کلیدی آینده این حوزه را شکل می‌دهند. ۱. استفاده گسترده از هوش مصنوعی و تحلیل داده‌ها: از اتوماسیون تا پیش‌بینی ریسک

یکی از مهم‌ترین تحولات در حسابرسی فناوری اطلاعات، بهره‌گیری روزافزون از هوش مصنوعی (AI) و ابزارهای تحلیل داده‌های پیشرفته است. این فناوری‌ها دیگر تنها ابزارهایی کمکی نیستند، بلکه به هسته فرآیندهای حسابرسی نوین تبدیل شده‌اند.

اتوماسیون وظایف تکراری: هوش مصنوعی قابلیت خودکارسازی حجم عظیمی از وظایف تکراری و زمان‌بر مانند استخراج، پاک‌سازی و تطبیق داده‌ها را فراهم می‌کند.

این امر به حسابرسان اجازه می‌دهد تا زمان انرژی خود را بر روی فعالیت‌های با ارزش‌تر مانند ارزیابی ریسک‌های پیچیده، تجزیه و تحلیل یافته‌ها و ارائه مشاوره‌های استراتژیک متمرکز کنند.

تحلیل پیشرفته داده‌ها و پیش‌بینی ریسک: با استفاده از الگوریتم‌های یادگیری ماشین و تکنیک‌های تحلیل داده‌های بزرگ (Big Data)، حسابرسان می‌توانند الگوهای ناهنجار و انحرافات را در حجم وسیعی از داده‌ها شناسایی کنند که پیش از این امکان‌پذیر نبود.

روندهای کلیدی در حسابرسی فناوری اطلاعات در سال ۲۰۲۵:

آمادگی برای آینده‌ای دیجیتال



۲. تمرکز بی‌سابقه بر امنیت سایبری و حاکمیت داده‌ها: دفاع در برابر تهدیدات فزاینده در عصری که حملات سایبری پیچیده‌تر و فراگیرتر شده‌اند، امنیت سایبری و حاکمیت داده‌ها به محور اصلی فعالیت‌های حسابرسی فناوری اطلاعات تبدیل شده‌اند.

افزایش تهدیدات سایبری و اولویت حسابرسی: با توجه به آسیب‌پذیری فزاینده سازمان‌ها در برابر حملات باج‌افزار، فیشینگ و نشت اطلاعات، حسابرسی امنیت اطلاعات به یک اولویت استراتژیک بدل گشته است. حسابرسان نه تنها باید کنترل‌های امنیتی موجود را ارزیابی کنند، بلکه باید توانایی ارزیابی آمادگی سازمان در برابر تهدیدات جدید و توانایی پاسخگویی مؤثر به حوادث امنیتی را نیز داشته باشند.

حاکمیت داده‌ها و الزامات نظارتی: مقررات جدید حفاظت از داده‌ها مانند GDPR و CCPA، سازمان‌ها را ملزم به پیاده‌سازی سیاست‌های قوی در زمینه حاکمیت، حفظ و محرمانگی داده‌ها کرده‌اند. حسابرسان فناوری اطلاعات نقش حیاتی در اطمینان از انطباق سازمان‌ها با این مقررات و اجرای صحیح سیاست‌های حاکمیت داده‌ها ایفا می‌کنند.

۳. ارزیابی راهبردهای ابری و فناوری‌های نوظهور: همگامی با پیشرفت‌های فناوری‌های گسترش چشمگیر رایانش ابری و ظهور فناوری‌های نوین، چالش‌های جدیدی را برای حسابرسان فناوری اطلاعات به ارمغان آورده است.

۴. مدیریت ریسک‌های فناوری‌های ابری: با مهاجرت سازمان‌ها به پلتفرم‌ها و خدمات ابری (Cloud Services)، حسابرسان باید تخصص لازم برای ارزیابی ریسک‌های مرتبط با امنیت داده‌ها در محیط‌های ابری، انطباق با مقررات در سطح بین‌المللی و مدیریت قراردادهای ارائه‌دهندگان خدمات ابری را کسب کنند.

این شامل درک مدل‌های مسئولیت مشترک در ابر و اطمینان از پیاده‌سازی کنترل‌های مناسب توسط هر دو طرف است. هوش مصنوعی مولد و اینترنت اشیا (IoT): ظهور فناوری‌هایی مانند هوش مصنوعی مولد (Generative AI) که در تولید محتوا و کد نقش دارند، و همچنین اینترنت اشیا که منجر به اتصال میلیاردها دستگاه به شبکه می‌شود، نیازمند ارزیابی ریسک‌های جدیدی هستند. حسابرسان باید روش‌های خود را برای پوشش این فناوری‌ها، از جمله ریسک‌های حریم خصوصی، امنیت داده‌های حجیم و مسائل اخلاقی، تطبیق دهند.

۵. تطبیق با استانداردها و مقررات جدید: حرکت در محیطی پویا، محیط نظارتی و استانداردهای حرفه‌ای در حوزه حسابرسی فناوری اطلاعات به طور مداوم در حال تغییر و تکامل هستند.

۶. استانداردهای جدید حسابرسی داخلی: مؤسسات حسابرسی داخلی با استانداردهای جدیدی مواجه هستند که بر هم‌راستایی استراتژیک حسابرسی با اهداف کلی سازمان و همچنین بر ارزیابی جامع ریسک‌ها تأکید دارند. حسابرسان باید رویکردهای خود را برای انطباق با این تغییرات و ارائه ارزش بیشتر به ذینفعان بازنگری کنند. ۷. مقررات متغیر و الزامات انطباق: محیط نظارتی پیچیده و متغیر، از جمله مقررات خاص صنعت و الزامات گزارش‌دهی جدید، حسابرسان را ملزم می‌کند که به طور مداوم دانش خود را به‌روز نگه دارند و روش‌های حسابرسی خود را مطابق با آخرین الزامات تنظیم کنند. عدم انطباق می‌تواند منجر به جریمه‌های سنگین و آسیب به اعتبار سازمان شود.

۸. توسعه مهارت‌های جدید و جذب استعدادها: روندهای فوق، نیاز مبرم به توسعه مهارت‌های جدید در حسابرسان فناوری اطلاعات و جذب استعدادهای متخصص را برجسته می‌سازند. حسابرسان آینده باید دارای مهارت‌های قوی در تحلیل داده‌ها، آشنایی عمیق با معماری سیستم‌های اطلاعاتی، دانش کافی در مورد امنیت سایبری و درک درستی از فناوری‌های نوظهور باشند. این شامل توانایی کدنویسی پایه، استفاده از ابزارهای تحلیل داده و درک مفاهیم بلاکچین و رایانش کوانتومی می‌شود.

