

در این شماره می‌خوانید...

- ۱ وقتش رسیده اتاق سرور کوچک خود را تبدیل به دیتاسنتر کنید
- ۲ خطرات بالقوه ربات‌ها و هوش مصنوعی
- ۳ اگر می‌خواهید اتاق سرور بسازید؛ این ۹ نکته حیاتی را رعایت کنید
- ۴ دیتاسنترهای هوش مصنوعی؛ هدف جنگ‌های آینده

**عوامل
قطعی‌های
برنامه‌ریزی نشده
مرکز داده!!**
قطعی برق پرچم دار قطعی‌ها...



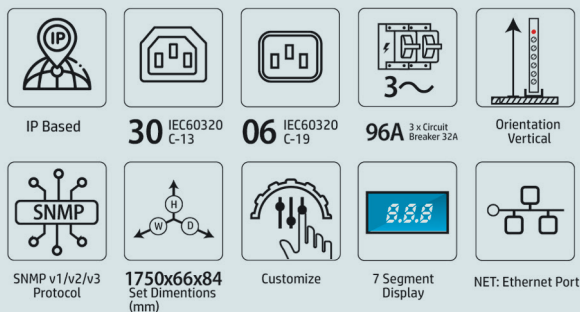
شما دعوتید به بازدید از غرفه شرکت تیمام شبکه در بیست و هشتمین نمایشگاه فناوری اطلاعات و ارتباطات (الکامپ) از تاریخ ۳ تا ۶ مهر ماه در محل دائمی نمایشگاه‌های بین‌المللی تهران سالن ۳۸





TPD-836BS3

IP-Based Bank
Monitoring & Switching
PDU (Circuit Breaker)
Power Distribution Unit



مشخصات فنی:

- امکان ارتباط از راه دور بر اساس پروتکل اینترنت (IPBased)
- دارای پریز ها و قاب های مژولار کشویی با قابلیت سفارشی سازی
- قابلیت انتقال جریان ۹۶ آمپر (۳ فاز) و پنج شاخه IEC60309
- اختصاص حداکثر جریان ۳۲ آمپر ورودی به هر مژول
- دارای ۳ عدد Circuit breaker ۳۲ آمپر، به منظور محافظت دستگاه در برابر نوسانات جریان برق
- دارای RTC (real-time clock) به همراه باتری پشتیبان
- امکان اتصال ۹ دستگاه به صورت Master/Slave از طریق پورت RS-485 با پروتکل Modbus

شما همه، ما
سه فاز قدرتمند!
قابلیت دسترسی و کنترل!
نسل هوشمند پنل های
توزیع برق داخل رک



تلفن گویا: ۹۱۰۷۲۳۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
اپراتور: ۶۶۹۴۷۲۰۰
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

۲	●	سرمقاله به وقت تصمیم گیری در میانه طوفان
۴	●	اخبار فناوری اطلاعات ایران و جهان « سرعت ۶G چین به ۲۸۰ گیگابیت بر ثانیه رسید « سریع ترین ابررایانه های جهان با سیستم های AMD « اولین کامپیوتر کوانتومی به فضا پرتاب شد « ساخت یک ابررایانه هوش مصنوعی نیازمند ۹ نیروگاه هسته ای « ابررایانه ای شبه مغز انسان، با ۶۵۰ هزار هسته پردازشی، داروهای جدید را کشف می کند « الکامپ ۱۴۰۴ سوم تا ششم مهر برگزار می شود
۶	●	گزارش کشنده تر از بمب هسته ای
۱۰	●	مقاله فنی وقتش رسیده اتاق سرور کوچک خود را تبدیل به دیتاسنتر کنید
۱۴	●	مقاله مدیریتی چگونه بدون اخراج کارمندان هزینه ها را کاهش دهیم
۱۸	●	اینفوگرافی خطرات بالقوه ربات ها و هوش مصنوعی
۲۰	●	مقاله فنی اگر می خواهید اتاق سرور بسازید؛ این ۹ نکته حیاتی را رعایت کنید
۲۴	●	مقاله مدیریتی چگونه مدیران باهوش مصنوعی تصمیم های بهتری می گیرند
۲۸	●	داستان یک موفقیت فرمول موفقیت: نوآوری نگاهی کوتاه به تاریخچه شرکت فیلیپس
۳۲	●	مقاله مدیریتی سوالاتی که باید پیش از ترک شغل، از خودتان بپرسید
۳۶	●	مقاله فنی دیتاسنترهای هوش مصنوعی؛ هدف جنگ های آینده
۳۹	●	نکته ها و گفته ها
۴۰	●	مقاله مدیریتی اگر به رییس مان دروغ گفتیم و او متوجه شد چه باید کرد؟
۴۳	●	مقاله فنی چگونه خطرات ایمنی محل کار دیتاسنترها را کاهش دهیم
۴۷	●	مقاله مدیریتی هنر تصمیم گیری در بحران؛ چگونه کسب و کارمان را در طوفان ها نجات دهیم
۵۷	●	کتاب باز استاندارد زیر ساخت مراکز داده TIA۹۴۲ (بخش نهم)
۵۹	●	مقاله فنی چگونه از سرورهای خود در برابر حملات جنگی محافظت کنیم؟
۶۰	●	سرگرمی

فصلنامه اقتصادی فرهنگی

سال هشتم / شماره ۲۹ / تابستان ۱۴۰۴

صاحب امتیاز و مدیرمسئول: فرزانه شوقی لیسار
گرافیک: محمد راجی مهدی نصرتی

نشانی اینترنتی: www.viragostar.ir

تلفن: ۶۶۹۴۴۹۸۰

برای دریافت فصلنامه به لینک زیر مراجعه فرمایید:
<https://tiamnetworks.ir/blog1/emagazine>
برای خرید فصلنامه با داخلی ۶۱۰ تماس حاصل فرمایید.
ایمیل: info@viragostar.ir

آدرس: فاطمی غربی، بین بزرگراه چمران و جمالزاده، پلاک ۲۶۹
چاپ: مرکز چاپ دیجیتال ایران کهن
نوبت چاپ: اول

با حمایت شرکت تیام شبکه
مدیر عامل: بابک رشیدی آشتیانی

نشانی اینترنتی: www.tiamnetworks.ir
اینستاگرام: [instagram.com/tiamnetworks](https://www.instagram.com/tiamnetworks)

تلگرام: ۰۹۲۲۳۱۱۹۱۷۸

منتظر شنیدن نظرات شما در press@tiamnetworks.ir یا داخلی ۶۱۰ هستیم.

شرکت تیام شبکه



به وقت تصمیم گیری در میانه‌ی طوفان!

✍️ فرزانه شوقی لیسار

است. مدیران باید بین واکنش سریع برای کاهش هزینه‌ها و نگاه استراتژیک به حفظ سرمایه‌ی انسانی، تعادل ایجاد کنند. تعدیل نیرو شاید در کوتاه‌مدت فشار مالی را کم کند، اما بازسازی تیم‌های از هم‌پاشیده در آینده، بسیار پرهزینه‌تر خواهد بود. در مقابل، حمایت از نیروها و سرمایه‌گذاری روی نوآوری، نه تنها شانس عبور از بحران را افزایش می‌دهد، بلکه پیام روشنی به بازار و سرمایه‌گذاران مخابره می‌کند: «ما برای ماندن آمده‌ایم».

بحران‌ها می‌آیند و می‌روند، اما شرکت‌هایی که در میانه طوفان، به ارزش‌های انسانی و نوآوری وفادار می‌مانند، آینده را می‌سازند. اکنون زمان آن است که به جای کوچک‌تر کردن رویاها، به بزرگ‌تر کردن توان و انگیزه تیم بیندیشیم. آینده اکوسیستم فناوری، به همین تصمیمات امروز گره خورده است.

را کاهش می‌دهد، بلکه پیام ناامیدی به سایر نیروها و حتی بازار مخابره می‌کند. در شرایط بحرانی، از دست دادن انگیزه و اعتماد، شاید خطرناک‌تر از ضرر مالی باشد.

به همین دلیل، امروز بیش از هر زمان دیگری نیاز به همدلی و حمایت از نیروها احساس می‌شود. مدیران می‌توانند با ایجاد فضای امن روانی، برگزاری جلسات گفت‌وگو، شفاف‌سازی وضعیت سازمان و حتی اقدامات کوچک اما معنادار مانند انعطاف در ساعات کاری یا امکان کار از راه دور، به ایجاد آرامش و حفظ انگیزه کارکنان کمک کنند. سرمایه‌گذاری روی آموزش و ارتقای مهارت‌ها، هرچند هزینه‌بر به نظر برسد؛ در این شرایط می‌تواند پیامی قوی برای تعهد به آینده و بقا باشد.

همزمان، بحران می‌تواند فرصتی برای بازاندیشی در مدل‌های کسب‌وکار باشد. بسیاری از نوآوری‌ها و تغییرات بزرگ در دل شرایط سخت متولد شده‌اند. تمرکز بر محصولاتی که نیاز فوری بازار را پاسخ می‌دهند؛ یافتن روش‌های جدید درآمدزایی، ورود به بازارهای کم‌رقیب یا همکاری با شرکت‌های دیگر برای کاهش هزینه‌ها، راهکارهایی است که می‌تواند شرکت‌ها را از مسیر بقا به مسیر رشد بازگرداند.

این لحظه، لحظه آزمون مدیریت کسب‌وکار

جنگ ایران و اسرائیل، فراتر از یک رویداد سیاسی و نظامی، موجی از اثرات اقتصادی و روانی در اکوسیستم فناوری و IT کشور ایجاد کرد. شرکت‌های کوچک و بزرگ این حوزه، که پیش‌تر با امید به توسعه‌ی پایدار پیش می‌رفتند و رشدی هرچند کند و آرام داشتند؛ ناگهان خود را در میانه‌ی طوفانی از بی‌ثباتی، قطع زنجیره‌ی تامین، کاهش سرمایه‌گذاری و افت شدید تقاضا یافتند.

در هفته‌ها و ماه‌های پس از آغاز بحران، گزارش‌ها و مشاهدات میدانی نشان داد که بسیاری از کسب‌وکارهای فناوری به ناچار دست به تصمیمات دشواری زدند؛ تعدیل و اخراج نیرو، توقف پروژه‌های در دست اجرا، کاهش بودجه‌ی تحقیق و توسعه، و انجماد یا لغو طرح‌های سرمایه‌گذاری، از جمله واکنش‌های غالب بود. این اقدامات، هرچند در نگاه نخست پاسخی منطقی به کاهش درآمد و افزایش ریسک بازار به نظر می‌رسند، اما در بلندمدت می‌توانند زیان‌هایی جبران‌ناپذیر بر پیکره‌ی سازمان و کل اکوسیستم وارد کنند.

نیروی انسانی متخصص، بزرگ‌ترین سرمایه‌ی شرکت‌های فناوری است؛ سرمایه‌ای که به راحتی جایگزین نمی‌شود. از دست دادن مهندسان باتجربه، طراحان خلاق و مدیران پروژه کارآزموده، نه تنها توان عملیاتی سازمان

28th

IRAN INTERNATIONAL EXHIBITION OF ELECOMP الکامپ

۳ الی ۶ شهریور ۱۴۰۴



با سلام و احترام؛

بدینوسیله از شما دعوت می‌شود برای بازدید از غرفه شرکت تیام شبکه بیست و هشتمین نمایشگاه فناوری اطلاعات و ارتباطات (الکامپ) که از تاریخ ۳ تا ۶ شهریور ماه در محل دائمی نمایشگاه‌های بین‌المللی تهران سالن ۳۸ برگزار می‌شود، حضور بهم رسانید.

با تقدیم احترام
شرکت تیام شبکه



تلفن گویا: ۹۱۰۷۲۳۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
اپراتور: ۶۶۹۴۷۲۰۰
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

سرعت 6G چین به ۲۸۰ گیگابیت بر ثانیه رسید

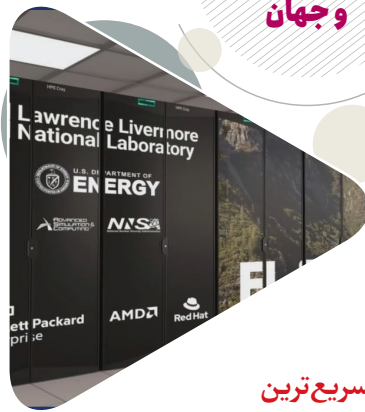
منبع: www.androidheadlines.com

اپراتور چینا موبایل موفق شد رکورد انتقال داده روی نسل ششم شبکه‌های موبایل را شکسته و به سرعت خیره‌کننده‌ی ۲۸۰ گیگابیت بر ثانیه دست یابد؛ یعنی دانلود یک فایل ۵۰ گیگابایتی فقط در ۱.۴ ثانیه. این دستاورد که در کنفرانس اینترنت چین ۲۰۲۵ رونمایی شد؛ جدیدترین آزمایش 6G در این کشور است. چنین سرعتی، حدوداً ۱۴ برابر سرعت تئوری شبکه‌های 5G است و در صورت پیاده‌سازی عملی، می‌تواند انقلاب بزرگی در گوشی‌های هوشمند و ارتباطات بی‌سیم ایجاد کند؛ حتی فراتر از اینترنت ثابت کابلی. تصور کنید به راحتی بتوان فایل‌های بزرگ چند ده گیگابایتی را در ۱ تا ۲ ثانیه جابه‌جا کرد. با این نرخ انتقال، می‌توان یک فیلم دو ساعته با کیفیت بلوری را در کمتر از دو ثانیه منتقل کرد. چینا موبایل بیش از ۱۰۰ سایت تحقیقاتی 6G راه‌اندازی کرده و در حال توسعه فناوری‌های کلیدی نسل ششم موبایل است. این شرکت در ۴ پروژه ملی پیشگام مشارکت دارد و اعلام کرده است که برای توسعه شبکه‌های 6G بیش از ۳۹.۱ میلیارد یوان (۵.۴۶ میلیارد دلار) سرمایه‌گذاری خواهد کرد.

همچنین، در فوریه امسال هم چینا موبایل، نخستین ماهواره مخابراتی پر سرعت خود را به فضا پرتاب کرد. این ماهواره در ارتفاع ۵۰۰ کیلومتری سطح زمین قرار دارد و می‌تواند ارتباطات ماهواره‌ای با تاخیر بسیار پایین را فراهم کند. اگرچه، هنوز تاریخ دقیقی برای عرضه شبکه‌های 6G مشخص نشده، اما کارشناسان پیش‌بینی می‌کنند که این فناوری بین سال‌های ۲۰۲۸ تا ۲۰۳۰ به‌طور رسمی وارد عرصه تجاری شود.