جمع‌بندی

حسابرسی فناوری اطلاعات در سال ۲۰۲۵، فراتر از یک وظیفه سنتی، به یک کارکرد استراتژیک تبدیل شده است که نقشی حیاتی در تضمین تاب‌آوری، امنیت و موفقیت سازمان‌ها در چشم‌انداز دیجیتال ایفا می‌کند. با پذیرش هوش مصنوعی و تحلیل داده‌ها، تمرکز بر امنیت سایبری و حاکمیت داده‌ها، ارزیابی دقیق فناوری‌های ابری و نوظهور، تطبیق با مقررات جدید و سرمایه‌گذاری در توسعه مهارت‌های نیروی انسانی، حسابرسان فناوری اطلاعات می‌توانند به عنوان شریکان استراتژیک در تحول دیجیتال سازمان‌ها عمل کنند و ارزش بی‌سابقه‌ای را ارائه دهند.



چه خبر از دنیای فناوری؟

پیام‌رسانی حتی بدون اینترنت؟! بیت‌چت معرفی شد!

+جک دورسی (هم‌بنیان‌گذار توییتر) از یه اپ پیام‌رسان جدید به اسم Bitchat رونمایی کرده است. پیام‌رسانی غیرمتمرکز که حتی بدون اینترنت هم کار می‌کند! -چطوری ممکنه؟

+با استفاده از فناوری بلوتوث کم‌مصرف (BLE) و ایجاد یه شبکه مش (Mesh) بین دستگاه‌ها، پیام‌ها مستقیماً بین کاربرها جابه‌جا می‌شن - بدون نیاز به سرور، شماره تلفن یا حتی اکانت!

-امنیتش چطوره؟

+رمزنگاری سرتاسری (E2EE)

پیام‌ها فقط روی خود دستگاه ذخیره می‌شن...

اگه کسی آفلاینه، سیستم به‌صورت موقت پیام رو نگه می‌داره و بعد تحویل می‌ده (store & forward)

معرفی Onit-AI دسترسی به همه چت بات‌ها، حتی آفلاین!!!

اگه به یه جایگزین متن‌باز برای ChatGPT و کلی هوش مصنوعی دیگه نیاز داری که روی دستکاپ اجرا بشه و حتی آفلاین هم کار کنه، Onit-AI یه گزینه عالیه!

← ویژگی‌های باحال Onit-AI:

- حالت آفلاین
- متن‌باز و رایگان
- پشتیبانی از مدل‌های مختلف
- مثل Anthropic، Google AI، xAI و بقیه ...

ترکیب هوش مصنوعی و هولوگرام برای رمزگذاری غیرقابل هک

+ محققان جدیداً با ترکیب هوش مصنوعی و هولوگرام‌های تولید شده با لیزر، یک سیستم رمزگذاری «غیرقابل هک» ایجاد کردن!!

- چطوری؟

+ دانشمندی یونانی یه سیستم رمزگذاری نوری را توسعه دادن که می‌تونه روش‌های هک سنتی رو منسوخ کنه.

برخلاف روش‌های رمزگذاری سنتی، که به الگوریتم‌های ریاضی متکی هستن، این رویکرد نوری از خواص فیزیکی نور استفاده می‌کنه و اون رو در برابر حملات حتی پیشرفته‌ترین کامپیوترها، از جمله ماشین‌های کوانتومی، مقاوم می‌کنه.

تحول دیجیتال در توسعه کسب و کار: فرصت یا چالش؟



..... سیده سمیه حبیب‌اله پور
امروزه تحول دیجیتال برای همه مشاغل از کسب و کارهای کوچک گرفته تا شرکت‌ها و کارخانه‌های بزرگ به یک امر ضروری تبدیل شده است. اما موضوعی که وجود دارد اینکه بسیاری از صاحبان کسب و کارهای کوچک و بزرگ هنوز به شناخت مناسبی درباره مفهوم تحول دیجیتال یا دیجیتالی شدن فرایندهای کسب و کار دست پیدا نکرده‌اند. در همین راستا در گفت‌وگوی اختصاصی با نیما رحیمی، مشاور مدیریت در حوزه توسعه کسب و کار و بازاریابی و عضو کمیسیون مشاوران سازمان نظام صنفی رایانه‌ای استان تهران، ضمن تشریح مفهوم تحول دیجیتال در توسعه کسب و کار به بررسی فرصت‌ها و چالش‌های آن می‌پردازیم.

سیاس‌گزار از وقتی که در اختیار نشریه زمان تحول قرار دادید. به عنوان اولین سوال بفرمائید چرا تحول دیجیتال برای سازمان‌ها دارای اهمیت است؟

تحول دیجیتال فقط استفاده از فناوری‌های جدید نیست، بلکه تغییری اساسی در مدل‌های کسب و کار و نحوه تعامل با مشتریان است. ما در عصری زندگی می‌کنیم که رفتار مشتریان به سرعت تغییر می‌کند. انتظارات مشتریان امروزی با ده سال پیش کاملاً متفاوت است. آن‌ها انتظار دارند خدمات سریع‌تر، شخصی‌سازی‌شده‌تر و باکیفیت‌تری دریافت کنند. سازمان‌هایی که نتوانند این تغییرات را بپذیرند، مزیت رقابتی خود را از دست خواهند داد. تحول دیجیتال به کسب و کارها کمک می‌کند تا فرآیندهایشان را بهینه کنند، هزینه‌ها را کاهش دهند و فرصت‌های جدیدی برای رشد ایجاد کنند. به همین دلیل، تحول دیجیتال دیگر یک انتخاب نیست، بلکه یک ضرورت است.

امروزه مفاهیم دیجیتالی‌سازی، دیجیتال‌سازی و تحول دیجیتال زیاد به گوش می‌رسد، آیا این مفاهیم دارای یک مفهوم هستند؟

این سه مفهوم اغلب به جای یکدیگر استفاده می‌شوند، اما در واقع تفاوت‌های اساسی دارند که شناخت آن‌ها برای سازمان‌ها بسیار مهم است: دیجیتالی‌سازی Digitization ابتدایی‌ترین سطح از ورود به دنیای دیجیتال است و به تبدیل اطلاعات فیزیکی به فرمت دیجیتال اشاره دارد. به عنوان مثال، تبدیل اسناد کاغذی به فایل‌های PDF یا دیجیتالی کردن داده‌های بانکی. در این سطح، کسب و کار هنوز مدل عملیاتی خود را تغییر نداده و فقط از ابزارهای دیجیتال برای کارهای سنتی استفاده می‌کند. اما دیجیتال‌سازی Digitalization شامل استفاده از فناوری‌های دیجیتال برای بهینه‌سازی و خودکارسازی فرآیندهای کسب و کار است. برای مثال، سازمانی که قبلاً سفارش‌های مشتریان را به صورت دستی ثبت می‌کرد، با پیاده‌سازی یک نرم‌افزار CRM، فرآیند مدیریت مشتری را بهینه می‌کند. در این سطح، بهره‌وری افزایش می‌یابد، اما مدل کسب و کار هنوز دگرگون نشده است.