China has rolled out the world's first 10gigabit internet connection, marking a major milestone in global broadband technology



سریع‌ترین ابرایانه‌های جهان با سیستم‌های AMD

منبع: top500.org

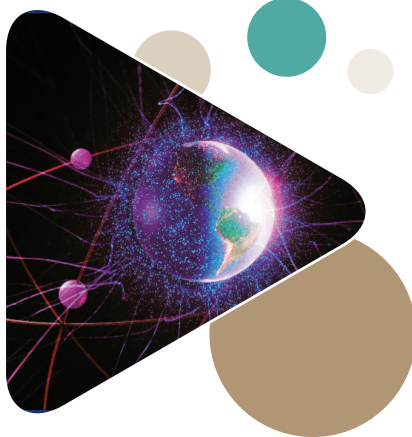
در تازه‌ترین فهرست قدرتمندترین ابررایانه‌های دنیا که توسط وب سایت Top500 منتشر شده؛ نه تنها خبری از ابررایانه‌های چینی و اروپایی نیست؛ بلکه این بار تراشه‌های AMD توانستند صدر جدول را از آن خود کنند. سه ابررایانه برتر، همگی در ایالات متحده قرار دارند و از شرکت‌هایی مانند میکروسافت یا XAI ایلان ماسک هم نیستند. در جدیدترین رده‌بندی جهانی محاسبات با عملکرد بالا (HPC)، ابررایانه El Capitan که بر پایه شتاب‌دهنده‌های AMD Instinct MI300A ساخته شده، با ثبت عملکرد ۱.۷ اگرافلاپس FP64، جایگاه نخست را به خود اختصاص داد. پس از آن، Frontier با قدرت پردازشی ۱.۳۵۳ اگرافلاپس که آن هم از فناوری AMD بهره می‌برد، در رتبه دوم قرار گرفت. جایگاه سوم نیز به Aurora با پردازنده‌های اینتل و توان محاسباتی ۱.۰۱۲ اگرافلاپس رسید. هر سه ابررایانه توسط آزمایشگاه‌های وزارت انرژی ایالات متحده اداره می‌شوند. ابررایانه ال کاپیتان با بیش از ۱۱ میلیون هسته پردازشی، روی پلتفرم HPE Cray EX255a و با اتصال شبکه HPE Slingshot کار می‌کند. این سیستم در بنچمارک‌های دیگر مانند HPCG و HPLMxP نیز رتبه‌های نخست را کسب کرده است. اگرچه رتبه‌های اول و دوم و در مجموع پنج سیستم از میان ۱۰ رتبه برتر به AMD تعلق دارد، اما پردازنده‌های اینتل همچنان بیشترین سهم بازار را حفظ کرده‌اند. در حال حاضر، از مجموع ۵۰۰ ابررایانه موجود در فهرست، ۲۹۴ سیستم با پردازنده‌های اینتل و ۱۷۳ سیستم با پردازنده‌های AMD کار می‌کنند.

World's fastest memory writes 25 billion bits per sec, 10,000x faster than current tech

اولین کامپیوتر کوانتومی به فضا پرتاب شد

منبع: futurism.com

تیمی بین‌المللی از پژوهشگران موفق شدند نخستین کامپیوتر کوانتومی فوتونی ویژه فضا را به مدار زمین بفرستند. این کامپیوتر که روی یک ماهواره نصب شده است، اکنون در ارتفاع ۵۵۰ کیلومتری سطح زمین در مدار قرار گرفته و داده‌هایی درباره عملکرد رایانش کوانتومی در شرایط سخت فضایی جمع‌آوری می‌کند. این پروژه با رهبری فیلیپ والتز از دانشگاه وین انجام شد. به گفته‌ی او، برای ساخت این کامپیوتر محدودیت‌های زیادی وجود داشت: «اندازه‌ی آن باید به اندازه‌ی یک جعبه‌ی کفش باشد، در برابر شوک‌های مکانیکی و حرارتی مقاوم باشد و نرم‌افزاری داشته باشد که به‌طور خودکار عمل کند و در صورت بروز مشکل واکنش نشان دهد.» کامپیوترهای کوانتومی به جای صفر و یک از «کیوبیت» استفاده می‌کنند؛ واحدی که می‌تواند همزمان در حالت صفر، یک یا ترکیبی از هر دو قرار گیرد. کیوبیت‌ها به عوامل محیطی مانند دما و میدان مغناطیسی بسیار حساس هستند و همین موضوع ساخت و استفاده از آن‌ها را دشوار می‌کند. در فضای خارج از زمین، امکان کالیبره کردن یا نظارت دائمی بر کامپیوتر وجود ندارد؛ به همین دلیل سیستم باید کاملاً خودکار و مقاوم باشد. پیش از این، ماهواره‌ها برای توسعه‌ی اینترنت کوانتومی نیز استفاده شده بودند؛ از جمله برای اتصال دو مرکز کوانتومی در چین، یا لینک‌هایی میان چین و اتریش و همچنین چین و آفریقای جنوبی.



Scientists Just Launched the First Quantum Computer Into Space

● الکامپ ۱۴۰۴ سوم تا ششم مهر برگزار می شود

منبع: iranmr.org

تاریخ جدید بیست و هشتمین نمایشگاه الکامپ اعلام شد. این رویداد بزرگ فناوری، از سوم تا ششم مهرماه ۱۴۰۴ در محل دائمی نمایشگاه‌های بین‌المللی تهران برگزار خواهد شد. این دوره از نمایشگاه با محوریت هوش مصنوعی و با شعار «سرمايه‌گذاری هوشمند، توسعه پایدار» برگزار خواهد شد. تمرکز امسال نمایشگاه علاوه بر هوش مصنوعی، بر موضوعات کلیدی چون امنیت سایبری و حوزه‌های متنوع فناوری اطلاعات است. این نمایشگاه پیش‌تر قرار بود ۲۷ تا ۳۰ خرداد برگزار شود، اما به دلیل شرایط ناشی از جنگ به تعویق افتاد. روز ۲۲ مرداد ماه نیز نشست خبری نمایشگاه الکامپ برگزار شد. صدیف بیک‌زاده مدیرعامل شرکت سهامی نمایشگاه‌های بین‌المللی با تأکید بر تحول ماهیت نمایشگاه‌ها از صرفاً عرضه کالا و خدمات به بستری برای سیاست‌گذاری و تبادل دانش، گفت: «نمایشگاه‌ها را با نگاه گفتمان‌سازی و تقویت فرهنگ نوآوری برگزار می‌کنیم. نمایشگاه الکامپ نیز به‌طور کامل به این رویداد اختصاص یافته است.» او همچنین از ارائه تخفیف‌های ۱۰ تا ۵۰ درصدی برای شرکت‌های حاضر در نمایشگاه خبر داد و هدف اصلی را حمایت از فعالیت‌های اقتصادی و فناورانه عنوان کرد. عباس رمدانی، دبیرکل سازمان نصر کشور، نیز اعلام کرد: «نمایشگاه الکامپ امسال علاوه بر حضور فیزیکی، به‌صورت هم‌زمان در فضای متاورس نیز برگزار خواهد شد.» رضا حیدری دبیر اجرایی بیست و هشتمین نمایشگاه الکامپ با اشاره به حضور بیش از ۵۰۰ شرکت داخلی و ۷۰ شرکت خارجی در الکامپ بیان کرد: «الکامپ امسال، همانند دوره‌های پیشین، دارای رویدادهای جانبی متعدد و متنوعی است. یکی از این رویدادها که همواره با همکاری سازمان‌ها و نهادهای تخصصی برگزار می‌شود، رویدادهای فناورانه است. همچنین امسال، سخنرانی‌هایی تحت عنوان «تاکس‌ها» در سه نقطه از نمایشگاه پیش‌بینی شده که تاکنون حدود ۱۵۰ نفر برای شرکت در این برنامه‌ها ثبت‌نام کرده‌اند.» او در ادامه تأکید کرد: «سالن تخصصی «الکامپ ای‌آی» برای شرکت‌های دانش‌بنیان فعال در حوزه هوش مصنوعی در نظر گرفته شده است. همچنین، سالن «دولت هوشمند» در سالن ۲۷ با حضور دستگاه‌های اجرایی برگزار می‌شود. مسابقات استارت‌آپی نیز به‌عنوان بخشی از برنامه‌های جانبی در جریان خواهند بود.»



● ابررایانه‌ای شبه مغز انسان، با ۶۵۰ هزار هسته پردازشی، داروهای جدید را کشف می‌کند



منبع: eetimes.com

شرکت نوپای SpiNNcloud پیشگام در حوزه سخت‌افزار نورومورفیک، یک سیستم محاسباتی فوق‌العاده بر پایه تراشه‌های اختصاصی خود را به دانشگاه لایپزیگ عرضه کرده است. این ابررایانه شامل ۴۳۲۰ تراشه SpiNNaker2 است که در مجموع بیش از ۶۵۶.۶۴۰ هسته پردازشی دارند. توان این ابرکامپیوتر به گونه‌ای طراحی شده که بتواند دست کم ۱۰.۵ میلیارد نورون را شبیه‌سازی کند و در پروژه‌هایی همچون کشف دارو در زمینه پزشکی شخصی‌سازی شده، مورد استفاده قرار گیرد. «ریچارد اسپینکلر»، یکی از بنیان‌گذاران SpiNNcloud، می‌گوید: «معماری ما برای پردازش موازی گسترده و الگوریتم‌هایی با پراکندگی پویا طراحی شده است و به‌طور چشمگیری بسیار بهینه‌تر از پردازنده‌های گرافیکی متداول عمل می‌کند.» این ابرکامپیوتر دست‌کم ۱۸ برابر کارآمدتر از GPUها عمل می‌کند و ضمن مصرف انرژی کمتر، می‌تواند در کمتر از یک ساعت، ده‌ها میلیارد مولکول را بررسی کند؛ قابلیتی که برای پیوند مولکول‌ها با پروتئیل ژنتیکی بیماران نقطه عطفی محسوب می‌شود. معماری SpiNNaker2 متکی بر تراشه‌هایی با توان مصرفی پایین (بین ۰.۸ تا ۲.۵ وات برای هر تراشه) است و در یک رک ایستاده قابل نصب است، اما دانشگاه لایپزیگ ناچار شد آن را در دو رک نصب کند تا مطمئن شود مصرف انرژی کل سیستم در محدوده ۲۵ کیلووات باقی می‌ماند. با این پروژه، SpiNNcloud گامی مهم در توسعه فناوری نورومورفیک و ایجاد زیرساخت‌های کم‌مصرف برای هوش مصنوعی برداشته است. این سیستم نه تنها سرعت انجام محاسبات را به‌طور چشمگیری افزایش می‌دهد، بلکه هزینه‌های انرژی و اثرات زیست‌محیطی را نیز به میزان فراوانی کاهش می‌دهد. دانشگاه لایپزیگ اکنون با این فناوری، در خط مقدم تحقیقات هوش مصنوعی و داروسازی شخصی قرار گرفته است.

SpiNNcloud Sells Neuro-morphic Supercomputer For Drug Discovery

● ساخت یک ابررایانه هوش مصنوعی نیازمند ۹ نیروگاه هسته‌ای

منبع: interestingengineering.com

مطالعات جدید نشان می‌دهند رشد سریع هوش مصنوعی و گسترش ابررایانه‌های پیشرفته، به‌زودی منابع انرژی جهانی را با بحرانی بزرگ مواجه خواهد کرد. براساس پژوهشی مشترک از محققان دانشگاه جرج‌تاون، Epoch AI و مؤسسه RAND، مصرف انرژی مراکز داده و سخت‌افزارهای هوش مصنوعی تقریباً هر سال دو برابر می‌شود. اگر این روند ادامه یابد، تا سال ۲۰۴۰ یک ابررایانه AI با دو میلیون تراشه، هزینه‌ای بالغ بر ۲۰۰ میلیارد دلار و مصرف برق معادل ۹ گیگاوات (معادل توان تولیدی ۹ نیروگاه هسته‌ای) خواهد داشت. این میزان برق مصرفی برای تأمین انرژی میان ۷ تا ۹ میلیون خانه کافی است. هرچند بهره‌وری انرژی ابررایانه‌ها از سال ۲۰۱۹ تا ۲۰۲۵ به‌طور متوسط سالانه ۱.۳۴ برابر افزایش یافته، اما این بهبود نتوانسته رشد عظیم مصرف برق را جبران کند؛ چراکه توان مصرفی در همین بازه زمانی به‌طور تقریبی دو برابر افزایش یافته است. نمونه بارز این



وضعیت، ارتقای ابررایانه Colossus xAI است که با

هزینه ساخت حدود ۷ میلیارد دلار و توان مصرفی ۳۰۰ مگاوات، برقی معادل مصرف ۲۵۰۰۰۰ خانه را نیاز دارد. این یافته‌ها نشان می‌دهد که در کنار شتاب بی‌سابقه پیشرفت فناوری هوش مصنوعی، چالش اصلی پیش‌رو، تأمین انرژی مورد نیاز برای چنین محاسبات عظیمی است؛ بحرانی که ضرورت تغییرات بنیادین در طراحی، بهره‌برداری و تأمین انرژی مراکز داده هوشمند را بیش از پیش آشکار می‌سازد.

AI supercomputers may cost \$200B by 2030, demand power of 9 nuclear plants

گزارش

کشنده تر از بمب هسته‌ای!

گزارشی درباره وضعیت امنیت سایبری در ایران و نقاط ضعفی که باید رفع شوند

اشاره

جنگ ۱۲ روزه ایران و اسرائیل یک نکته را کاملاً روشن کرد: زیرساخت‌های دیجیتالی ایران در برابر حملات سایبری ضعیف و آسیب‌پذیر هستند. هک و از کار افتادن چندین بانک و طولانی شدن روند بازگشت دوباره آن‌ها به چرخه خدمات آنلاین، هک چند صرافی رمزارز و طلا، هک وبسایت‌های دولتی و مشکلات بزرگی که در این ایام رخ داد؛ زنگ خطر جدی برای امنیت سایبری کشور بود.

جنگ‌های امروزی دیگر تنها فیزیکی و سخت‌افزارمحور نیستند؛ بلکه با جنگ‌های ترکیبی روبرو هستیم که بخش بزرگی از آن‌ها، جنبه نرم‌افزاری و سایبری دارند. حملات سایبری در دنیای امروز، نقشی مهم‌تر از موشک، بمب یا تانک ایفا می‌کنند و می‌توانند مرگ‌آورتر، کشنده‌تر و فلج‌کننده‌تر از یک بمب هسته‌ای برای یک کشور باشند.

آمار از حملات سایبری در جنگ ۱۲ روزه

بهزاد اکبری درباره منشا این حملات هم می‌گوید: «در مقطعی حملات دی‌داس با حجم بسیار بالا افزایش یافت و در این مدت، حملات دی‌داس با حجم‌هایی تا ۴۰۰ گیگابایت در ثانیه گزارش شده است که بخشی از این حملات خارج از ایران انجام می‌شود و بخش دیگر در داخل کشور است.»

معاون وزیر ارتباطات ادامه می‌دهد: «برای مثال، حملات خارجی به داخل شبکه در یک بازه ۲۴ ساعته، حدود ۱۶ هزار و ۵۰۰ حمله بوده است، در حالی که حملات داخلی به خارج نیز حدود ۱۶ هزار و ۵۰۰ بوده و حملات داخلی به

اجازه بدهید ابتدا به یک بینش و چشم‌انداز دقیق درباره هجوم سایبری که طی دو هفته به زیرساخت‌های فناوری اطلاعات و اینترنت کشور شد؛ برسیم و بعد درباره ابعاد مختلف آن، صحبت کنیم. معاون وزیر ارتباطات و رئیس هیات مدیره و مدیرعامل شرکت ارتباطات زیرساخت طی گزارشی از وضعیت حملات سایبری در طول جنگ اخیر می‌گوید: «از دو روز قبل از جنگ تحمیلی رژیم صهیونیستی به کشورمان، حملات گسترده سایبری به کشور آغاز شد و تا چندین روز پس از آتش‌بس نیز ادامه داشت و حتی به ۴۰۰ گیگابایت در ثانیه رسید.»

جنگ ۱۲ روزه ایران و اسرائیل نشان داد زیرساخت‌های دیجیتال ایران در برابر حملات سایبری بسیار آسیب‌پذیرند و این هشدار جدی است که در جنگ‌های ترکیبی امروز، سایبری‌ها می‌توانند حتی از سلاح‌های هسته‌ای خطرناک‌تر باشند.



مالی خود دست یابند.» وی با اشاره به دلایل مهاجرت نیروهای متخصص گفت: «این نارضایتی‌ها باعث شد تا بسیاری از افراد کارآزموده و باتجربه، کشور را ترک کنند. اغلب این افراد با تکیه بر رزومه‌ی حرفه‌ای خود توانستند در کشورهای حاشیه‌ی خلیج فارس، اروپا و حتی ایالات متحده، به درآمدهای قابل توجهی دست یابند؛ چرا که شرکت‌های پیشروی جهان عمدتاً در همین حوزه‌های فناوری اطلاعات، ارتباطات و هوش مصنوعی فعالیت دارند.»

وی ادامه داد: «بر اساس تجربیات ما از تعامل با فعالان صنعت، یکی از چالش‌های اصلی این است که برخی از متخصصان احساس می‌کنند تأثیرگذاری‌شان در شرکت‌های داخلی کاهش یافته است. این مسئله دلایل مختلفی دارد؛ از جمله مشکلات اقتصادی،

از کشور، و گاهی بی‌توجهی سازمان‌های دولتی به متخصصان فعلی هشدار داده‌اند؛ جنگ ۱۲ روزه این ضعف را آشکارتر از همیشه نشان داد. «بهزاد اکبری» رئیس شرکت زیرساخت هم به این موضوع به عنوان پاشنه آشیل امنیت سایبری کشور اشاره می‌کند و در این باره می‌گوید: «در سال‌های اخیر، به دلیل مهاجرت گسترده، نیروهای متخصص در امنیت سایبری کاهش یافته و سازمان‌ها در تأمین نیروی انسانی کارآمد، دچار مشکل شده‌اند. این مشکل در سطح جهانی نیز وجود دارد، زیرا با رشد تحول دیجیتال، نیاز به منابع انسانی متخصص بیشتر احساس می‌شود و شرکت‌ها به سمت بهره‌گیری از خدمات امنیتی ابری رفته‌اند، اما در کشور ما، هنوز زیرساخت‌های لازم برای خدمات ابری داخلی شکل نگرفته است.»

سیدعلی حسینی، معاون مرکز تعاملات بین‌المللی علم و فناوری نیز بر همین موضوع تأکید دارد: «مهاجرت گسترده‌ی متخصصان فناوری اطلاعات و امنیت سایبری از ایران، نتیجه‌ی محدودیت‌های داخلی و جذابیت فرصت‌های بین‌المللی است.»

او ادامه می‌دهد: «حوزه‌هایی مانند هوش مصنوعی، برنامه‌نویسی حرفه‌ای و امنیت سایبری، در دوره‌ای درآمدهای بسیار بالایی برای متخصصان ایجاد کرده بودند. اما با تغییر ساختار شرکت‌ها و جابه‌جایی نیروها، بسیاری از این متخصصان نتوانستند به انتظارات فنی و

داخل حدود ۱۲ هزار مورد ثبت شده است. این حملات از ۱۷۰ کشور دنیا صورت می‌گیرد و اغلب توسط سازمان‌ها یا گروه‌های بزرگ و توزیع شده انجام می‌شود، به طوری که حملات حجیم نمی‌تواند توسط یک فرد یا گروه کوچک انجام شود.»

اما این حملات چگونه بر ضد زیرساخت کشور سازمان‌دهی می‌شوند؟ اکبری می‌گوید: «نکته مهم دیگر این است که حجم بالای حملات خارجی، عمدتاً توسط سازمان‌ها و گروه‌های بزرگ و با استفاده از شبکه‌های توزیع شده انجام می‌شود و این حملات به شدت سازمان‌یافته است. بخش زیادی از حملات داخلی ناشی از دستگاه‌های آلوده در داخل کشور است که مورد سوءاستفاده قرار می‌گیرند و این وضعیت، شبکه‌های داخلی را بسیار آسیب‌پذیر می‌سازد.

معاون وزیر ارتباطات خاطر نشان کرد: «وضعیت امنیتی شبکه در این مدت نشان‌دهنده حجم بالای حملات و پیچیدگی آن‌ها است، اما با وجود ظرفیت‌های موجود، تلاش می‌شود تا این حملات، مدیریت و کنترل شوند.»

اولین نقطه ضعف: کمبود نیروی خبره

سال‌ها است که کارشناسان امنیت شبکه و کامپیوتر نسبت به کمبود نیروی متخصص امنیت سایبری، مهاجرت این نیروها به خارج

اولین نقطه ضعف امنیت سایبری ایران، کمبود و مهاجرت نیروهای متخصص است که به دلیل محدودیت‌های داخلی و جذابیت فرصت‌های خارجی، پاشنه آشیل دفاع سایبری کشور شده است.



آسیب‌پذیری سایبری ایران
ریشه در سرورها و دستگاه‌های
آلوده، سیاست‌گذاری نادرست
در فیلترینگ، کمبود زیرساخت
ابری و نیروی متخصص دارد و
نیازمند تحول دیجیتال، بازنگری
سیاست‌ها و آموزش عمومی
برای مقابله با تهدیدات پیچیده و
هوشمند جهانی است.

ضعف زیرساخت‌های فنی، و سطح دانش فنی بالای این افراد که امکان بهره‌برداری مؤثر از توانمندی‌هایشان را محدود کرده است.» به گفته‌ی وی، امنیت سایبری امروز یکی از اولویت‌های اصلی در سطح بین‌الملل است و در بسیاری از کشورهای پیشرفته، ملیت افراد در این حوزه از اهمیت کمتری برخوردار است. امنیت یکی از چالش‌های کلیدی شرکت‌ها به شمار می‌رود و متخصصانی که در زمینه‌ی امنیت سایبری فعالیت دارند، معمولاً در اولویت جذب قرار می‌گیرند. ایرانی‌ها نیز سهم مهمی از این بازار جهانی را به خود اختصاص داده‌اند.

حسینی درباره نقش دولت در این زمینه می‌گوید: «نکته این است که متخصصان برجسته‌ی مهاجر در حوزه‌های مختلف، معمولاً چندان نیازی به حمایت مستقیم دولت ندارند. وظیفه‌ی دولت این است که زیرساخت‌های لازم را فراهم کند تا این افراد بتوانند بدون دغدغه به اکوسیستم فناوری کشور متصل شده، دانش خود را منتقل کرده و به کار بگیرند. اغلب این متخصصان تمایل دارند شرکت‌های خود را در ایران راه‌اندازی کنند و به فعالیت بپردازند. بنابراین دولت باید شرایط را به گونه‌ای تسهیل کند که این فعالیت‌ها به راحتی امکان‌پذیر باشد.»

سرورها و گوشی‌های آلوده؛ سربازان نفوذی دشمن در داخل

دومین نقطه ضعف بزرگ امنیت سایبری ایران، میلیون‌ها گوشی و دستگاه آلوده به فیلترشکن‌های رایگان است.

اکبری در گزارش خود اشاره دارد: «استفاده گسترده از نرم‌افزارهای ناامن و سخت‌افزارهای وارداتی دست دوم، به ویژه در حوزه سرورها و تجهیزات شبکه، باعث افزایش آسیب‌پذیری شبکه‌های داخلی شده است. تحریم‌ها در سال‌های گذشته منجر به واردات سرورهای دست دوم و سخت‌افزارهای آلوده شده است که این تجهیزات در زنجیره تأمین قرار دارند و امکان آلوده‌سازی و نفوذ به شبکه‌ها را آسان‌تر می‌کنند.» مدیرعامل شرکت ارتباطات زیرساخت تأکید دارد که استفاده زیاد از وی‌پی‌ان‌ها و نرم‌افزارهای غیرمطمئن، شبکه‌های داخلی را بیشتر در معرض تهدید قرار داده است.

«محمد کشوری»، مدیرعامل گروه طیف و از کارشناسان باسابقه ارتباطات، نیز با اشاره به حملات سایبری اخیر به زیرساخت‌های کشور، تأیید کرد که بخشی از این حملات نه از بیرون، بلکه از درون شبکه ملی و از سوی دستگاه‌های کاربران ایرانی انجام می‌شود. به گفته وی، کاربرانی که گوشی‌هایشان به واسطه فیلترینگ، استفاده از فیلترشکن و ترافیک ناایمن، ناخواسته به «زامبی‌های سایبری» تبدیل شده‌اند، در این حملات نقش دارند. «کشوری» بیان کرد که در سطح جهانی، حملات DDOS موضوع پیچیده‌ای نیست و راه‌حل‌های فنی متعددی برای مقابله با آن وجود دارد، اما ایران همچنان نسبت به این حملات آسیب‌پذیر است. «کشوری» این واقعیت را بیان می‌کند که وقتی بخش زیادی از پهنای باند کشور از طریق VPN‌ها و روی

سرورهای ناشناس و غیرقابل ردیابی عبور می‌کند، عملاً شبکه ملی از کنترل زیرساخت خارج می‌شود و حتی نظارت پایه‌ای نیز با مشکل جدی روبرو می‌شود.

سیاست‌گذاری اشتباه و عدم شفافیت

مدیرعامل شرکت زیرساخت با انتقاد از شیوه فعلی سیاست‌گذاری، بیان کرد: «در حال حاضر، نهادهای خاصی بدون حضور نمایندگان فنی یا بخش خصوصی درباره دسترسی به اینترنت تصمیم می‌گیرند. این وضعیت باعث می‌شود کسب‌وکارها ناگهان با تصمیماتی مواجه شوند که بدون هیچ توضیح یا پاسخگویی، بر معیشت آن‌ها تأثیر می‌گذارد.» اکبری بر نیاز مبرم به شفافیت و پاسخگویی واقعی در این حوزه تأکید کرد و افزود: «تصمیم‌گیری درباره قطعی اینترنت، باید تنها در موارد بسیار بحرانی و به صورت کاملاً مقطعی اتفاق بیفتد.»

کشوری هم معتقد است: «بخشی از آسیب‌پذیری امنیتی کشور فقط فنی نیست، بلکه ریشه در تصمیم‌ها و سیاست‌های غلط دارد. او در ادامه به آسیب‌های سیاست فیلترینگ اشاره می‌کند و می‌گوید که سال‌هاست بر سر بستن پلتفرم‌ها بحث وجود دارد؛ در حالی که همین پلتفرم‌ها سهم بزرگی از پهنای باند کشور را به خود اختصاص



بدافزارهایی است که به نظر می‌رسد با کمک هوش مصنوعی تولید شده و نوعی هوشمندی از خود نشان می‌دهند. این امر نشان‌دهنده قرار گرفتن ایران در جریان اصلی تهدیدات سایبری جهانی است.

به طور خلاصه، تهدیدات سایبری امروزه پیچیده‌تر، سازمان‌یافته‌تر و پرتعدادتر شده‌اند و انگیزه‌هایی از مالی تا اهداف سیاسی و جاسوسی را در برمی‌گیرند. سازمان‌ها و افراد باید با آموزش مستمر، به‌روزرسانی سیستم‌ها و استفاده از راهکارهای امنیتی پیشرفته از دارایی‌های خود محافظت کنند.

در ایران، مانند بسیاری از کشورهای در حال توسعه، برخی حوزه‌ها به دلایل فنی، مدیریتی و زیرساختی مورد توجه جدی مهاجران سایبری هستند. مهم‌ترین عامل این آسیب‌پذیری‌ها، کمبود آموزش‌های تخصصی و آگاهی رسانه‌ای عمومی است.

نرم‌افزارهای هکی، همگی به عوامل جدی برای آسیب‌پذیری زیرساخت‌های کشور تبدیل شده‌اند.»

رئیس سازمان زیرساخت معتقد است: «ساختار تصمیم‌گیری درباره اینترنت در کشور نیازمند بازنگری اساسی است.» او از بی‌پاسخ ماندن تصمیم‌های کلان در حوزه اینترنت انتقاد کرد و بیان داشت که وزارت ارتباطات و سایر نهادهای ذی‌ربط باید در این تصمیم‌گیری‌ها نقش فعال‌تری داشته باشند.

تحول و پیچیدگی تهدیدات سایبری در ایران و جهان

تهدیدات سایبری به یکی از چالش‌های اصلی امنیتی جهان تبدیل شده‌اند و حوزه‌های هدف و روش‌های حملات به طور مداوم در حال تغییر و پیچیده شدن هستند. در ایران، تهدیدات همپوشانی‌های زیادی با روندهای بین‌المللی دارند؛ از جمله: افزایش پیچیدگی حملات، گسترش مهندسی اجتماعی، و حملات زنجیره تأمین.

در ایران، تهدیدات به ترتیب متوجه حوزه‌های سیاسی و حاکمیتی، ارتباطات، بانکی، و انرژی هستند. نکته قابل توجه، کشف آلودگی‌ها و

داده‌اند. به گفته وی، وقتی این بسترها مسدود می‌شوند، دولت برای جلوگیری از دور زدن محدودیت‌ها ناچار می‌شود فشار بیشتری به مسیرهای ارتباطی وارد کند. نتیجه این می‌شود که کاربران برای دسترسی به فیلترشکن‌ها روی می‌آورند و همین ابزارها گاهی دستگاه کاربران را خواسته به بخشی از حمله تبدیل می‌کنند. به گفته «محمد کشوری»، مدیرعامل گروه طیف، «فیلترینگ نه تنها امنیت را به ارمغان نیاورده، بلکه نظارت مؤثر بر شبکه را نیز از بین برده است.»

راهکار ارتقای امنیت سایبری: تحول دیجیتال، سرویس‌های ابری و بازنگری در سیاست‌ها

بهباد اکبری درباره دلایل آسیب‌پذیری امنیت زیرساخت ارتباطی کشور تأکید کرد: «راهکار جهانی برای مقابله با بحران‌های سایبری، حرکت به سمت تحول دیجیتال، پیاده‌سازی امنیت به عنوان خدمت (Security as a Service)، و استفاده از زیرساخت‌های پیشرفته ابری است». او تصریح کرد که این رویکردها باید در ایران نیز دنبال شود. به گفته وی: «نبود سرویس‌های ابری با کیفیت در کشور، عدم حرکت به سمت تحول دیجیتال و همچنین مواردی نظیر کمبود نیروی متخصص و وجود

وقتش رسیده اتاق سرور کوچک خود را تبدیل به دیتاسنتر کنید؟

شاید هنوز اتاق سرور شما خوب کار کند ولی پاسخگوی سرویسهای جدید و افزایش ترافیک دیتاهای ورودی نباشد و ارتقا به دیتاسنتر یک راه حل است!



منبع: datacenterknowledge.com

مترجم: گلنوش کزازی

مقاله فنی

اشاره

به ندرت پیش می آید که یک کسب و کار از همان ابتدا، دیتاسنتر راه اندازی کند. مسیر رایج و منطقی تر، ایجاد یک اتاق سرور برای شروع با یک سرور ورک و بعد افزایش آن ها به چند رک و سرور و تجهیزات ذخیره سازی است. اما در این سفر، از یک نقطه ای به بعد، نیازمند ارتقا به دیتاسنتر هستید؛ جایی که سرویس های فناوری اطلاعات شما گسترش پیدا کردند؛ مشتریان شما چند برابر شدند و به ظرفیت های جدید نیاز دارید.

بنابراین، این سوال مطرح می شود که چه زمانی باید یک کسب و کار، اتاق سرور خود را با یک مرکز داده، جایگزین کند؟ و در هنگام این ارتقا، کدام ملاحظات امنیتی، کارایی، هزینه و غیره در نظر گرفته می شود؟

در این مقاله، برای کسب و کارهایی نوشته شده که اکنون اتاق سرور دارند و دقیقاً در نقطه جایگزینی آن با یک دیتاسنتر اما با انبوهی سوال پاسخ نگرفته هستند:

اتاق سرور در برابر دیتاسنتر: چه تفاوتی دارند؟

• **دیتاسنتر:** تأسیساتی بزرگ است که می تواند هزاران سرور را در خود جای دهد و برای پشتیبانی از عملیات گسترده طراحی شده است.

سیستم های سرمایش

• **اتاق سرور:** از سیستم های تهویه مطبوع معمولی برای خنک سازی استفاده می کند؛ مثلاً یک یا دو کولر گازی در اتاق سرور نصب شده است.

• **دیتاسنتر:** از فناوری های پیشرفته تری

اتاق سرور و دیتاسنتر هر دو برای میزبانی تجهیزات فناوری اطلاعات طراحی شده اند، اما تفاوت های اساسی در مقیاس، زیرساخت، امنیت و قابلیت اطمینان دارند. عمده ترین این تفاوت ها عبارتند از:

مقیاس و ظرفیت

• **اتاق سرور:** فضایی کوچک در داخل یک ساختمان است که معمولاً چند ده سرور را میزبانی می کند.