و در نهایت تحول دیجیتال Digital Transformation این مرحله فراتر از دیجیتال‌سازی است و شامل تغییرات بنیادی در مدل کسب و کار، فرآیندها و نحوه ارائه ارزش به مشتریان می‌شود. در این مرحله، فناوری نه تنها برای بهینه‌سازی بلکه برای ایجاد مزیت رقابتی جدید و خلق ارزش‌های نوین استفاده می‌شود. برای مثال، اسنپ نه تنها فرآیند رزرو تاکسی را دیجیتالی کرده، بلکه کل مدل سنتی تاکسی‌رانی را با استفاده از فناوری بازتعریف کرده است.

بنابراین می‌توان گفت تحول دیجیتال فقط یک ابزار نیست؛ بلکه مستلزم تغییر فرهنگ سازمانی، توسعه مهارت‌های جدید و استفاده از فناوری به عنوان یک عامل استراتژیک است. سازمان‌هایی که به درستی این مراحل را طی کنند، می‌توانند در رقابت باقی بمانند، در حالی که شرکت‌های سنتی که تنها به دیجیتال‌سازی فرآیندها بسنده کنند، در بلندمدت آسیب خواهند دید.

چگونه می‌توان از داده‌ها در تحول دیجیتال بهره برد؟

داده‌ها امروز به یکی از ارزشمندترین دارایی‌های هر سازمان تبدیل شده‌اند. اما تفاوت اصلی بین سازمان‌های پیشرو و سایر شرکت‌ها در این است که چگونه این داده‌ها را پردازش، تحلیل و به تصمیم‌گیری‌های استراتژیک تبدیل می‌کنند.

۱. تصمیم‌گیری داده‌محور (Data-Driven Decision Making)

سازمان‌های موفق از داده‌ها برای تصمیم‌گیری‌های دقیق‌تر و مؤثرتر استفاده می‌کنند. به عنوان مثال، شرکت‌های بیمه با استفاده از تحلیل داده‌های مشتریان، ریسک‌های بیمه‌ای را بهتر ارزیابی کرده و مدل‌های قیمت‌گذاری بهینه‌تری ارائه می‌دهند.

۲. شخصی‌سازی تجربه مشتری (Personalization)

داده‌ها به سازمان‌ها کمک می‌کنند تا نیازهای مشتریان را بهتر درک کنند و تجربه‌ای شخصی‌سازی‌شده ارائه دهند. برای مثال، پلتفرم‌هایی مانند نتفلیکس و اسپاتیفای با استفاده از الگوریتم‌های یادگیری ماشین، محتوای پیشنهادی را براساس رفتار کاربران تنظیم می‌کنند که این امر باعث افزایش تعامل و وفاداری کاربران می‌شود.

۳. بهینه‌سازی عملیات سازمانی

تحلیل داده‌های داخلی می‌تواند به سازمان‌ها در بهینه‌سازی عملیات کمک کند. مثلاً در صنعت خرده‌فروشی، شرکت‌ها از تحلیل داده‌ها برای مدیریت موجودی، پیش‌بینی تقاضا و بهینه‌سازی زنجیره تأمین استفاده می‌کنند که منجر به کاهش هزینه‌ها و افزایش بهره‌وری می‌شود.

۴. تحلیل پیش‌بینی‌کننده (Predictive Analytics)

با استفاده از داده‌های گذشته و مدل‌های یادگیری ماشین، سازمان‌ها می‌توانند روندهای آینده را پیش‌بینی کنند. برای مثال، بانک‌ها از تحلیل پیش‌بینی‌کننده برای شناسایی

مشتریانی که احتمالاً به سمت رقبا خواهند رفت استفاده می‌کنند و با ارائه پیشنهادها و ویژه، نرخ حفظ مشتریان را افزایش می‌دهند. در نهایت، بهره‌گیری از داده‌ها در تحول دیجیتال نیازمند زیرساخت‌های قوی، استفاده از فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین و همچنین یک فرهنگ سازمانی داده‌محور است که تصمیم‌گیری‌ها را بر اساس شواهد واقعی، نه حدس و گمان، هدایت کند.

نقش نیروی انسانی در پیاده‌سازی سیستم‌های اطلاعاتی و تحول دیجیتال چگونه است؟

تحول دیجیتال یک پروژه مقطعی نیست، بلکه یک تغییر مستمر و استراتژیک در سازمان است که نیاز به تیمی متخصص با مهارت‌های چندبعدی دارد. برخی از نقش‌های کلیدی در این مسیر عبارت‌اند از:

۱. مدیر تحول دیجیتال که مسئول هدایت استراتژی تحول دیجیتال در سازمان است و باید بین فناوری، فرهنگ سازمانی و اهداف تجاری تعادل برقرار کند.

۲. متخصص داده و هوش تجاری که مسئول تحلیل داده‌ها، استخراج الگوها و ارائه بینش‌های قابل اجرا برای بهبود تصمیم‌گیری‌های سازمان است.

۳. معمار فناوری؛ وظیفه طراحی و پیاده‌سازی زیرساخت فناوری مناسب را دارد تا سازمان بتواند از فناوری‌های دیجیتال به‌صورت یکپارچه استفاده کند.

۴. متخصص تجربه مشتری که یکی از مهم‌ترین جنبه‌های تحول دیجیتال است. این فرد مسئول بهبود نقاط تماس دیجیتال مشتریان و طراحی سفر مشتری به‌صورت دیجیتالی و یکپارچه است. ۵. کارشناس امنیت سایبری که افزایش وابستگی به فناوری‌های دیجیتال، سازمان‌ها را در معرض تهدیدات امنیتی قرار می‌دهد. این نقش برای حفاظت از داده‌های حساس و جلوگیری از حملات سایبری حیاتی است.

اهمیت مشاوره توسعه کسب و کار در کنار مشاوره فنی و فناوری اطلاعات چیست؟

نقش مشاوران در این مسیر بسیار حیاتی است. بسیاری از شرکت‌ها درک دقیقی از مسیر تحول دیجیتال ندارند و ممکن است سرمایه‌گذاری‌های اشتباهی انجام دهند؛ در واقع سازمان‌ها تصور می‌کنند تنها با پیاده‌سازی راهکارهای فناوری، می‌توانند به موفقیت برسند. در حالی که تحول دیجیتال

یک پروژه فناوری نیست، بلکه یک تحول در مدل کسب و کار و فرهنگ سازمانی است. مشاوره فنی و فناوری به سازمان‌ها کمک می‌کند تا زیرساخت‌های مناسب را انتخاب و پیاده‌سازی کنند، اما اگر این تغییرات با یک استراتژی کسب و کار هماهنگ نباشد، نه تنها تأثیر مثبتی نخواهد داشت، بلکه ممکن است باعث هدررفت منابع شود.