اتاق سرور و دیتاسنتر هر دو برای میزبانی تجهیزات IT هستند، اما دیتاسنترها در مقیاس بزرگ تر، با امنیت، پایداری و سرمایش پیشرفته طراحی شده اند. وقتی فضای اتاق سرور کم می شود، قطعی های مکرر دارید یا روی سرورهای گران قیمت سرمایه گذاری می کنید، وقت آن رسیده به دیتاسنتر مهاجرت کنید. گزینه های جایگزین مثل کلوکیشن یا رایانش ابری هم وجود دارند. تصمیم گیری درست، بستگی به نیاز، بودجه و آینده فناوری شما دارد.



Is It Time to Replace Your Server Room with a Data Center?

چگونه بفهمیم دیگر اتاق سرور ما کافی نیست؟

برای برخی شرکت‌ها، انتخاب بین مرکز داده و اتاق سرور کاملاً واضح است. یک اتاق سرور، ایده‌آل‌ترین گزینه برای یک کسب‌وکار کوچک و مشاغل تازه شکل گرفته است که نیاز به سرویس‌ها و زیرساخت‌های گسترده فناوری اطلاعات ندارند. اما سازمان‌های بزرگ یا شرکت‌های تجاری که قدمت طولانی دارند؛ معمولاً نیاز به مرکز داده دارند.

برای شرکت‌های با اندازه متوسط، کار کمی سخت می‌شود و انتخاب میان اتاق سرور و دیتاسنتر، راحت و شفاف نیست. اگر یک کسب‌وکار، سال‌ها با یک اتاق سرور کار کرده باشد؛ اغلب هیچ نشانه‌ای وجود ندارد که بتوان بفهمید زمان ارتقا به یک مرکز داده فرا رسیده است. این خطر وجود دارد که انجام این کار، بدون اینکه ضروری باشد و زودتر اتفاق بیفتد؛ هزینه زیادی در پی داشته باشد. بنابراین، مسئله این است که چگونه تشخیص دهید اتاق سرور شما دیگر کافی نیست و یک مرکز داده بهتر است؟ در بیشتر اوقات، تصمیم‌گیری شما وابسته به عوامل زیر است:

• **دیتاسنتر:** با داشتن منابع تغذیه پشتیبان، سیستم‌های خنک‌کننده افزونه و طراحی‌های مقاوم، قابلیت اطمینان بالاتری دارد. به طور کلی، مراکز داده پیشرفته‌تر هستند و برای پشتیبانی از نیازهای فناوری اطلاعات در مقیاس‌های بزرگ و پیچیده، مناسب‌تر از اتاق‌های سرور خواهند بود.

مانند خنک‌سازی مایع یا غوطه‌وری بهره می‌برد که کارایی بالاتری دارند.

امنیت فیزیکی

• **اتاق سرور:** معمولاً فقط با قفل درب محافظت می‌شود یا نهایت یک دوربین مداربسته و اثر انگشت دارند.

• **دیتاسنتر:** دارای لایه‌های متعدد امنیتی از جمله احراز هویت بیومتریک، نظارت و کنترل دسترسی پیشرفته، انواع حسگرها و سیستم‌های نظارتی آنلاین است.

بهره‌وری انرژی و پایداری

• **اتاق سرور:** به دلیل محدودیت‌های فضا و منابع، کمتر به بهره‌وری انرژی توجه دارد.

• **دیتاسنتر:** اغلب از منابع انرژی تجدیدپذیر و طراحی‌های پایدار برای کاهش مصرف انرژی استفاده می‌کند؛ ضمن اینکه منابع انرژی افزونه و پشتیبان مانند ژنراتورهای برق دارند.

قابلیت اطمینان و افزونگی

• **اتاق سرور:** ممکن است فاقد سیستم‌های پشتیبان قوی باشد و در برابر قطعی‌ها آسیب‌پذیرتر است.

اتاق سرور برای میزبانی محدود سرورها در مقیاس کوچک طراحی شده، در حالی که دیتاسنتر با زیرساخت پیشرفته، امنیت بالا و قابلیت اطمینان بیشتر، برای پشتیبانی از عملیات‌های گسترده و حیاتی مناسب است.

۱- فضای ناکافی برای سرورهای جدید

احتمالا رایج‌ترین دلیل مهاجرت از اتاق سرور به دیتاسنتر، فضای فیزیکی رو به اتمام است. اگر نیاز دارید رک‌ها و سرورهای بیشتری نصب کنید ولی اتاق سرور گنجایش رک و سرور جدید ندارد؛ به وضوح مشخص است شما نیاز به یک مرکز داده دارید و باید با اتاق سرور محدود و کوچک، خدا حافظی کنید.

۲- سرمایه‌گذاری روی سرورهای پیشرفته

هرچه سرورهای شما گران‌تر باشند؛ منطقی‌تر است در یک مرکز داده به کار گرفته شوند تا در یک اتاق سرور، اگر سرورهای ارزان قیمت و معمولی دارید؛ اگر برایشان مشکلی پیش بیاید؛ مثلاً بر اثر نشتی آب یا گرمای زیاد یا مشکلات قطعی برق، به آن‌ها آسیبی وارد شود؛ کمتر ضرر کردید اما وقتی دارید یک سرور گران قیمت برای کارهای سنگین، مثلاً هوش مصنوعی یا ارائه سرویس‌های آنلاین به هزاران نفر، می‌خرید و نصب می‌کنید؛ احتمالاً باید سیستم سرمایشی، شبکه توزیع برق، برق اضطراری پشتیبان، سیستم کابل‌کشی استاندارد و ساختار یافته و انواع حسگرهای دما و رطوبت را هم راه‌اندازی کنید تا از این سرور، نگهداری کنند و سرمایه شما به هدر نرود.

۳- قطعی‌های زیاد سرویس‌های IT

اگر با مشکل قطعی یا خرابی زیاد سرورها روبرو هستید؛ نشانه خوبی برای مهاجرت به یک مرکز داده است. به‌ویژه، اگر این قطعی‌ها ذاتاً به مسایل اتاق سرور ارتباط پیدا می‌کنند. مثلاً، بار ترافیکی زیادی روی سرورها هست و مرتباً خراب می‌شوند یا گرمای زیادی در اتاق سرور تولید می‌شود و باعث از کار افتادن تجهیزات الکترونیکی می‌شود. خرابی سیستم برق ساختمان نیز دلیلی است که شما را به سوی ساخت یک دیتاسنتر هدایت می‌کند.

۴- چالش‌های کارایی شبکه

اگر احساس می‌کنید عملکرد بخش شبکه اتاق سرورتان ضعیف است؛ دلیل خوبی برای رفتن به سوی یک دیتاسنتر اختصاصی است. دیتاسنترها پهنای باند بیشتری دارند و نسبت به اتاق سرورها که محدود به یک ساختمان و زیرساخت شبکه شدند؛ دسترسی‌ها و ظرفیت‌های بیشتری ارائه می‌کنند. ضمن اینکه دیتاسنترها از نظر محل استقرار سرورها، پیکربندی‌های مختلف و استفاده از تجهیزات گوناگون، انعطاف‌پذیری بیشتری دارند. مثلاً، شما می‌توانید از دیتاسنترهای موبایل یا دیتاسنترهای لبه در نزدیکی محل زندگی مشتریان استفاده کنید تا سرویس‌های سریع‌تر و با کیفیت‌تری دریافت کنند اما اتاق سرور حتماً باید در ساختمان شرکت باشد.

جایگزین‌هایی برای اتاق سرور و دیتاسنتر

همیشه ارتقای یک اتاق سرور به مرکز داده، تنها گزینه نیست و راه‌حل‌های دیگر در دنیای فناوری وجود دارد:

- به جای ساخت یک دیتاسنتر اختصاصی داخل شرکت‌تان، از کلوکیشن‌ها یا اجاره فضا در دیتاسنترهای اشتراکی استفاده کنید.
- انتقال کل حجم بار کاری یا برخی سرویس‌ها و دیتاها به ابر عمومی که نیاز به زیرساخت خصوصی نخواهد داشت.
- سرمایه‌گذاری روی یک دیتاسنتر کوچک و قابل حمل که ارزان‌تر و انعطاف‌پذیرتر از یک دیتاسنتر سنتی و ثابت است. دیتاسنترهای موبایل، برخلاف اتاق‌های سرور، دارای سیستم سرمایشی، سیستم برق و امنیت پیشرفته‌تر و یکپارچه‌ای هستند.

نتیجه‌گیری

وقتی اتاق سرور شما دیگر جوابگو نیست؛ گزینه‌های زیادی دارید اما بزرگ‌ترین چالش، تصمیم‌گیری درباره زمان مهاجرت به راه‌کارهای جدید و عبور از یک اتاق سرور سنتی است. در اولین نگاه، مراکز داده برای هر کسب‌وکاری جذاب هستند ولی لزوماً برای همه آن‌ها مناسب نیستند و شاید بهتر باشد ابتدا به یک سرویس کلوکیشن یا ابر عمومی منتقل شوند و پس از چند سال و گسترش سرویس‌های IT، یک دیتاسنتر اختصاصی بسازند.



اگر اتاق سرور شما با کمبود فضا، قطعی‌های مکرر، گرمای زیاد یا عملکرد ضعیف شبکه مواجه است، زمان آن رسیده به دیتاسنتر مهاجرت کنید. دیتاسنترها زیرساختی حرفه‌ای‌تر با امنیت، سرمایش و پایداری بالاتر دارند. البته گزینه‌هایی مانند کلوکیشن یا انتقال به ابر نیز می‌توانند جایگزین‌های منطقی‌تری باشند.

برگزاری وبینارهای تخصصی

شرکت تیام شبکه، در سال های اخیر اقدام به برگزاری
سمینارهای حضوری در استان های مختلف و وبینارهای آنلاین
کاملاً تخصصی و آموزشی در حوزه های مختلف مراکز داده
و مدیریت فروش با موضوعات زیر کرده است:

- بایدها و نبایدهای استاندارد TIA-۹۴۲

- تداوم و پایداری مراکز داده

- مفاهیم کاربردی در طراحی مرکز داده

- راهکارهای سرمایه‌گذاری مرکز داده و ..

- چرا موبایل دیتاسنتر سیار؟

- بازاریابی صنعتی

- اصول و فنون مذاکره

شرکت در این وبینارها

رایگان است.



اسکن و ثبت نام کنید.



برای ثبت نام در سمینارها
و وبینارها، کیو آر کد روبرو را
اسکن کنید.



تلفن گویا: ۹۱۰۷۲۳۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
اپراتور: ۰۰۰ ۶۶۹۴۷۲۰۰
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

چگونه بدون اخراج کارمندان، هزینه‌ها را کاهش دهیم؟

تعدیل نیرو راه‌حلی کوتاه مدت برای مشکلات بلندمدت است

منبع: forbes.com



مترجم: زهره اسماعیلی

مقاله مدیریت

اشاره

پس از درگیری‌های خرداد ماه، اکوسیستم زیست فناوری ایران دچار شوک و رکودی وحشتناک شد و اقتصاد دیجیتال ضربه‌ها و آسیب‌های جبران‌ناپذیری خورد؛ آسیبی که نتایج آن بلافاصله در تعدیل گسترده نیروی انسانی شرکت‌ها بروز کرد. مدیران شرکت‌ها برای کاهش هزینه‌ها، به سراغ اولین گزینه و ساده‌ترین راه‌کار رفتند و بین ۱۵ تا گاهی ۴۰ درصد از نیروهای خود را اخراج کردند؛ تصمیمی برای بقا و تلاشی برای ادامه مسیر که شاید واکنشی سریع به یک شوک غافل‌گیرکننده بود. این وضعیت، منحصر به ایران نیست. در سراسر جهان، در دل بحران‌های اقتصادی یک الگوی قابل پیش‌بینی وجود دارد: شرکت‌ها شوکه می‌شوند؛ رهبران کسب‌وکارها برای عبور از طوفان، هزینه‌ها را کاهش می‌دهند و در پی آن اخراج‌ها آغاز می‌شود یا جلوی استخدام‌های جدید گرفته می‌شود.

اما آیا تعدیل نیرو بهترین راه‌کار در زمان بروز بحران‌های اقتصادی یا شرایط جنگی است؟ آیا گزینه‌های کم هزینه‌تری نسبت به از دست دادن نیروهایی که سال‌ها آموزش دیده‌اند، مهارت کسب کرده‌اند، در پلتفرم‌ها رشد یافته‌اند و اکنون به دوران بهره‌وری رسیده‌اند؛ وجود ندارد؟ ما هرگز به جای رهبران و مدیران کسب‌وکارها نیستیم و فشار، استرس و نگرانی‌های سایه افکننده بر ذهن و تصمیم‌های آنان را درک نمی‌کنیم اما می‌خواهیم به سراغ راه‌حل‌های دیگری برای کاهش هزینه‌ها، بدون اخراج کارمندان برویم؛ راه‌حلی که شاید و باز تاکید می‌کنیم که شاید برخی شرکت‌های فناوری ظرفیت بهره‌گیری از آن‌ها را داشته باشند.

تمرکز بر بهره‌وری: جسورانه اما پرخطر

ایلان ماسک به محض خرید توییتر که اکنون «ایکس» نامیده می‌شود؛ دست به اقدامی جنجالی زد و ۸۰ درصد کارمندان را تعدیل کرد. این تصمیم بی‌شک بدون آسیب نبود و به ماسک نشان داد که تاکید و تمرکز بر بهره‌وری، بهتر از ایجاد تغییرات شدید در نیروی انسانی است. او در سال‌های بعد، هنگامی که وارد وزارت خانه بهره‌وری دولت شد؛ به بهره‌وری

فراتر از یک استراتژی مالی نگاه کرد و در پی تبدیل آن به یک فرهنگ بود. شاید اخراج‌ها و تعدیل نیروهای گسترده، باعث صرفه‌جویی‌های سریع شوند، اما تیم‌ها را بی‌ثبات می‌کنند و به روحیه کارکنان آسیب وارد خواهند کرد؛ در نتیجه، در بلندمدت شاهد افت کارایی و بهره‌وری خواهید بود. بهتر است پیش از تصمیم به اخراج کارمندان، بررسی کنید که آیا راهی برای افزایش بهره‌وری و جبران افزایش هزینه‌ها وجود دارد؟ با همین

در بحران‌های اقتصادی، شرکت‌ها به تعدیل نیرو روی می‌آورند، اما شاید راهکارهای کم هزینه‌تری برای کاهش هزینه‌ها بدون از دست دادن سرمایه انسانی وجود داشته باشد.



How To Cut Costs Without Laying Off Employees

کارمندان فعلی، چند درصد می‌توان تولید و کارایی را افزایش داد و این افزایش چه میزان آورده مالی خواهد داشت؟

هزینه‌های پنهان اخراج کارمندان

وقتی کسب‌وکارها برای کاهش هزینه‌ها عجله می‌کنند؛ معمولاً نخستین اقدامشان اخراج بخشی از نیروی انسانی است؛ راهی سریع و قابل مشاهده برای کاهش هزینه‌ها، اما همراه با پیامدها و هزینه‌های پنهانی که کمتر به چشم می‌آیند:

- تخصص‌های از دست رفته: کارمندانی که از شرکت اخراج می‌شوند (یا جدا می‌شوند)، سال‌ها دانش، تجربه و مهارتی با خود می‌برند که جایگزینی آن در فرد جدید، زمان‌بر و پرهزینه است.
- افت روحیه: کارمندانی که باقی می‌مانند؛ مدام با این پرسش مواجه هستند که «آیا نفر بعدی، من هستم؟» در چنین فضایی، صحبت از بهره‌وری و کارایی بالا، تقریباً غیرممکن است.
- آسیب به اعتبار برند: اخراج‌ها، به ویژه در صنایعی که مزیت رقابتی بر پایه نیروی متخصص بنا شده، می‌تواند باعث کاهش اعتبار و جایگاه یک برند در بازار شود.
- پس، شاید بهتر باشد این‌طور بگوییم: اخراج نیروی انسانی، راه‌حلی کوتاه مدت برای مشکلی بلندمدت است. رهبران شرکت‌ها،

باید به جای تمرکز بر تعداد کارمندان، از خود بپرسند: کجا بیش از حد هزینه می‌کنیم؟ چه ناکارآمدی‌هایی در سیستم وجود دارد و ما از آن‌ها غفلت کرده‌ایم.

با بهره‌وری‌های سازنده شروع کنید؛ نه مخرب

- بهره‌وری واقعی به معنای کاهش بی‌رویه بودجه نیست؛ بلکه به معنای شناسایی فرصت‌های مناسب برای بهینه‌سازی است. ما با کسب‌وکارهایی روبرو بودیم که بدون دست زدن به تعداد کارمندان (بدون کاهش حتی یک نفر از نیروها)، توانسته‌اند میلیاردها دلار صرفه‌جویی کنند. رویکردهای بدون تعدیل نیرو، وقتی به جای تمرکز کورکورانه بر بودجه، بر مدیریت هزینه‌های ثابت متمرکز شوند، می‌توانند برای یک سازمان، معجزه‌آفرین باشند. پیش از هر اقدامی، سه اصل کلیدی را برای کاهش هزینه‌ها مدنظر قرار دهید:
- اختلال حداقلی: دستیابی به صرفه‌جویی‌ها بدون ایجاد اختلال در عملیات روزانه.
- مدیریت فعال: بهینه‌سازی مداوم و مستمر به جای اقدامات ناگهانی و مخرب.

- روابط بهتر با تامین‌کنندگان: ایجاد مشارکت و همکاری، برای ارزش‌های بلندمدت.

صورت‌حساب‌هایتان را با دقت بازرسی و حسابرسی کنید. در بسیاری از موارد، در صورت‌حساب‌ها و پرداخت‌ها به اپراتورها، فروشندگان، نمایندگان شهرستانی و ... اشتباهاتی رخ می‌دهد که می‌تواند منشا صرفه‌جویی‌های قابل توجهی باشد. هزینه‌های ثابت و تکراری را زیر نظر بگیرید و راه‌هایی برای کاهش آن‌ها پیدا کنید؛ مانند هزینه آب، برق، خریدهای روزانه و تن‌خواه‌ها. گاهی اوقات با تغییر فروشگاهی که خریدهای روزمره شرکت از آن انجام می‌شود؛ می‌توانید هزینه‌ها را کاهش دهید یا با تغییر رویکردهای مالیاتی و بیمه‌ای، از بروز ضررها و جریمه‌ها جلوگیری کنید.

تغییر فرهنگ سازمانی به سوی بهره‌وری

مشکل اینجا است که بسیاری از شرکت‌ها، تا زمانی که با بحران اقتصادی مواجه نشوند؛

باب گفت‌وگوهای درون سازمانی برای افزایش کارایی و بهره‌وری را باز نمی‌کنند. در شرایط اقتصادی کنونی، بهره‌وری نه یک کالای لوکس، بلکه یک ضرورت و استراتژی برای رشد است. به ویژه در شرکت‌های خصوصی، تغییر فرهنگ به سوی افزایش بهره‌وری، با هر یک دلار صرفه‌جویی، مستقیماً روی حاشیه سود، تاثیرگذار است. حتی شرکت‌های دولتی نیز اکنون فشار فزاینده‌ای را برای انجام کارهای بیشتر با منابع کمتر تجربه می‌کنند. پیام واضحی در این بازار وجود دارد: بهره‌وری اختیاری نیست؛ بلکه مسیری رقابتی برای باقی ماندن در بازی است!

در بحران‌هایی مثل رکود یا تحریم، بسیاری از شرکت‌ها به تعدیل نیرو روی می‌آورند؛ اما این کار باعث از دست رفتن استعدادها، کاهش انگیزه و آسیب به برند می‌شود. به جای اخراج، می‌توان با تمرکز بر بهره‌وری، تعریف پروژه‌های سودآورتر و ورود به بازارهای جدید هزینه‌ها را مدیریت کرد. این رویکرد علاوه بر حفظ سرمایه انسانی، مزیت رقابتی سازمان را تقویت کرده و مسیر عبور موفق از بحران را فراهم می‌کند.

ایجاد تعادل میان جسارت و پایداری

اخراج‌های گسترده و تعدیل نیروی شدید، یک تصمیم جسورانه و پرخطر است که اغلب هزینه‌های سنگینی برای سازمان به همراه دارد و تبعات آن می‌تواند تا سال‌ها باقی بماند. برخی مدیران این ریسک را می‌پذیرند و وارد کردن یک شوک بزرگ و ناگهانی به کل مجموعه را بهتر از مرگ تدریجی و آرام کسب‌وکارشان می‌دانند. این رویکرد همیشه منفی نیست و در برخی مواقع نتیجه‌بخش بوده است، اما رویکرد هوشمندانه‌تر حرکت به سمت بهره‌وری واقعی و پرهیز از تصمیم‌های با ریسک بسیار بالاست. بهره‌وری واقعی به معنای کاهش بی‌هدف هزینه‌ها نیست؛ بلکه به معنای

کاهش هدفمند و متناسب آنها است. به بیان دیگر، بهره‌وری باید از رشد و توسعه سازمان پشتیبانی کند؛ نه اینکه با تضعیف چارت سازمانی، باعث خالی شدن برخی پست‌ها و اتاق‌ها شود. سازمان‌ها زمانی قوی‌تر و تاب‌آورتر می‌شوند که با شناسایی و هدف قرار دادن هزینه‌های ثابت و جلب مشارکت بیشتر تیم‌ها در فرآیندها، بتوانند بدون به خطر انداختن ارزش‌ها، دارایی‌ها یا آسیب زدن به برند خود، صرفه‌جویی‌های معنادار و پایداری ایجاد کنند.



دورکاری

و تغییر در روش‌های همکاری

یکی دیگر از رویکردهای موثر در زمان بحران‌های اقتصادی، بازنگری در نوع همکاری با کارکنان است. این رویکرد در دوران کووید ۱۹ مورد توجه قرار گرفت و بسیار خوب جواب

داد. سازمان‌ها می‌توانند برخی از کارکنان را به دورکاری بفرستند تا بخشی از هزینه‌ها (مانند انرژی، اینترنت، تجهیزات، نظافت و پذیرایی) کاهش یابد. علاوه بر آن، می‌توان نوع قراردادهای را بازنگری کرد و نوع همکاری متفاوتی را به کار گرفت؛ مانند کاهش ساعت کاری، دادن مرخصی بدون حقوق، یا همکاری به صورت پاره‌وقت و پروژه‌ای. این روش باعث می‌شود ارتباط با نیروی متخصص و ماهر حفظ شود و از دانش و تجربه‌اش استفاده کنید، در عین حال فشار هزینه‌های حقوقی کاهش یابد. رویکرد دیگر می‌تواند جابه‌جایی کارمندان و بازآموزی (Reskilling) آن‌ها باشد. براساس تغییرات بازار، شاید نیاز باشد کارمندان یک بخش کمتر شوند و به کارمندان بخش دیگری اضافه شود، یا آموزش‌ها و مهارت‌های جدیدی برای قبول مسئولیت‌های تازه تعریف شده، ببینند. مفهوم Reskilling برای استفاده از نیروهای موجود در حوزه‌های درآمدزا و اجرای پروژه‌های جدید با منابع انسانی فعلی، در قالب استارت‌آپ‌های درون سازمانی یکی از مهم‌ترین اصلاحات کسب‌وکارهای چابک، پس از بحرانی مانند جنگ است.

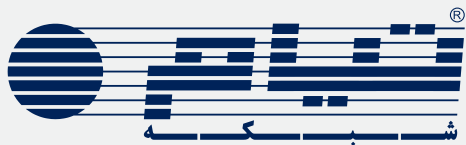
نتیجه‌گیری

در شرایط بحرانی مثل رکود اقتصادی، جنگ، یا تحریم، بسیاری از کسب‌وکارها به‌ویژه در حوزه فناوری به ناچار برای بقا، به سراغ تعدیل نیرو می‌روند. اما اخراج کارکنان نه تنها از نظر اخلاقی چالش‌برانگیز است، بلکه در بلندمدت نیز آسیب‌هایی به همراه دارد؛ از جمله از دست رفتن استعدادها، کاهش انگیزه نیروهای باقی مانده، لطمه به اعتبار برند، و تحمیل هزینه‌های سنگین برای جذب و آموزش مجدد در آینده و...

به جای این رویکرد، در این شرایط سازمان‌ها می‌توانند با تمرکز بر بهره‌وری واقعی، تعریف پروژه‌های سودآورتر، ورود به بازارهای جدید پرسودتر، افزایش مشارکت کارکنان در بهبود کارایی، و بازتعریف نقش‌ها و نوع همکاری، مسیر رشد و تاب‌آوری را در پیش بگیرند. چنین راهبردهایی علاوه بر کاهش فشار هزینه‌ها، به حفظ سرمایه انسانی و تداوم مزیت رقابتی نیز کمک می‌کنند و امکان عبور موفق از بحران را بدون آسیب جدی به ساختار سازمان فراهم می‌سازند.



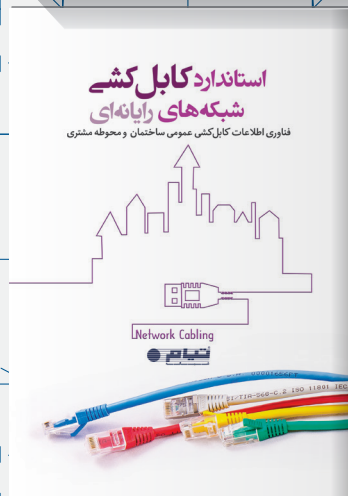
اسکن کنید!



با مسئولیت محدود



نخستین ترجمه رسمی
استانداردهای جهانی
دیتاسنتر با حمایت مالی
شرکت تیام شبکه
منتشر شد.



خطرات بالقوه ربات‌ها و هوش مصنوعی



۱

تجاوز به حریم خصوصی

فناوری‌هایی مانند تشخیص چهره، می‌توانند بدون رضایت کاربران، اطلاعات شخصی آن‌ها را جمع‌آوری و تحلیل کنند. هوش مصنوعی پتانسیل به خطر انداختن حریم خصوصی کاربران را از طریق فناوری‌هایی مانند تشخیص چهره دارد.

۲

بیکاری انسان‌ها

هرچه قدر هوش مصنوعی پیشرفته‌تر شود؛ مشاغل بیشتری را تصاحب کرده و جایگزین مشاغل می‌شود که به طور سنتی توسط انسان‌ها انجام می‌شدند.



۳

ربات‌های قاتل

سیستم‌های سلاح خودمختار، دیگر صرفاً در فیلم‌های علمی‌تخیلی نیستند و در دنیای واقعی می‌توانند اهداف از قبل تعریف شده را شناسایی کرده، و براساس یک سری دستورالعمل‌های از پیش تعیین شده و بدون دخالت انسان‌ها هدف را نابود کنند؛ تهدیدی جدی برای امنیت جهانی.





۰۴

تروریسم هوش مصنوعی

ابزارهای هوش مصنوعی، می‌توانند تبدیل به بهترین یار تروریست‌ها در حملات مختلف شوند. از جمع‌آوری داده و تجزیه و تحلیل الگوها گرفته، تا پیش‌بینی نتایج و شناسایی اهداف و حتی اجرای حملات سایبری!



۰۵

سوگیری هوش مصنوعی

از آنجا که الگوریتم‌ها توسط انسان‌ها طراحی می‌شوند، تعصبات، جانبداری‌ها و سوگیری‌های انسانی مانند مسایل مذهبی، جنسیتی و نژادی، قابلیت راه پیدا کردن در تصمیم‌های هوش مصنوعی را دارند و می‌توانند به تصمیم‌های ناعادلانه در استخدام، قضاوت یا اعطای خدمات منجر شوند.



۰۶

نابرابری اجتماعی اقتصادی

از بین رفتن مشاغل و تمرکز ثروت در دست شرکت‌های بزرگ فناوری، باعث می‌شود فاصله طبقاتی افزایش یابد و شکاف بین فقیر و غنی عمیق‌تر شود. این موضوع در هوش مصنوعی می‌تواند منجر به گسترش نابرابری‌ها و بی‌عدالتی‌های اجتماعی اقتصادی شود.

۰۷

دستکاری شبکه‌های اجتماعی

هوش مصنوعی می‌تواند محتواهای به نمایش درآمده در شبکه‌های اجتماعی را به طور کامل براساس علایق و تعاملات افراد، سفارشی‌سازی کند. این موضوع علاوه بر ایجاد فیلتر حبابی (Filter Bubble) می‌تواند زمینه دستکاری افکار عمومی و انتشار اطلاعات نادرست را فراهم کند و در نتیجه برخی اطلاعات از دید کاربر پنهان بماند.



اگر می خواهید اتاق سرور بسازید؛ این ۹ نکته حیاتی را رعایت کنید!

در عوض، به دنبال ساختن یک کسب و کار واقعی و پایدار باشید؛
همان طور که در مقاله زیر توضیح داده شده است

منبع: webitservices.com



✍ مترجم: مینا حیدری

اشاره

شاید کسب و کارتان را با یک رک و سرور آغاز کرده باشید و در کنار آن ها، یک دستگاه یوپی اس برای افزودن برق نصب کرده باشید؛ اما به مرور زمان تعداد زیرساخت های آی تی شما به چند رک با چندین سرور در هر کدام می رسد و ناچار روزی باید تصمیم بگیرید یک اتاق سرور کامل و استاندارد در دل شرکتتان بسازید.

اما این اتاق سرور باید چه مساحتی داشته باشد و سرورها چگونه در آن نگهداری شوند؟ آیا به برق و سیستم سرمایش جداگانه نیاز دارید؟ مشخصات فیزیکی اتاق میزبان باید شامل چه استانداردهایی باشد؟

برخی باورهای نادرست درباره اتاق های سرور وجود دارد. برای مثال، این که رک ها و سرورها باید در دورترین و کوچک ترین اتاق ساختمان قرار داده شوند یا حتما باید اتاق سرور در مرکز اتاق های دیگر ساخته شود.

ما با سابقه ای ۲۵ ساله در مشاوره، طراحی و ساخت اتاق سرور برای کسب و کارهای کوچک و متوسط، به ۹ سوال یا نکته مهم رسیدیم که اغلب، مدیران فناوری اطلاعات سازمان ها در ابتدای شروع ساخت یک اتاق سرور از ما پرسیده و به دنبال پاسخی روشن و صریح برای آن هستند. دانستن این ۹ نکته حیاتی به شما کمک می کند تا براساس نیازهای خود، ویژگی های بهترین اتاق سرور را مشخص کرده و ارزیابی دقیقی از فضا، نکات امنیتی، تعداد رک ها و سرورهای لازم برای نگهداری از داده ها داشته باشید.

با خرید یک رک و قرار دادن آن در فضایی امن و مطمئن، به هیچ گونه سیستم سرمایشی و شبکه توزیع برقی نیاز پیدا نکنند.

اما یک سازمان با چندین سرور، به فضای بیشتری برای استقرار آن ها و همچنین خنک سازی محیط نیاز پیدا می کند؛ زیرا بدیهی است که چندین سرور در کنار یکدیگر، گرمای بیشتری تولید خواهند کرد.

۹ پرسشی که باید پیش از ساخت یک اتاق سرور از خودتان بپرسید!