برای مثال، سازمانی که یک CRM (مدیریت ارتباط با مشتری) خریداری می‌کند، اما استراتژی مشخصی برای ارتباط با مشتریان ندارد، از این ابزار بهره‌برداری مناسبی نخواهد کرد. بنابراین، ترکیب مشاوره توسعه کسب و کار با مشاوره فناوری اطلاعات، باعث می‌شود که فناوری به‌عنوان یک ابزار در خدمت اهداف سازمانی قرار گیرد، نه صرفاً یک هزینه اضافی.

جایگاه هوش مصنوعی را در تحول دیجیتال چگونه می‌بینید؟

بی‌شک هوش مصنوعی یکی از مهم‌ترین پیشران‌های تحول دیجیتال است. این فناوری می‌تواند در سه سطح کلیدی بهینه‌سازی فرآیندها، تصمیم‌گیری هوشمند و شخصی‌سازی تجربه مشتری به کسب و کارها کمک کند. با این حال، موفقیت در

استفاده از هوش مصنوعی نیازمند داده‌های باکیفیت و استراتژی مناسب است. اگر سازمانی داده‌های نادرست یا ناقص داشته باشد، نتایج تحلیل‌های هوش مصنوعی نیز غیرقابل اعتماد خواهند بود.

تحول دیجیتال در کدام صنایع بیشترین تأثیر را داشته است؟

تحول دیجیتال در بسیاری از صنایع تأثیرگذار بوده است، اما به نظر من در صنایع لجستیک، فولاد و معدن، خودروسازی، ساختمان و FMCG تغییرات ساختاری و عمیق‌تری ایجاد کرده است.

چه چالش‌هایی در مسیر تحول دیجیتال کسب و کارها وجود دارد؟

چالش‌های زیادی در این مسیر وجود دارد، اما مهم‌ترین آن‌ها عبارت از مقاومت در برابر تغییر، نبود استراتژی مشخص و مشکلات فنی و زیرساختی است. برخی از تهدیدهای احتمالی عبارت‌اند از:

۱. سرمایه‌گذاری اشتباه: اگر یک سازمان بدون شناخت دقیق از نیازهایش، روی فناوری‌های نادرست سرمایه‌گذاری کند، نه تنها نتیجه مطلوبی نخواهد گرفت، بلکه منابع مالی خود را نیز هدر می‌دهد.

۲. افزایش پیچیدگی فرآیندها: اگر فرآیندهای سازمان به‌درستی دیجیتالی نشوند، ممکن است پیچیده‌تر از قبل شوند و کارایی کاهش یابد.

۳. مقاومت کارکنان: اگر فرهنگ سازمانی آماده پذیرش تغییر نباشد، کارکنان در برابر فناوری‌های جدید مقاومت خواهند کرد که باعث شکست پروژه می‌شود.

۴. مشکلات امنیتی: افزایش وابستگی به فناوری‌های دیجیتال می‌تواند سازمان را در برابر حملات سایبری آسیب‌پذیرتر کند.

آینده تحول دیجیتال را چطور می‌بینید؟

از دیدگاه من، آینده تحول دیجیتال را می‌توان در سه روند کلیدی خلاصه کرد:

۱. افزایش هوشمندسازی کسب و کارها: استفاده از هوش مصنوعی، یادگیری ماشین و اتوماسیون هوشمند، کسب و کارها را کارآمدتر و رقابتی‌تر خواهد کرد.

۲. تمرکز بر تجربه مشتری: شرکت‌هایی که بتوانند تعاملات دیجیتالی خود را شخصی‌سازی کنند، برنده بازار خواهند بود. آینده متعلق به برندهایی است که نه تنها محصول، بلکه یک تجربه منحصر به فرد به مشتری ارائه می‌دهند.

۳. افزایش اهمیت امنیت سایبری و حریص خصوصی: با رشد داده‌های دیجیتالی، نیاز به راهکارهای امنیتی پیشرفته‌تر بیشتر خواهد شد. سازمان‌ها باید اطمینان حاصل کنند که اطلاعات مشتریان‌شان در برابر تهدیدات سایبری محافظت می‌شود. در مجموع، تحول دیجیتال دیگر یک انتخاب نیست، بلکه یک الزام برای بقا و رشد در دنیای کسب و کار است. سازمان‌هایی که سریع‌تر و هوشمندانه‌تر این مسیر را طی کنند، حتماً در آینده موفق‌تر خواهند بود.

در پایان برای سازمان‌هایی که می‌خواهند تحول دیجیتال را شروع کنند، چه توصیه‌ای دارید؟

اول اینکه تحول دیجیتال یک پروژه کوتاه‌مدت نیست، بلکه یک مسیر بلندمدت است که نیاز به برنامه‌ریزی دقیق دارد؛ بنابراین سازمان‌ها باید یک استراتژی مشخص داشته باشند. دوم اینکه روی نیازهای واقعی کسب و کار تمرکز کنند؛ چرا که هر تغییری باید به بهبود عملکرد سازمان و ایجاد ارزش برای مشتری منجر شود. و سوم موضوع آموزش تیم‌هاست؛ فناوری‌ها به تنهایی نمی‌توانند یک کسب و کار را متحول کنند، بلکه افراد سازمان باید آمادگی پذیرش تغییر را داشته باشند.

در گفت‌وگو با مدیرعامل شرکت «مهندسی اندیشه پردازان مبتکر» مطرح شد: تحول ابزارهای پرداخت الکترونیک از کارتخوان تا بلاک چین



.....دکتر کارن خاقان

صنعت پرداخت الکترونیک طی دهه‌های اخیر، مسیری پرشتاب از فناوری‌های ابتدایی تا نوآوری‌های پیشرفته را پیموده است.

این تحولات نه تنها تجربه کاربران را متحول کرده، بلکه مدل‌های کسب‌وکار و زیرساخت‌های مالی را نیز دگرگون ساخته است. در این مقاله، نسل‌های مختلف ابزارهای پرداخت را از گذشته تا آینده مرور، و چشم‌انداز این صنعت را بررسی خواهیم کرد.

نسل اول: کارتخوان‌های سنتی و کارت‌های مغناطیسی

آغاز صنعت پرداخت الکترونیک با کارتخوان‌های ساده و کارت‌های مغناطیسی رقم خورد. این دستگاه‌ها نخستین گام برای انتقال پول به شیوه‌ای امن‌تر و سریع‌تر نسبت به پول نقد بودند. اما محدودیت‌هایی چون امنیت پایین، سرعت پردازش اندک و ابعاد بزرگ دستگاه‌ها، چالش‌های جدی این نسل به شمار می‌رفت.