۱ چند سرور دارید؟

هرچه سرور و تجهیزات ذخیره سازی بیشتری داشته باشید؛ گرمای بیشتری تولید می کنند. برای مثال، یک سازمان کوچک با یک سرور، شاید به اتاق سرور نیاز نداشته باشد و صرفا

مقاله فنی

اتاق سرور باید با فضای کافی، تهویه و برق استاندارد و در مکانی ایمن و مرکزی طراحی شود. طراحی آن باید بر اساس رشد آینده و نه نیاز امروز سازمان باشد.



بتوانند به تمام بخش‌های تجهیزات دسترسی آزاد داشته باشند تا بتوانند همه اتصالات و سخت‌افزارها را بررسی کنند.

اگر فضای اتاق سرور تنگ باشد و تکنسین نتواند وارد اتاق سرور شود یا نتواند به پشت رک‌ها برود تا اتصالات برق، کابل‌ها یا پنل‌های توزیع برق را بررسی کند؛ فرایند پشتیبانی به کندی پیش می‌رود. در چنین شرایطی، ممکن است لازم شود سرورها از رک بیرون کشیده و دوباره نصب شوند که این کار علاوه بر اتلاف زمان، خطر قطعی برق و شبکه را افزایش می‌دهد.

بنابراین طراحی اتاق سرور باید به‌گونه‌ای باشد که مسیرهای دسترسی در جلو و پشت رک‌ها، هم برای کار روزمره و هم برای عملیات اضطراری، کاملاً باز و ایمن باشند.

۴ آیا اتاق سرور شما امن است؟

منظور از امنیت اتاق سرور، قفل‌دار بودن درب و استفاده از سنسورهای بیومتریک برای ورود افراد دارای دسترسی است. بسیار مهم است که تنها افراد دارای مجوز و مرتبط، امکان رفت و آمد به اتاق سرور را داشته باشند تا از سرقت و خرابی تجهیزات جلوگیری شود.

همچنین، سرورها نباید مزاحم دیگران باشند؛ برای مثال، نباید از اتاق فرد دیگری به اتاق

افزون بر این، فارغ از شرایط آب و هوای بیرون از اتاق سرور؛ داخل اتاق سرور باید در تمام طول سال خنک و در یک دمای ثابت نگه داشته شود.

برای مثال، در زمستان ممکن است کل ساختمان گرم باشد، اما دمای اتاق سرور باید همچنان پایین باشد. در تابستان نیز سیستم سرمایش باید بتواند بر گرمای تولیدی سرور و گرمای احتمالی محیط، غلبه کند.

در این زمینه نیز تعداد رک‌ها و سرورها، نقش تعیین‌کننده‌ای دارد. یک رک سرور با چگالی استاندارد، به جریان هوای مطبوع و خنک نیاز دارد، اما ممکن است نیازی به سیستم سرمایشی کاملاً مجزا و اختصاصی نداشته باشد.

۳ آیا فضای کافی برای کار و حرکت افراد در جلو و پشت سرورها وجود دارد؟

در زمان تعمیر یا نگهداری، تکنسین‌ها باید

ساختاردهی و نحوه اتصال سرورها، و میزان قدرت محاسباتی آن‌ها نیز در میزان تولید گرما موثر است.

برای نمونه، هنگامی که شما یک رک سرور دارید که نزدیک به ۴۰ سرور را در خود جای می‌دهد؛ گرمای زیادی در یک فضای متمرکز و عمودی ایجاد می‌شود، اما تقسیم این سرورها میان ۲ تا ۳ رک مجزا، می‌تواند به کاهش گرما کمک کند؛ هر چند این کار به فضای بیشتر و کابل‌کشی افزوده نیاز خواهد داشت.

۲ آیا فضای مورد نظرتان، جریان هوای کنترل شده دارد؟

شکی نیست که اتاق سرور به یک جریان هوای خنک و پایدار نیاز دارد. گاهی اوقات، صرفاً نصب یک کولر یا تعبیه یک دریچه متصل به سیستم تهویه مرکزی ساختمان، پاسخگوی نیازهای سرمایشی شما نیست و لازم است به سراغ یک سیستم جریان هوای خنک قابل اعتماد و پایدار بروید.

سرور، گذرگاه یا درب و پنجره‌ای وجود داشته باشد.

گاهی دیده می‌شود که اتاق سرور با یک پارتیشن از اتاق مدیر IT سازمان جدا شده است. در این شرایط، زمانی که تکنسین مرکز داده یا شبکه، مشغول کار روی سرورها است؛ مزاحم مدیر و سایر افرادی می‌شود که در آن اتاق حضور دارند و این شکل از طراحی اتاق سرور اصلاً توصیه نمی‌شود.

۵ آیا لوله‌های آب از سقف عبور می‌کنند؟

یک نکته کلیدی که باید بدانید؛ این است که اتاق سرورها نباید هیچ‌گونه لوله‌کشی آب در سقف یا هر فضای بالای رک‌ها و سرورها، داشته باشد. حتی بهترین لوله‌ها و سیستم‌های لوله‌کشی نیز ممکن است دچار نشتی شوند و آب، بزرگ‌ترین دشمن سرورهاست.

برای جلوگیری از خطر نشتی آب روی تجهیزات برقی و شبکه، بهتر است اتاق سرور هیچ لوله‌کشی آب داخلی یا بیرونی نداشته باشد.

۶ چه جنبه‌های دیگری برای اتاق سرور مهم است؟

معماری و ساختار برق‌کشی فضای مورد نظر، به شدت روی طراحی کلی اتاق سرور تاثیرگذار است. برای مثال، محل قرارگیری پرینرها نسبت به کانکتورهای شبکه کجاست؟ آیا نزدیک به هم هستند یا دور از هم قرار دارند؟ آیا به کابل‌کشی برق زیادی در یک فضای کوچک نیاز است؟

کف اتاق سرور در چه وضعیتی است؟ آیا تحمل بار و فشار رک‌ها را دارد و قابلیت نشست ندارد؟ آیا به اندازه کافی محکم و پایدار است؟ آیا می‌توان کابل‌های شبکه و برق را از کف عبور داد؟

چه نوع رکی استفاده می‌کنید؟ رک‌های ایستاده یا رک‌های دیواری؟ وزن سخت‌افزارهای شما چقدر است و آیا خطر افتادن رک‌ها وجود دارد؟ اگر چنین است؛ باید مطمئن شوید که به مرور زمان، گچ دیوار بر اثر فشار وارد شده، کنده نمی‌شود و به اندازه کافی مقاوم است.

بهترین روش، استفاده از کف کاذب یا نصب تخته‌های پشتیبان روی دیوار است تا از ریزش

تنها، سخت‌افزارهای ضروری و در حال استفاده باید در اتاق سرور نگهداری شوند و حتی بهتر است هارددیسک‌های نو و پشتیبان، یوپی‌اس‌ها و باتری‌های پشتیبان آفلاین و ... در مکان امن دیگری باشند.

ما روی برجسب‌گذاری همه کابل‌ها، کانکتورها و سخت‌افزارها تاکید زیادی داریم؛ چون در غیر این صورت، فرایند شناسایی مشکل، تعمیر خرابی و عیب‌یابی بسیار طولانی می‌شود و درصد خطای انسانی را چندین برابر افزایش می‌دهد.

۸ آیا مسیر کابل‌ها به اندازه کافی بزرگ و ضد حریق است؟

مسیرهای کابل‌ها به شما اجازه می‌دهند که در محل‌های لازم؛ کابل‌ها به یکدیگر متصل شوند. کابل‌های شبکه بسیار ضخیم‌تر از اکثر کابل‌های برق هستند و به مسیرهای بزرگ‌تری نسبت به کابل‌های الکتریکی مشابه خود نیاز دارند.

مسیرهای کابل شبکه باید ضد حریق باشند. آتش‌بندها، سازه‌هایی هستند که به ساختار مسیر کابل اضافه می‌شوند تا منافذ را آب‌بندی کرده و از گسترش آتش جلوگیری کنند. به این ترتیب، اگر آتش در اتاق سرور شروع شود؛ از طریق مسیر کابل‌ها به دیوارها، کف یا سقف‌ها سرایت نخواهد کرد.

۹ کدام ضوابط ساختمانی باید در اتاق سرور رعایت شود؟

اتاق‌های سرور اغلب فضای مشترکی با تابلوهای برق دارند که باید ضوابط ساختمانی سختگیرانه‌ای برای ایمنی آن‌ها رعایت شود. این ضوابط معمولاً مقرر می‌کنند که تابلوهای برق باید فضای خالی مشخص و مناسبی داشته باشند.

صنایع مختلف، ضوابط ایمنی خاص خود را دارند؛ به عنوان مثال، ضوابط ایمنی یک مدرسه با بانک یا بیمارستان متفاوت است. در هنگام انتخاب اتاق سرور و راه‌اندازی آن، ضوابط ایمنی ساختمان را بررسی کنید. عوامل خاصی مانند ضوابط و تابلوهای برق را در نظر داشته باشید.

جلوگیری شود. گاهی، رک‌ها روی یک پایه‌ای محکم قرار دارند و قابل جابه‌جا شدن هستند و قفل‌هایی برای جلوگیری از تحرک آن‌ها تعبیه شده است.

۷ کابل‌کشی‌ها مرتب و منظم هستند و همه چیز برجسب‌گذاری شده است؟

همه کابل‌ها، اعم از کابل‌های شبکه، برق و سخت‌افزارها، باید در نهایت نظم و مرتب‌سازی، سازمان‌دهی شده و با بست‌هایی، از هم جدا و برجسب‌گذاری شده باشند. اصلاً مناسب نیست که کابل‌های برق و شبکه روی زمین یا بین رک‌ها و سرورها رها شده باشند و فقط اپراتور IT سازمان بدانند کدام کابل به کدام سرور متصل است.

اتاق سرورها، محل نگهداری و ذخیره‌سازی هیچ چیز دیگری نیستند؛ نه تجهیزات شبکه و نه تجهیزات نامرتب مانند دسته‌ای از کاغذها. گرما می‌تواند باعث آتش‌سوزی کاغذها یا مستندات شود؛ بنابراین بهتر است این دارایی‌ها را به بیرون از اتاق سرور منتقل کنید.



TAC-1631DP

In-Row

Cooling System



Pressure control system



Energy saving



Temperature sensor



EBM Variable speed fan



300x1970x1070 Set Dimensions (mm)



Modbus RTU



Top or bottom feeding



**دما رو
قفلش کن!!**

نسل جدید سیستم
سرمايش هوشمند
اتاق سرور

مشخصات فنی

- مجهز به سیستم Inverter برای کنترل دور فن کندانسور
- مجهز به فن دور متغیر شرکت EBM
- قابلیت مانیتورینگ تمامی پارامترهای اساسی سیستم سرمایشی
- قابلیت مانیتورینگ وضعیت خطا در عملکرد سیستم

- ظرفیت نامی ۲۰ کیلووات
- سیستم کنترلی PLC
- سیستم کنترل فشار
- شیر اکسپنشن الکتریکی
- پشتیبانی از پروتکل Modbus RTU



تلفن گویا: ۹۱۰۷۲۳۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
اپراتور: ۰۶۶۹۴۷۲۰۰
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

چگونه مدیران با هوش مصنوعی تصمیم‌های بهتری می‌گیرند؟

۸ ترفند برای بهبود تصمیم‌گیری در کسب و کار با کمک AI

منبع: [linkedin.com/pulse/](https://www.linkedin.com/pulse/)



مترجم: محمود شاملیام

اشاره

مقاله مدیریتی

در محیط پر شتاب کسب و کار امروز، تصمیم‌گیری یکی از حیاتی‌ترین وظایف مدیران و رهبران سازمان‌هاست. با توجه به حجم عظیم داده‌هایی که هر ثانیه تولید می‌شوند؛ توانایی تصمیم‌گیری آگاهانه و به موقع می‌تواند تاثیر چشمگیری بر موفقیت یک کسب و کار داشته باشد. اما ذهن انسان، تنها قادر است مقدار محدودی از اطلاعات را به طور همزمان پردازش کند. اینجا است که هوش مصنوعی وارد عمل می‌شود و می‌تواند رویکرد رهبران تجاری را در فرآیند تصمیم‌گیری متحول کند. AI ابزارهایی ارائه می‌کند که در تجزیه و تحلیل داده‌ها، پیش‌بینی روندها، و کشف بینش‌ها کمک می‌کند و اجازه نمی‌دهد تصمیم‌گیری‌ها صرفاً بر اساس دانش و اطلاعات محدود ذهن انسان انجام شود.

در ادامه، به ۸ روش به کارگیری هوش مصنوعی برای بهبود تصمیم‌گیری رهبران کسب و کارها اشاره می‌کنیم:

۱- بینش‌های داده‌محور: درک کلان داده‌ها

در عصر دیجیتال، شرکت‌ها هر روز حجم عظیمی از داده‌ها را تولید می‌کنند. از تعاملات مشتری گرفته تا عملکردهای عملیاتی. این داده‌ها ارزش بسیار بالایی دارند، اما، تجزیه و تحلیل دستی چنین مجموعه‌ای از داده‌های بزرگ، غیرعملی، زمان‌بر و اغلب منجر به خطای انسانی می‌شود.

ابزارهای تحلیلی مبتنی بر هوش مصنوعی، می‌توانند در کسری از زمانی که یک انسان صرف می‌کند، حجم عظیمی از داده‌ها را پردازش کرده و بینش‌های کاربردی ارائه دهند که تصمیم‌گیری را هدایت می‌کند. هوش

مصنوعی می‌تواند روندها را برجسته سازد؛ همبستگی‌ها را شناسایی کند و حتی بر اساس داده‌های تاریخی، نتایج آینده را پیش‌بینی کند. این رویکرد داده‌محور، به مدیران کسب و کار کمک می‌کند تصمیماتی آگاهانه‌تر و عینی‌تر بگیرند و وابستگی به شهود صرف را کاهش دهند.

۲- تحلیل‌های پیش‌گویانه:

پیش‌بینی آینده

یکی از قدرتمندترین کاربردهای هوش مصنوعی در تصمیم‌گیری، تحلیل‌های پیش‌بینی‌کننده است. با بهره‌گیری از داده‌های تاریخی و الگوریتم‌های یادگیری ماشین، مدل‌های

هوش مصنوعی با تحلیل داده‌ها و پیش‌بینی روندها، تصمیم‌گیری رهبران کسب و کار را سریع‌تر، دقیق‌تر و آگاهانه‌تر می‌کند. ■



How AI Can Improve Decision-Making for Business Leaders

هوش مصنوعی می‌تواند روندها و رفتارهای آینده را پیش‌بینی کنند. برای مثال، هوش مصنوعی می‌تواند الگوهای خرید مشتریان، تغییرات بازار یا اختلالات زنجیره تأمین را پیش‌بینی کند و به رهبران این امکان را بدهد که استراتژی‌های خود را به صورت پیشگیرانه تنظیم کنند.

مصنوعی برای تصمیم‌گیری‌هایی استفاده کنند که بیشتر مبتنی بر واقعیت‌ها و داده‌ها هستند و رویکردی سازگارتر و منصفانه‌تر را در مدیریت تضمین می‌کنند.

گزارش‌ها، تصمیمات کارآمدتری بگیرند. هرچه مدیران زودتر به اطلاعات مرتبط دسترسی داشته باشند؛ سریع‌تر می‌توانند به چالش‌ها و فرصت‌ها پاسخ دهند و کسب‌وکار را چابک و رقابتی نگه دارند.

این توانایی پیش‌بینی به مدیران کسب‌وکار کمک می‌کند تا یک گام از بازار جلوتر باشند. به جای واکنش در زمان بروز مشکلات، هوش مصنوعی به مدیران کمک می‌کند تا تصمیمات پیشگیرانه بگیرند؛ تصمیماتی که می‌تواند هم از بروز خطرات جلوگیری کند و هم فرصت‌ها را پیش از رقبا در اختیارشان قرار دهد.

۵- پشتیبانی از تصمیم‌گیری‌های شخصی‌سازی شده

هوش مصنوعی این توانایی را دارد که تصمیمات مدیران را بر اساس زمینه‌ها، شرایط و داده‌های منحصر به فرد هر کسب‌وکار تنظیم کند و توصیه‌هایی شخصی‌سازی شده ارائه دهد. برای مثال، در حوزه‌ی بازاریابی، هوش مصنوعی می‌تواند با تجزیه و تحلیل داده‌های رفتاری مشتریان، بهترین کانال‌های تعامل و موثرترین شیوه‌های جذب را مشخص کند و به مدیران در تصمیم‌گیری در مورد اولویت‌بندی استراتژی‌ها کمک کند.

به طور مشابه، در امور مالی، الگوریتم‌های هوش مصنوعی می‌توانند بر اساس شرایط بازار، سطح ریسک‌پذیری و اهداف شرکت، گزینه‌های سرمایه‌گذاری بهینه را پیشنهاد دهند. این قابلیت شخصی‌سازی به مدیران کمک می‌کند تا تصمیماتی بگیرند که نه تنها

۴- به حداقل رساندن سوگیری در تصمیم‌ها

تصمیم‌گیری انسان اغلب تحت تأثیر سوگیری‌های شناختی، مانند تمایل به تأیید، در دسترس بودن یا لنگر انداختن قرار می‌گیرد. این سوگیری‌ها می‌توانند به قضاوت‌های نادرست و تصمیم‌هایی منجر شوند که کاملاً عینی نیستند. از سوی دیگر، هوش مصنوعی بر اساس الگوریتم‌ها و داده‌ها عمل می‌کند و تا حد زیادی تأثیرات ذهنی را از فرآیند تصمیم‌گیری حذف می‌کند. البته سیستم‌های هوش مصنوعی کاملاً در برابر سوگیری‌ها مصون نیستند، زیرا ممکن است این سوگیری‌ها را از داده‌هایی که با آن‌ها آموزش دیده‌اند به ارث ببرند؛ با این حال، معمولاً در پردازش داده‌ها به شیوه‌ای بی‌طرفانه و عینی بهتر عمل می‌کنند. مدیران کسب‌وکار می‌توانند از هوش

۳- افزایش سرعت تصمیم‌گیری

مدیران کسب‌وکار اغلب با چالش تصمیم‌گیری سریع در محیط‌های پرشتاب و پویا مواجه هستند. هوش مصنوعی می‌تواند با خودکارسازی وظایف تکراری روزانه و همچنین ارائه بینش‌های فوری و بلادرنگ، این فرآیند را ساده‌تر کند. برای مثال، داشبوردهای مبتنی بر هوش مصنوعی می‌توانند در لحظه، دید جامعی از معیارهای کلیدی مانند فروش، سطح موجودی یا رضایت مشتری، به تصمیم‌گیرندگان ارائه دهند. این دسترسی سریع به داده‌های حیاتی، باعث می‌شود مدیران به جای انتظار برای جمع‌آوری دستی

HOW AI CAN HELP
BUSINESS LEADERS MAKE
BETTER DECISIONS

AI AND BETTER BUSINESS DECISIONS

هوش مصنوعی با بهبود دقت،
سرعت و چابکی تصمیم‌گیری،
به شریک استراتژیک و مزیت
رقابتی پایدار کسب‌وکارها تبدیل
می‌شود.

ارزشمندی را برای مدیران کسب‌وکار آزاد می‌کند
تا بتوانند تمرکز خود را بر تصمیم‌گیری‌های
سطح بالاتر و توسعه استراتژی‌های کلان
بگذارند.

نتیجه‌گیری:

هوش مصنوعی شریک استراتژیک مدیران کسب‌وکارها

هوش مصنوعی دیگر یک مفهوم دور از دسترس
نیست؛ بلکه یک ابزار واقعی و کاربردی امروز
است که می‌تواند فرآیند تصمیم‌گیری مدیران
را به طور بنیادین تغییر دهد. با بهره‌گیری از
هوش مصنوعی در تجزیه و تحلیل داده‌ها،
پیش‌بینی روندها و بهینه‌سازی استراتژی‌ها،
مدیران می‌توانند تصمیماتی آگاهانه‌تر،
کارآمدتر و عینی‌تری بگیرند. با تکامل هوش
مصنوعی، نقش آن در تصمیم‌گیری افزایش
می‌یابد و به مدیران تیم‌ها و شرکت‌ها کمک
می‌کند تا در محیط پیچیده و پرچالش
کسب‌وکار با اطمینان حرکت کنند.

استفاده از هوش مصنوعی، تنها به معنای
همگام شدن با فناوری نیست؛ بلکه به معنای
دستیابی به یک مزیت رقابتی واقعی است.
مدیرانی که از هوش مصنوعی برای تقویت و
بهبود تصمیم‌گیری‌های خود بهره می‌برند،
می‌توانند سازمان‌های خود را به سمت
موفقیت و نوآوری بیشتر سوق دهند، در حالی
که تصمیمات‌شان هوشمندانه و مبتنی بر داده
خواهد بود.

کرده و به مرور زمان دقت و کارایی بالاتری
پیدا کنند. این بدان معنا است که هوش
مصنوعی می‌تواند همگام با رشد و تغییرات
کسب‌وکار تکامل یابد و به مدیران کمک کند تا
تصمیمات خود را بر پایه‌ی تازه‌ترین اطلاعات
تنظیم کنند. این ویژگی به ویژه در صنایعی که
با تحولات سریع یا شرایط غیرقابل پیش‌بینی
روبرو هستند؛ اهمیت زیادی دارد. در نتیجه
مدیران کسب‌وکار می‌توانند به هوش مصنوعی
نه تنها برای تصمیمات روزمره، بلکه برای
برنامه‌ریزی‌های بلندمدت نیز تکیه کنند؛
زیرا می‌دانند که این فناوری در مسیر تکامل،
همگام با سازمان پیش خواهد رفت.

۸- همکاری و کار تیمی مبتنی بر هوش مصنوعی

ابزارهای هوش مصنوعی می‌توانند همکاری
میان مدیران کسب‌وکار و تیم‌هایشان را به
شکل چشمگیری تقویت کنند. برای مثال،
پلتفرم‌های مبتنی بر هوش مصنوعی با
ارائه به روزرسانی‌ها، هشدارها و توصیه‌های
بلادرنگ، ارتباطات درون سازمانی را روان‌تر
می‌سازند. مدیران شرکت‌های تجاری
می‌توانند با به اشتراک گذاشتن بینش‌های
مبتنی بر داده (داده‌محور)، از هوش مصنوعی
برای مشارکت فعال‌تر تیم‌ها در فرآیندهای
تصمیم‌گیری استفاده کنند؛ این موضوع به
هماهنگی بهتر اهداف و افزایش اثربخشی
همکاری‌ها منجر می‌شود.

همچنین، هوش مصنوعی می‌تواند وظایف
اداری مانند برنامه‌ریزی جلسات، پیگیری
پیشرفت ابتکارات و تولید گزارش‌ها را
خودکارسازی کند. این خودکارسازی زمان

دقیق‌تر و عملی‌تر باشند، بلکه هماهنگی
بیشتری با اهداف خاص سازمان داشته و
تأثیرگذاری بالاتری نیز ایجاد کنند.

۶- مدیریت ریسک:

شناسایی و کاهش خطرات

هر تصمیمی همواره با سطحی از خطر (ریسک)
همراه است و هوش مصنوعی می‌تواند مدیریت
ریسک را به طور قابل توجهی ارتقا دهد. با
استفاده از مدل‌های پیش‌بینی و تحلیل
سناریو، هوش مصنوعی می‌تواند ریسک‌های
بالقوه‌ی ناشی از تصمیمات مختلف را شناسایی
و راهکارهایی برای کاهش آن‌ها پیشنهاد دهد.
برای مثال، هوش مصنوعی می‌تواند احتمال
موفقیت یا شکست در ورود به یک بازار جدید،
عرضه‌ی یک محصول جدید، یا سرمایه‌گذاری
روی فناوری‌های نوین را ارزیابی کند. همچنین
از طریق شبیه‌سازی سناریوهای مختلف،
هوش مصنوعی به مدیران کمک می‌کند تا
تهدیدها و چالش‌های احتمالی را پیش‌بینی
کرده و از اشتباهات پرهزینه جلوگیری کنند. در
نتیجه، مدیران قادر خواهند بود تا تصمیماتی
بگیرند که حساب‌شده است، از میزان خطرات
آن آگاه هستند، احتمال موفقیت را افزایش
داده و پیامدهای منفی را تا حد امکان کاهش
دهند.

۷- یادگیری و سازگاری مداوم

یکی از بزرگترین مزایای هوش مصنوعی، توانایی
آن در یادگیری و سازگاری مستمر است. هر چه
سیستم‌ها با داده‌های جدید بیشتری روبه‌رو
شوند، می‌توانند الگوریتم‌های خود را اصلاح

انگیزه تلاش برای بهترین ماندن، قریب به سه دهه همراهی شماست...

مشاوره، طراحی،
پیاده سازی، نظارت،
پشتیبانی و پیش
میزی مرکز داده



- سیستم‌های مدیریت زیر ساخت مرکز داده (DCIM)
- سیستم‌های سرمایشی مرکز داده (Cooling)
- مرکز داده ثابت و سیار (Datacenter)
- رک و تجهیزات جانبی (Rack)
- کابل و اتصالات (UNICOM)
- پنل‌های تغذیه برق (PDU)



تلفن گویا: ۹۱۰۷۲۳۲۳	تهران، خیابان فاطمی غربی، پلاک ۲۴۸
تلفن گویا: ۶۶۹۴۲۳۲۳	اپراتور: ۶۶۹۴۷۲۰۰
دورنگار: ۶۶۹۴۲۳۲۴	www.tiamnetworks.ir
info@tiamnetworks.ir	tiamnetworks
	company/tiamnetworks

فرمول موفقیت: نوآوری فناورانه، استراتژی جهانی و مدیریت چابک

نگاهی کوتاه به تاریخچه شرکت بایت دنس و دلایل موفقیت تیک تاک

منبع: howtheygrow.co



مترجم: مائده مافی

اشاره

شرکت بایت دنس، غول فناوری چینی و مالک پلتفرم جهانی تیک تاک، یکی از نمونه‌های برجسته موفقیت استارت‌آپ‌های دیجیتال در دهه اخیر به شمار می‌رود. این شرکت با بهره‌گیری از الگوریتم‌های پیشرفته و نوآوری در تولید محتوا، توانسته در کمتر از یک دهه از یک استارت‌آپ محلی به یک قدرت جهانی در حوزه رسانه اجتماعی تبدیل شود. داستان بایت دنس، داستانی شرکتی است که برای تبدیل شدن به یک «یونیکورن» و سپس دستیابی به جایگاه بزرگ‌ترین استارت‌آپ جهان، زمان را هدر نداد. این شرکت ظرف کمتر از یک دهه، موفقیت‌هایی در صنعت فناوری اطلاعات به دست آورد که برای بسیاری از شرکت‌های معروف و قدیمی امریکایی، نیازمند چند دهه تلاش بود. در سال‌های اخیر، ارزش شرکت بایت دنس (ByteDance) به بیش از ۲۰۰ تا ۳۰۰ میلیارد دلار رسیده و تیک تاک ماهانه بیش از یک میلیارد کاربر فعال دارد. بایت دنس همزمان با رشد سریع، در آخرین سرمایه‌گذاری خود، مبلغ ۸.۸ میلیارد دلار را صرف ساخت دیتاسنترهایی کرده تا بتواند قدرت هوش مصنوعی و زیرساخت‌های فنی خود را تقویت و بازسازی کند. با این حال، این مسیر خالی از چالش نبوده و شرکت با مسائلی همچون تحریم‌های آمریکا و نگرانی‌ها درباره نقض حریم خصوصی مواجه است. در این مقاله، تاریخچه، عوامل موفقیت، و وضعیت کنونی ByteDance بررسی می‌شود.

داستان موفقیت



بایت دنس در کمتر از یک دهه به غولی ۳۰۰ میلیارد دلاری تبدیل شد و با سرمایه‌گذاری بزرگ در دیتاسنتر، قدرت هوش مصنوعی خود را افزایش داد، اما با تحریم‌ها و نگرانی‌های حریم خصوصی دست‌وپنجه نرم می‌کند.

تاریخچه تأسیس و مراحل رشد

بایت دنس

۲۰۱۲: آغاز کار

بایت دنس در مارس ۲۰۱۲ توسط «ژانگ ییمینگ» و «لیانگ روبرو» در پکن تأسیس شد. نخستین محصول این شرکت، Neihan Duanzi، یک اپلیکیشن طنز و جوک بود که بعدها توسط دولت چین مسدود شد. نقطه عطف موفقیت بایت دنس با معرفی Toutiao (به معنی «تیترها») آغاز شد، اپلیکیشن خبرخوان هوشمندی که محتوای پیشنهادی را بر اساس

علاقه کاربر ارائه می‌داد.

در سال‌های ۲۰۱۱-۲۰۱۲، ژانگ ییمینگ متوجه شد که بخش بزرگی از مردم چین هنوز اخبار و محتوای آنلاین را از طریق وبسایت‌ها یا نسخه‌های دسکتاپ می‌خوانند، در حالی که گوشی‌های هوشمند به سرعت چشمگیری در حال فراگیر شدن بودند.

او مشاهده کرد که اپلیکیشن‌های خبری موجود، تجربه کاربری ضعیفی دارند و تقریباً برای همه کاربران محتوای مشابهی نمایش می‌دهند. ایده او این بود که یک سیستم

ByteDance | TikTok: Origins, How They Grow, and The Future of The Internet



کاربران را در معرض دید میلیون‌ها نفر قرار می‌داد. این مدل باعث شد حتی کاربران تازه‌کار نیز انگیزه پیدا کنند و محتوای بیشتری تولید کنند؛ چرا که خیلی سریع بازخورد می‌گرفتند. ویدئوهای کوتاه ۱۵ تا ۶۰ ثانیه‌ای، امکانات ویرایش درون برنامه‌ای، افکت‌ها و موسیقی‌های آماده، موانع تولید محتوا را به حداقل رسانده بود. این ویژگی برای نسل Z که حوصله محتوای طولانی نداشتند، ایده‌آل بود.

بایت‌دنس با استفاده از هشتگ‌ها، چالش‌های ویروسی و موسیقی‌های محبوب، انگیزه مشارکت کاربران را افزایش داد. بسیاری از آهنگ‌ها و میم‌ها^۱ صرفاً به خاطر تیک‌تاک در سطح جهان شناخته شدند.

در آن دوره، بایت‌دنس میلیون‌ها دلار برای تبلیغات در فیس‌بوک، اینستاگرام، اسنپ‌چت و حتی یوتیوب هزینه کرد. تیک‌تاک تقریباً همه‌جا دیده می‌شد و همین کنجکاوی کاربران را برای نصب آن برانگیخت.

شرایط بازارهای جهانی در سال ۲۰۱۸ نیز به نفع تیک‌تاک پیش می‌رفت. اینستاگرام و فیس‌بوک با بحران‌های حریم خصوصی و رسوایی Cambridge Analytica دست و پنجه نرم می‌کردند و محبوبیتشان در میان جوانان رو به کاهش بود. اسنپ‌چت نیز روند رشد خود را از دست داده بود. درست در همین

آن با نام TikTok در سال ۲۰۱۷ منتشر شد.

۲۰۱۷ تا ۲۰۱۸: خرید و ادغام Musical.ly

در نوامبر ۲۰۱۷، بایت‌دنس استارت‌آپ Musical.ly را با قیمت ۱ میلیارد دلار خریداری کرد و در سال ۲۰۱۸ آن را با تیک‌تاک ادغام نمود. این تصمیم موجب رشد انفجاری تعداد کاربران شد و تیک‌تاک را به یکی از پرنصب‌ترین اپلیکیشن‌های دنیا تبدیل کرد.