نسل دوم: کارت‌های هوشمند و امنیت بالاتر

با ظهور کارت‌های هوشمند (چیپ‌دار)، امنیت تراکنش‌ها به‌طور چشمگیری افزایش یافت. این کارت‌ها با تراشه‌های رمزنگاری‌شده، اطلاعات را به‌صورت ایمن‌تری ذخیره می‌کردند و سرعت پردازش نیز بهبود یافت. البته، نیاز به دستگاه‌های جدیدتر و هزینه‌های پیاده‌سازی، موانعی برای پذیرش گسترده‌تر این نسل بود.

نسل سوم: پرداخت‌های موبایلی و آنلاین

ورود پرداخت‌های موبایلی و آنلاین، نقطه عطفی در تجربه کاربران ایجاد کرد. اپلیکیشن‌هایی مانند PayPal، Apple Pay و Google Pay امکان انجام تراکنش‌ها را از هر نقطه و در هر زمان فراهم ساختند. هرچند، وابستگی به اینترنت و دغدغه‌های امنیتی، چالش‌هایی بودند که باید مدیریت می‌شدند.

نسل چهارم: پرداخت‌های بدون تماس (NFC)

با توسعه فناوری NFC، پرداخت‌ها بیش از پیش ساده و سریع شدند. کافی است کارت یا گوشی هوشمند را به دستگاه نزدیک کنید تا تراکنش در کسری از ثانیه انجام شود. این نسل، تجربه‌ای راحت و مدرن برای مصرف‌کنندگان به ارمغان آورد، اما نیاز به زیرساخت‌های جدید و دستگاه‌های سازگار با NFC، همچنان مطرح بود.

هوش مصنوعی و تحلیل کلان‌داده‌ها، وارد مرحله‌ای عمیق‌تر و در عین حال پیچیده‌تر خواهد شد. در سیستم‌های مبتنی بر اینترنت اشیا مالی، دستگاه‌هایی چون خودروهای هوشمند، یخچال‌ها یا حتی گجت‌هایی مانند ساعت‌های هوشمند، قادر خواهند بود به صورت خودکار تراکنش‌های مالی را انجام دهند. برای مثال، یک خودروی برقی می‌تواند به محض ورود به ایستگاه شارژ، هزینه را بدون دخالت انسان پرداخت کند. این مدل، که در کشورهای پیشرو مانند ژاپن، کره جنوبی و آلمان در حال توسعه است، می‌تواند سبک زندگی مردم و نحوه تعامل آن‌ها با خدمات مالی را متحول کند. از سوی دیگر، شرکت‌های فین‌تک، با تمرکز بر کلان‌داده‌ها (Big Data) و الگوریتم‌های یادگیری ماشین، مدل‌های رفتاری مشتریان را تحلیل کرده و راهکارهای پرداخت شخصی‌سازی‌شده ارائه می‌دهند. برای مثال، اپلیکیشن‌هایی مانند Klarna یا Affirm در اروپا و آمریکا، امکان خرید اقساطی یا پرداخت مبتنی بر امتیاز اعتباری لحظه‌ای را فراهم کرده‌اند؛ آن هم بدون نیاز به زیرساخت‌های سنتی بانکداری. این پلتفرم‌ها، با تحلیل رفتارهای پرداخت مشتریان، الگوهای جدیدی از اعتبارسنجی و پرداخت را خلق کرده‌اند که بر پایه اعتماد دیجیتال و سرعت بالا بنا شده‌اند.

یکی دیگر از روندهای قابل توجه، تلفیق فناوری واقعیت افزوده و پرداخت الکترونیک است. فروشگاه‌های آینده ممکن است کاملاً مجازی و مبتنی بر متاورس باشند، جایی که مشتری با انتخاب یک کالا در دنیای سه‌بعدی، مستقیماً از طریق کیف پول دیجیتال خود در همان فضا پرداخت را انجام دهد. شرکت‌هایی مانند Amazon و Meta در حال سرمایه‌گذاری گسترده روی چنین تجربه‌هایی هستند. البته، تمام این تحولات مستلزم ایجاد زیرساخت‌های فناورانه، چارچوب‌های رگولاتوری هوشمند و آموزش مستمر به کاربران است. مسئله حریم خصوصی، امنیت داده‌ها و پاسخگویی حقوقی در محیط‌های غیرمتمرکز از دغدغه‌های جدی این افق نوین هستند.

جمع‌بندی

تحول صنعت پرداخت الکترونیک، بیش از آنکه یک مسیر فناورانه صرف باشد، یک روند اجتماعی-اقتصادی پیچیده است که متاثر از رفتار کاربران، سیاست‌گذاری‌های کلان، زیرساخت‌های ملی و همگرایی فناوری‌های نوین است. هر نسل از ابزارهای پرداخت، پاسخی به نیازهای در حال تحول مصرف‌کننده بوده است؛ از امنیت و سرعت گرفته تا انعطاف پذیری و دسترسی همگانی. اکنون با هم افزایی هوش مصنوعی، اینترنت اشیا، بلاک چین و فین‌تک‌های داده محور، صنعت پرداخت به مرحله‌ای رسیده که مرز میان بانکداری سنتی، فناوری و سبک زندگی دیجیتال به کلی محو شده است. لذا تنها بازیگرانی که بتوانند پرداخت را در دل اکوسیستم‌های دیجیتال مانند حمل و نقل هوشمند، سلامت دیجیتال، خرده‌فروشی آنلاین، متاورس و حتی گیمینگ ادغام کنند، آینده بازار را در دست خواهند گرفت.

ثبت نام
آنلاین
DBAplus.ir

DBA MBA

گرایش مدیریت پدافند غیرعامل

۶۶۴۶۸۱۳۷ - ۶۶۹۶۸۱۴۸
۰۹۳۷۸۶۲۰۴۰۶

www.DBAplus.ir

مدت دوره: MBA ۲۵۰ ساعت

DBA ۳۵۰ ساعت

مدیر: دك. دانشگاه صنعتی امیرکبیر
مؤرر: تأیید سازمان پدافند غیرعامل

آقای آذری جهرمی از توسعه پدافند غیرعامل در زمان وزارت‌تان چه خبر؟

شوند؛ اما نمی‌تواند هر روز یک چماق بگیرد و بر سر وزیر بکوبد تا مصوبات را اجرایی کند. البته بازوهای اجرایی نظارتی دیگری نیز هستند که خیلی کارا نیست. خودش هم نمی‌تواند برود و یک تنه قوانین را در همه دستگاه‌ها پیاده‌سازی نمایند.

جواد آذری جهرمی، وزیر ارتباطات و فناوری اطلاعات دولت دوازدهم چون یک فرد اطلاعاتی می‌باشد باید بهتر از هر فرد دیگری اهمیت توسعه پدافند غیرعامل را بویژه پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات درک نماید.

سوال اینجاست که ایشان در زمان تصدی وزارت ارتباطات و فناوری اطلاعات چقدر توانسته است قوانین بالادستی و ابلاغی سازمان پدافند غیرعامل کشور و مصوبات مجلس را در وزارتخانه متبوع خود اجرایی نماید؟ چقدر توانسته است این قوانین را در سازمان‌ها و شرکت‌های تابعه خود پیاده‌سازی نماید؟ اپراتورهای همراه اول به عنوان یکی از زیر مجموعه‌های این وزارتخانه چقدر توانسته‌اند برای پیاده‌سازی اسناد و قوانین بالادستی پدافند غیرعامل موفق باشند؟

مدیر مسئول جواد آذری جهرمی وزیر ارتباطات و فناوری اطلاعات دولت دوازدهم در بحبویه جنگ ۱۲ روزه اسرائیل به ایران، در واکنش به اظهارات رئیس پدافند غیرعامل مبنی بر نقش واتس‌آپ در مکان‌یابی و ترور بعضی از فرماندهان حماس در کانال تلگرامی خود نوشت: «بعید است سرداران و دانشمندان شهید ایران از سکوهای پیام‌رسان خارجی استفاده کرده باشند، به احتمال بسیار، آن‌ها از دستورالعمل‌های حفاظتی در این خصوص تبعیت می‌کرده‌اند.

ساختار نیروهای مسلح ایران، ساختاری رسمی است نه پارتیزانی. نظم در آن تلبور دارد و الگوهای منظم قابل کشف. بجای فرافکنی بهتر است به بازنگری در شیوه‌ها و مبانی حفاظت اطلاعات پرداخت.»

اما آنچه در این پیام جناب آقای وزیر جوان مغفول مانده این است که سازمان پدافند غیرعامل کشور به عنوان متولی اصلی توسعه پدافند غیرعامل در کشور تاکنون اقدامات ارزنده‌ای در جهت توسعه زیرساخت‌های امن در کشور انجام داده است. تهیه دستورالعمل‌ها، استانداردها، رویه‌های مناسب و ابلاغ آن‌ها به دستگاه‌ها بخش کوچکی از این امور است.

از آنجایی که این دستورالعمل‌ها در روند اجرایی امور مردم عادی قرار ندارد، خیلی‌ها با اقدامات ارزشمند این سازمان آشنایی ندارند و تصورات نادرستی از آن در ذهن می‌پروراندند و برخی از این عدم اطلاع مردم سوءاستفاده کرده و سعی در حمله به این سازمان دارند.

وظیفه اصلی اجرا و پیاده‌سازی قوانین و دستورالعمل‌ها به عهده کمیته پدافند غیرعامل دستگاه‌های اجرایی است که بالاترین مقام آن دستگاه یعنی وزیر، رئیس سازمان، مدیرعامل بانک و... به عنوان رئیس کمیته، و در بسیاری از موارد مدیر حراست به عنوان دبیر کمیته مسئول اصلی اجرای این قوانین است.

پس مسئولیت پیاده‌سازی و اجرای تمام قوانین ابلاغ شده از سوی سازمان پدافند غیرعامل در آن دستگاه به عهده ایشان است و چنانچه کوتاهی درخصوص توسعه پدافند غیرعامل در سازمان صورت گیرد، ایشان باید خود پاسخگوی مشکلات باشد. سازمان پدافند غیرعامل به عنوان یک متولی، ناظر و تسهیل‌گر عمل می‌کند تا قوانین به درستی پیاده‌سازی

ایشان باید پاسخ دهند که در زمان تصدی وزارت ارتباطات، اپراتورهای تلفن همراه چقدر توانستند حداقل‌های اسناد بالادستی پدافند غیرعامل را پیاده‌سازی نمایند؟

آقای آذری جهرمی شما باید پاسخ دهید که چرا نتوانستید در دوره تصدی‌گری خود حتی یک زیرساخت امن یا یک پیام‌رسان امن برای توسعه کسب‌وکارها راه‌اندازی نمایید تا در مواقع بحران یا جنگ، کسب‌وکارها با زیان مواجه نشوند؟

آقای آذری جهرمی شما اکنون باید پاسخگو باشید نه مطالبه‌گر!

شما باید پاسخگو باشید که چرا نتوانستید قوانین بالادستی سازمان پدافند غیرعامل کشور را در وزارتخانه خود پیاده‌سازی نمایید؟

چرا نتوانستید پیاده‌سازی قوانین بالادستی پدافند غیرعامل را در اپراتورها پیگیر شوید تا همه اطلاعات مخاطبان به خارج از کشور درز نکند.

آقای آذری جهرمی لطفاً به مردم گزارش دهید که از پیاده‌سازی سند حفاظت از زیرساخت‌ها که توسط مجلس شورای اسلامی تصویب شده است و توسط دبیرخانه کمیته دائمی پدافند غیرعامل به تمام دستگاه‌ها ابلاغ شده است، چه خبر؟

خوب است یک بار هم که شده به جای دلفک‌بازی، هوجی‌گری و فرار به جلو به مردم پاسخ بدهید که چرا

نتوانستید یک زیرساخت امن در دوره تصدی‌گری خود برای مردم ایجاد کنید؟

اگر شما عرضه پیاده‌سازی کوچک‌ترین کار یعنی سند حفاظت از زیرساخت‌ها را حتی در ساختار وزارت ارتباطات هم نداشتید پس بهتر است صُم بکم بمانید که خیلی به مردم بویژه به کسب‌وکارها بدهکارید.

بانی وضع موجود ارتباطات کشور شما باید که با یک حمله کوچک کل زیرساخت‌های کشور به فنا می‌رود.

بانی وضع موجود شما باید که هیچ اطلاعات امنی در کشور باقی نمانده است.

شما در حدی نیستید که بتوانید مدعی و مطالبه‌گر شوید و سازمان پدافند غیرعامل را زیر سؤال ببرید.

شما نباید در دوره تصدی‌گری خود حداقل یک زیرساخت امن برای کسب‌وکارها ایجاد می‌کردید؟ بفرمائید در این خصوص چه کردید؟

شما که یک فرد اطلاعاتی بودید و به شنود اطلاعات مردم عادت کرده‌اید خوب بود براساس اطلاعاتی که از شنود مردم جمع‌آوری کرده بودید حداقل یک پیام‌رسان مطمئن و مطلوب آن‌ها ایجاد می‌کردید. نه اینکه به جای حمایت از پیام‌رسان‌های داخلی، آن‌ها را تحقیر و ناامن برشمرد.

حرکت شما به سمت تلگرام که در نهایت هم هیچی بارتان نکرد و هر کاری دوست داشت انجام داد، آیا جز تضعیف و تحقیر پیام‌رسان‌های داخلی نتیجه‌ای داشت؟

آیا شنود اطلاعات مردم که حقوقش هم از بیت‌المال همین مردم تأمین می‌شد، نباید برای خود مردم و کسب‌وکارها نیز مفید فایده باشد.

شما به جای حمله به سازمان پدافند غیرعامل بهتر است به سوال‌های بالا جواب دهید.

اگر جوابی برای سؤال‌های بالا ندارید یعنی قبول دارید که در دوره تصدی‌گری خود در وزارت ارتباطات هیچ اقدام مثبتی برای توسعه پدافند غیرعامل نکرده‌اید.

پس بهتر است خاموش بنشینید و در این روزهایی که مردم داغدار عزیزانشان هستند ولی باز بر طبل وحدت می‌کوبند، داغ جدیدی بر دل آن‌ها نیفزایید.



تهدیدات امنیت سایبری در عصر تحول دیجیتال



راهکارهای مقابله با تهدیدات

فناوری‌های امنیتی: استفاده از فناوری‌های پیشرفته امنیتی نظیر رمزنگاری، دیوارهای آتش و سیستم‌های تشخیص نفوذ می‌تواند به مقابله با تهدیدات کمک کند. این فناوری‌ها امکان تشخیص و جلوگیری از حملات را بهبود می‌بخشند. به عنوان مثال، استفاده از رمزنگاری پیشرفته می‌تواند امنیت داده‌ها را در هنگام انتقال بهبود بخشد و خطر سرقت اطلاعات را کاهش دهد. رمزنگاری: رمزنگاری یکی از اصلی‌ترین روش‌های حفاظت از اطلاعات است که با استفاده از الگوریتم‌های پیچیده، داده‌ها را به صورت کد شده ذخیره و منتقل می‌کند. این روش می‌تواند تضمین کند که حتی در صورت دسترسی غیرمجاز به اطلاعات، محتوای آن‌ها قابل خواندن و استفاده نباشد.

استفاده از پروتکل‌های رمزنگاری نظیر SSL و TLS برای انتقال اطلاعات در بستر اینترنت بسیار مهم است. دیوارهای آتش: متخصصین فناوری و دیگران معتقد به مزایای سخت‌افزار نسبت به نرم‌افزار هستند، اغلب آن‌ها برای دسترسی به اطلاعات داخلی شبکه اعم از پرینتر اشتراک‌گذاری شده و منابع شبکه داخلی نیاز به نرم‌افزار دیواره آتش را لازم می‌دانند. اما لازم است به دیواره آتش اطمینان کامل داشته باشیم؛ زیرا به عنوان محافظ کامپیوترها و جلوگیری از طیف وسیعی از سوءاستفاده‌ها و مقابله با ورود عوامل مخرب، ترافیک‌های غیرضروری، ویروس‌ها، کرم‌ها و عوامل آسیب‌رسان باید ما را در امان نگه دارند.

سیستم‌های تشخیص نفوذ: سیستم‌های تشخیص نفوذ (Intrusion Detection Systems) ابزارهایی هستند که با مانیتورینگ مداوم ترافیک شبکه، تلاش‌های نفوذ و حملات سایبری را شناسایی می‌کنند.

این سیستم‌ها می‌توانند به صورت فعال یا غیرفعال عمل کنند و با تحلیل الگوهای ترافیک، فعالیت‌های مشکوک را تشخیص دهند. استفاده از این سیستم‌ها می‌تواند به کاهش زمان واکنش در مقابل حملات و افزایش امنیت شبکه کمک کند.

آموزش و آگاهی: یکی از مهم‌ترین روش‌های مقابله با تهدیدات سایبری، آموزش و آگاهی‌بخشی به کاربران است. با افزایش دانش کاربران در مورد روش‌های حمله و تدابیر امنیتی، می‌توان خطرات را به میزان قابل توجهی کاهش داد. برگزاری دوره‌های آموزشی و ارائه اطلاعات به‌روز به کاربران می‌تواند در این زمینه مؤثر باشد.

آموزش کارکنان: کارکنان هر سازمان باید به خوبی با مفاهیم امنیت سایبری آشنا باشند و توانایی تشخیص حملات سایبری را داشته باشند. برگزاری دوره‌های آموزشی منظم و تمرین‌های شبیه‌سازی حملات می‌تواند به افزایش آگاهی و آمادگی کارکنان کمک کند. همچنین، ترویج فرهنگ امنیت در سازمان و تاکید بر اهمیت امنیت سایبری می‌تواند نقش مؤثری در کاهش خطرات داشته باشد.

آگاهی‌بخشی به عموم: آگاهی‌بخشی به عموم مردم نیز از اهمیت ویژه‌ای برخوردار است. با توجه به استفاده گسترده از اینترنت و فناوری‌های دیجیتال در زندگی روزمره، همه افراد باید با روش‌های حفاظت از اطلاعات شخصی و شناسایی تهدیدات سایبری آشنا باشند. استفاده از رسانه‌ها، شبکه‌های اجتماعی و برنامه‌های آموزشی برای افزایش آگاهی عمومی می‌تواند به کاهش حملات سایبری کمک کند.

نتیجه‌گیری

امنیت سایبری در عصر تحول دیجیتال به یک ضرورت اساسی تبدیل شده است. از آنجایی که جامعه ما به شدت به فناوری اطلاعات و ارتباطات وابسته می‌باشد، به حفاظت از اطلاعات و عملکرد در دنیای دیجیتال باید بیش از پیش توجه شود. این هدف به ایجاد یک جامعه امن و پایدار در دنیای دیجیتال کمک می‌کند و به ما این امکان را می‌دهد که با استفاده از فناوری از تهدیدات و خسارات تا حد امکان جلوگیری کنیم.



آینده هوش مصنوعی تا ۲۰۳۰

پیش‌بینی‌ها حاکی از آن است که تا سال ۲۰۳۰، هوش مصنوعی با استفاده از فناوری‌های نوین به سطوح جدیدی خواهد رسید. در این بخش، به بررسی این روندها می‌پردازیم:

الگوریتم‌های پیشرفته یادگیری عمیق

الگوریتم‌های یادگیری عمیق نقش اساسی در پردازش داده‌های حجیم و یادگیری از آن‌ها دارند. این الگوریتم‌ها تا سال ۲۰۳۰ توسعه یافته، و قادر خواهند بود مدل‌های پیچیده‌تر و با کارایی بیشتری ارائه دهند.

(IoT) هم‌افزایی هوش مصنوعی و اینترنت اشیا

ترکیب هوش مصنوعی با اینترنت اشیا، به امکان ارتباط و کنترل هوشمند دستگاه‌ها در مقیاس جهانی کمک خواهد کرد. این تعامل، خانه‌های هوشمند، شهرهای هوشمند و خودروهای خودران را به مرحله‌ای بی‌سابقه خواهد رساند.

(Explainable AI) هوش مصنوعی قابل توضیح

یکی از بزرگ‌ترین چالش‌های مدل‌های هوش مصنوعی فعلی، عدم شفافیت عملکرد آن‌هاست. تا سال ۲۰۳۰، توسعه مدل‌های هوش مصنوعی قابل توضیح، اعتماد کاربران و سازمان‌ها به این فناوری را افزایش خواهد داد.

محاسبات کوانتومی و هوش مصنوعی

استفاده از این فناوری در حل مسائل پیچیده، مانند پیش‌بینی الگوهای آبوهوا و تحلیل ژنتیکی، دورنمای جدیدی برای آینده هوش مصنوعی خواهد گشود.

کاربردهای صنعتی پیشرفته

پیشرفت هوش مصنوعی تا سال ۲۰۳۰، زمینه را برای استفاده گسترده‌تر و عمیق‌تر در صنایع مختلف فراهم می‌کند.

حوزه سلامت و پزشکی

سیستم‌های تشخیصی مبتنی بر AI، دقت تشخیص سرطان و بیماری‌های پیچیده را به طرز چشمگیری ارتقا خواهند داد.

مالی و اقتصاد

تا سال ۲۰۳۰، الگوریتم‌های هوشمند قادر خواهند بود سرمایه‌گذاری‌های هوشمند و بهینه‌سازی منابع مالی را به سطح جدیدی برسانند.

حمل و نقل و خودروهای خودران

خودروهای خودران با کمک AI قادر خواهند بود تعامل بهتری با محیط اطراف داشته باشند و ایمنی حمل و نقل را بهبود دهند. هوش مصنوعی در این حوزه می‌تواند از ترافیک شهری بکاهد و مصرف سوخت را بهینه کند.

چالش‌ها و ملاحظات اخلاقی

با وجود دستاوردهای عظیم، پیشرفت‌های هوش مصنوعی مسائل اخلاقی مهمی را نیز به همراه دارد:

حریم خصوصی داده‌ها

جمع‌آوری حجم بالای داده‌ها توسط سیستم‌های هوشمند، تهدیدی برای حریم خصوصی افراد خواهد بود. تلاش برای ایجاد استانداردهای بین‌المللی در حفاظت از اطلاعات، ضرورت پیدا خواهد کرد.

تبعیض الگوریتمی

الگوریتم‌های هوش مصنوعی ممکن است به دلیل داده‌های ناقص یا جهت‌دار، تبعیض‌های نژادی، جنسیتی یا اجتماعی ایجاد کنند. توسعه مدل‌های عادلانه و غیرمغرضانه در آینده امری ضروری خواهد بود.

تغییرات در بازار کار

اتوماسیون مبتنی بر AI می‌تواند منجر به از بین رفتن برخی مشاغل شود. ایجاد مشاغل جدید و توانمندسازی نیروی کار در مهارت‌های مرتبط با AI باید از اولویت‌های جهانی باشد.

جمع‌بندی

تا سال ۲۰۳۰، مدل‌های هوش مصنوعی تحولی بنیادین در فناوری، اقتصاد و جامعه ایجاد خواهند کرد. پیشرفت‌هایی مانند هوش مصنوعی عمومی، پردازش چندوجهی و ادغام با محاسبات کوانتومی، مرزهای جدیدی را در این حوزه باز می‌کنند.

انجمن مدیریت فناوری و نوآوری ایران برگزار نمود: پنل تخصصی «تحول دیجیتال و هوشمندسازی معادن به مثابه گذار اجتماعی-فنی؛ چالش ها و راهکارها»

دیجیتال و هوشمندسازی، دکتر سهراب آقازاده مدیر مشاوره تحول دیجیتال صنعتی شرکت فرا و مهندس محمد انتظام مدیرعامل شرکت برسام رایان برگزار شد.



انجمن مدیریت فناوری و نوآوری ایران با همکاری انجمن تحول دیجیتال ایران و اندیشکده سیاست پژوهان علم، فناوری و نوآور پنل تخصصی «تحول دیجیتال و هوشمندسازی معادن به مثابه گذار اجتماعی-فنی؛ چالش ها و راهکارها» را برگزار نمود.

در این رویداد، ضمن سخنرانی در خصوص تحول دیجیتال و هوشمندسازی در صنایع معدنی به نکات راهبردی و عملیاتی مبتنی بر برترین تجارب آزموده شده در سایر کشورها و شرکت های بین المللی در شیلی، کانادا و چین و شرکت ها و سازمان های ایرانی همچون ایمیدرو، میدکو، فولاد مبارکه، صنایع معدنی چادرملو، گل گهر و... و الزامات سیاست گذاری و طراحی نقشه راه صنایع مرتبط پرداخته شد.

گفتنی است این پنل با حضور دکتر مصطفی صفدری رنجبر عضو هیأت علمی دانشگاه تهران و مدیر اندیشکده سیاست پژوهان علم، فناوری و نوآوری، دکتر حبیب کراری رئیس کمیته آموزش و فرهنگ سازی انجمن تحول دیجیتال ایران، دکتر رسول سرائیان مدیرعامل شرکت توسعه فناوری سیما آترون، دکتر پیام حقیقی بروجنی رئیس مرکز یادگیری میدکو، دکتر مجید وفایی مدیر مرکز ایمینو، دکتر محمد نثاری پژوهشگر حوزه تحول

انعقاد تفاهم نامه «نشریه زمان تحول» با «انجمن تحول دیجیتال»



به منظور همکاری در جهت توسعه و نشر اقدامات حوزه های مرتبط با تحول دیجیتال، نشریه زمان تحول و انجمن تحول دیجیتال تفاهم نامه همکاری مشترک امضا کردند.

دکتر مصطفی بهمن آبادی، مدیرمسئول نشریه زمان تحول با اشاره به ظرفیت های رسانه در فرایند تحول دیجیتال اظهار داشت: رسانه ها نقش بسیار مهمی در شکل دهی و انتقال داده ها و اطلاعات ایفا می کنند. زمانی که صحبت از تکنولوژی و کسب و کار می شود، رسانه های فعال در این حوزه مسئولیت بزرگی برعهده دارند.

وی بیان کرد: رسانه ها فضای ارتباطی بی واسطه ای بین کسب و کارها و مخاطبان ایجاد می کنند که این امر می تواند به بهبود تجربه مشتری منجر شود، علاوه بر این با دسترسی به داده های رسانه ای، سازمان ها می توانند استراتژی های بازاریابی خود را هدفمندتر و کارآمدتر طراحی و اجرا کنند. در ادامه نیز محمدعلی معین دبیر انجمن تحول دیجیتال افزود: استفاده از ظرفیت های علمی و توسعه همکاری های آموزشی، تحقیقاتی و فناوری و همچنین رسانه ای، خبری و جریان سازی در جهت استمرار ارتباط سازمان یافته میان انجمن و نشریه مهم ترین هدف انعقاد این تفاهم نامه است.