۲۰۱۸ تا امروز: تنوع و گسترش جهانی

علاوه بر تیک‌تاک و Douyin، بایت‌دنس محصولات دیگری مثل Xigua Video (پلتفرم ویدیویی)، ابزار همکاری Lark/Feishu، سرویس‌های واقعیت مجازی (Pico VR) و حتی بخش آموزش آنلاین را راه‌اندازی کرده است. حضور این شرکت اکنون در بازارهای آمریکا، اروپا، آسیای جنوب شرقی و خاورمیانه گسترده شده است.

دلایل موفقیت تیک‌تاک چه بود؟

یکی از مهم‌ترین عوامل موفقیت تیک‌تاک، انتقال پایگاه داده میلیونی و فعال کاربران Musical.ly به تیک‌تاک بود؛ بدون آن‌که نیاز باشد از صفر برای جذب کاربر تلاش کند. تیک‌تاک با الگوریتم توصیه‌گر بسیار پیشرفته خود، حتی بدون داشتن فالور، ویدئوهای

کاملاً الگوریتمی و خودیادگیرنده ایجاد کند که بدون نیاز به ویراستار انسانی، محتوایی دقیقاً متناسب با علایق هر فرد ارائه دهد.

ژانگ ییمینگ که خود مهندس نرم‌افزار بود، پیش‌تر در مایکروسافت و Fanfou (شبکه اجتماعی مشابه توییتر) فعالیت کرده بود. با مشاهده موفقیت موتورهای جست‌وجو و شبکه‌های اجتماعی خارجی، به این نتیجه رسید که آینده رسانه در چین باید بر پایه موبایل و الگوریتم بنا شود، نه صرفاً بر اساس انتخاب‌های یک تحریریه انسانی.

موسسان بایت‌دنس اعلام کرده‌اند که هدف اولیه‌شان «ایجاد یک پلتفرم توزیع محتوا مبتنی بر هوش مصنوعی، برای اتصال هر فرد به اطلاعاتی که بیشترین اهمیت را برای او دارد» بوده است. آن‌ها باور داشتند که با این رویکرد، کاربران می‌توانند بدون نیاز به جست‌وجوی دستی، در کوتاه‌ترین زمان ممکن به جالب‌ترین و مرتبط‌ترین محتوا دسترسی پیدا کنند.

به همین دلیل، نام ByteDance را برگزیدند؛ نامی که ترکیبی از فناوری (Byte) و خلاقیت و سرگرمی (Dance) است، و فلسفه کاری آن‌ها را به خوبی بازتاب می‌دهد.

۲۰۱۶: ورود به دنیای ویدئو

در سال ۲۰۱۶، بایت‌دنس اپلیکیشن Douyin را ویژه بازار چین عرضه کرد. این اپلیکیشن به سرعت محبوبیت یافت و نسخه بین‌المللی

۱ میم (Meme) به محتوای طنزآمیز یا خلاقانه‌ای گفته می‌شود که به سرعت در فضای آنلاین دست‌به‌دست می‌شود و معمولاً بر پایه‌ی یک عکس، ویدئو یا عبارت خاص ساخته می‌شود.

زمان، تیک تاک به عنوان یک پلتفرم تازه، سرگرم‌کننده و متفاوت وارد صحنه شد.

چرا بایت دنس به سرعت به ارزشمندترین استارت‌آپ دنیا تبدیل شد؟

تنها ۶ سال پس از تاسیس، بایت دنس در اکتبر ۲۰۱۸ به ارزشی معادل ۷۵ میلیارد دلار رسید و عنوان ارزشمندترین استارت‌آپ جهان را به دست آورد. سرمایه‌گذاری ۳ میلیارد دلاری سافت بانک (SoftBank) در بایت دنس، یکی از مهم‌ترین دلایل این موفقیت بزرگ بود، اما دلایل اصلی را باید در لایه‌های عمیق‌تری جست‌وجو کرد. هسته اصلی موفقیت بایت دنس، سیستم پیشرفته توصیه‌گر محتواست که با استفاده از یادگیری ماشین، محتوایی کاملاً شخصی‌سازی شده به کاربران ارائه می‌دهد. این ویژگی، کاربران را برای مدت طولانی در پلتفرم نگه می‌دارد و نرخ تعامل را به شدت افزایش می‌دهد. به بیان ساده، بایت دنس خیلی خوب می‌داند که چطور باید از الگوریتم‌های هوشمند و داده محور استفاده کند.

دلیل مهم دیگر، ساختار سازمانی مسطح و فرهنگ OKR است که تصمیم‌گیری سریع و نوآوری را ممکن می‌سازد. همچنین بایت دنس با ایجاد «پلتفرم خدمات مشترک» (SSP) توانسته از مازول‌های نرم‌افزاری خود در محصولات مختلف به‌طور مجدد استفاده کند و توسعه را سرعت بخشد.

از همان ابتدا، بنیان‌گذاران بایت دنس استراتژی‌های مشخص، شفاف و پایداری اتخاذ کردند. «ژانگ ییمینگ» معتقد بود که موفقیت در گرو جهانی‌سازی است و خرید استارت‌آپ Musical.ly نمونه‌ای روشن از این استراتژی بود که امکان ورود سریع به بازارهای آمریکا و اروپا را فراهم کرد.

در نهایت، مدل درآمدی بایت دنس تنوع بالایی دارد. این شرکت تنها به تبلیغات وابسته نیست و از خریدهای درون برنامه‌ای، تجارت الکترونیک، خدمات ابری (BytePlus) و همکاری‌های B2B نیز درآمدزایی می‌کند. همین تنوع منابع درآمد، پایداری و رشد سریع ارزش شرکت را تضمین کرده است.

حال و آینده بایت دنس و چالش‌های پیش رو

بایت دنس، غول فناوری چینی، امروز ارزشی بیش از ۲۵۰ میلیارد دلار دارد و تنها اپلیکیشن تیک تاک آن بیش از ۱ میلیارد کاربر فعال

ماهانه را به خود جذب کرده است. این شرکت با داشتن بیش از ۱۵۰ هزار کارمند در سراسر جهان، دفاتری در بیش از ۲۰ کشور و



در شهرهایی نظیر بیجینگ، شانگهای، توکیو، لندن، برلین، سان پائولو، دبی، ریاض و ... دارد. طبق گزارش موسسه Synergy Research Group، تا پایان نیمه نخست ۲۰۲۴، بایت دنس یکی از پیشتازان چینی در رشد سریع زیرساخت‌های مراکز داده بوده و از نظر نرخ رشد از بسیاری از رقبای بزرگ خود پیشی گرفته است. هم‌اکنون، این شرکت در حال ساخت یک مرکز داده عظیم با سرمایه‌گذاری ۶۱۴ میلیون دلار در استان شانشی چین است؛ پروژه‌ای که شامل چند ساختمان و بیش از ۱۲،۶۰۴ رک سرور خواهد بود. همچنین، برنامه‌ریزی‌هایی برای احداث دیتاسنتری در تایلند در دست بررسی دارد تا خدمات ابری و هوشمند محلی را تقویت کند.

با این حال، مسیر رشد و پیشرفت بایت دنس با چالش‌های گوناگونی مانند فشارهای قانونی و تهدید به ممنوعیت فعالیت در برخی کشورها مانند آمریکا و هند، نگرانی‌ها درباره امنیت داده و حریم خصوصی، و اتهامات مطرح شده در آمریکا، اتحادیه اروپا، هند، و استرالیا از جمله موانع جدی هستند. براساس قانون سال ۲۰۲۴ ایالات متحده، این شرکت باید مالکیت تیک تاک را به یک شرکت آمریکایی واگذار کند، در غیر این صورت این شبکه اجتماعی در آمریکا فیلتر خواهد شد.

از سوی دیگر، دولت چین نظارت سخت‌گیرانه‌ای بر محتوای آنلاین دارد و شرکت‌های فناوری را ملزم به رعایت مقررات سانسور و کنترل اطلاعات می‌کند. در نتیجه، بایت دنس ناچار شد نسخه بین‌المللی TikTok

را به‌طور کامل از نسخه داخلی (Douyin) جدا نگه دارد و پایگاه داده‌ها و زیرساخت‌های آن را تفکیک کند. همچنین، فشار دولت چین برای الگوبرداری از مفهوم «رشد سالم اینترنت» باعث شد برخی محصولات این شرکت، به ویژه برای کاربران نوجوانان، محدودیت زمانی استفاده، داشته باشند.

بایت دنس علاوه بر تیک تاک و Douyin، مجموعه‌ای از اپلیکیشن‌ها و خدمات دیگر را نیز ارائه می‌دهد، با این حال، رقابت شدید با شرکت‌های غولی مانند متا (اینستاگرام و ریلز)، گوگل و Snapchat باعث شده که این شرکت به سرمایه‌گذاری سنگین در زمینه نوآوری، توسعه محصول و بازاریابی ادامه دهد. با وجود این چالش‌های حقوقی، سیاسی و نظارتی، بایت دنس همچنان در حال سرمایه‌گذاری روی فناوری‌های نوین مانند هوش مصنوعی پیشرفته، واقعیت مجازی و افزوده و تجارت الکترونیک اجتماعی است. به نظر می‌رسد با تداوم رشد و نوآوری، این شرکت همچنان یکی از بازیگران اصلی صحنه فناوری باقی بماند.

جمع‌بندی

بایت دنس نمونه‌ای بی‌نظیر از ترکیب نوآوری فناورانه، استراتژی جهانی و مدیریت چابک است. این شرکت مسیر شگفت‌انگیزی را از یک اپلیکیشن طنز محلی به یک امپراتوری رسانه‌ای جهانی پیموده و همچنان در خط مقدم تحولات دیجیتال قرار دارد. اگرچه تیک تاک درآمد تبلیغاتی بسیار بالایی دارد، اما هزینه‌های مرتبط با زیرساخت‌ها، توسعه هوش مصنوعی و دیتاسنترها بسیار سنگین است.

علاوه بر این، ورود بایت دنس به حوزه‌های جدید مانند هوش مصنوعی مولد (Generative AI) و بازی‌های ویدیویی، نیازمند سرمایه‌گذاری‌های کلان است که فشار قابل توجهی بر جریان نقدی شرکت وارد می‌کند. با این حال، توانایی بایت دنس در نوآوری مستمر و نفوذ در بازارهای جهانی می‌تواند آن را همچنان به یکی از بازیکنان اصلی دنیای فناوری تبدیل کند.



بایت دنس با نوآوری در الگوریتم، ساختار سازمانی پویا و سرمایه‌گذاری گسترده در زیرساخت و هوش مصنوعی، علیرغم چالش‌های جهانی، به غولی ۲۵۰ میلیارد دلاری تبدیل شده و رهبری دیجیتال را در دستان دارد.



از هر جهت بزرگتر!!

نسل جدید رک های دیتاسنتر
بر اساس نیاز شما، با ابعادی
بزرگ تر و دسترسی بهتر

سوالاتی که باید پیش از ترک شغل، از خودتان بپرسید

ترک شغل همیشه شکست نیست، بلکه می‌تواند تصمیمی آگاهانه و جسورانه باشد اگر در زمان درست و با آمادگی کامل انجام شود.



منبع: forbes.com

مترجم: نجمه رحمت‌اللهی

مقاله مدیریتی

اشاره

تصمیم به ترک شغل، امری طبیعی است و شاید برای هر فردی، نه یک بار بلکه چندین بار در مسیر رشد شغلی رخ دهد. زمانی فرا می‌رسد که به اندازه کافی در یک شغل و شرکت مانده‌اید و اکنون می‌خواهید تسلیم شوید؛ حتی اگر دیگران به شما بگویند: «هرگز تسلیم نشو و تحت هر شرایطی ادامه بده!». ما به شما پیشنهاد می‌کنیم که «تسلیم شوید»، اما باید به خوبی بدانید چه زمانی این کار را انجام دهید.

ترک شغل ذاتاً بد نیست اما در محیط پیرامونی ما، غالباً نشانه‌ای از ضعف یا شکست تلقی می‌شود. تنها شما هستید که باید تشخیص دهید آیا این، جسورانه‌ترین تصمیمی است که گرفته‌اید یا واقعا شکست خورده‌اید. مرحله بعد، تشخیص زمان درست ترک محل کار است. باید پیش از آن کاملاً درباره این تصمیم خوب فکر کرده و آماده شده باشید. گاهی به نظر می‌رسد تصمیم نهایی خود را گرفته و آماده ترک شغل‌تان هستید، اما با پاسخ دادن به چند پرسش، دوباره میان «رفتن» یا «ماندن» مردد می‌شوید و در یک دوراهی باقی می‌مانید.

خستگی و مسایل عاطفی، با ترک به دلیل نادیده گرفته شدن یا هدر رفتن استعدادها، تفاوت قائل شوید. مورد اول، معمولاً با کمی استراحت، تغییر رویکرد یا درخواست کمک از دیگران، برطرف می‌شود، اما مورد دوم به تصمیمی دشوارتر نیاز دارد.

به طور خلاصه، زمانی که احساس می‌کنید در آستانه ترک شغل هستید؛ لحظه‌ای مکث کرده، شرایط را ارزیابی و حتی روی کاغذ ثبت کنید. همه چیز را یادداشت کنید؛ اینکه چه احساسی دارید، چرا به فکر ترک شرکت

۱ از خودتان بپرسید: واقعا چرا می‌خواهید کارتان را ترک کنید؟

این نخستین و مهم‌ترین پرسشی است که باید صادقانه به خودتان پاسخ دهید. آیا خسته شده‌اید؟ ناامید شده‌اید؟ مسیر پیشرفت شغلی شما مسدود شده یا احساس می‌کنید قدر توانایی‌های شما را نمی‌دانند؟ آیا مهارت‌ها یا برنامه توسعه فردی‌تان که در ذهن دارید، با مسیری که در حال پیمودن آن هستید، همسو نیست؟

باید بیاموزید بین ترک شغل به دلیل

ترک شغل شکست نیست، بلکه اگر آگاهانه و با برنامه‌ریزی انجام شود، می‌تواند آغاز مسیری بهتر باشد. پیش از تصمیم، دلایل واقعی، همه راه‌های موجود، زمان‌بندی، پیامدها و نظر افراد قابل اعتماد را بررسی کنید تا انتخابی هوشمندانه و رو به جلو داشته باشید.



Questions To Consider Before You Quit

گاهی اوقات، ضررها و پیامدهای منفی، بیش از سودها و مزایا هستند و این موضوع نشانه‌ای است که باید کمی بیشتر در تصمیم‌تان تأمل کنید. اما گاهی سودها آن قدر قانع‌کننده هستند که ارزش تحمل یک ضربه کوتاه‌مدت را دارند. تنها به پیامدهای فوری تصمیم خود فکر نکنید؛ تأثیرات بلندمدت را نیز بسنجید؛ از آینده مسیر شغلی و اهداف مالی گرفته تا وضعیت خانوادگی، سلامت روان و روابط اجتماعی.

۵ از چیزی فرار می‌کنم یا به سمت آن می‌روم؟

این پرسش تعیین می‌کند که استعفای شما واکنشی لحظه‌ای است یا حرکتی آگاهانه به سوی آینده‌ای بهتر. آیا صرفاً برای رهایی از یک وضعیت ناخوشایند تصمیم به ترک شغل گرفته‌اید، یا به خاطر دستیابی به فرصتی که با استعدادها، نقاط قوت و اهداف زندگی‌تان همخوانی دارد؟ بین «فرار از ناراحتی» و «حرکت به سمت رشد» تفاوت بزرگی وجود دارد. ترک یک محیط نامطلوب اشکالی ندارد، اما اگر مقصد و مسیر آینده‌تان روشن باشد، تصمیم‌تان نه تنها آسان‌تر، بلکه در بلندمدت رضایت‌بخش‌تر خواهد بود. داشتن یک هدف مشخص باعث می‌شود ترک شغل تبدیل به

است. هرگز نباید بدون در نظر گرفتن آن چه پس از ترک کار اتفاق خواهد افتاد، شغل خود را رها کنید. رها کردن ناگهانی شغل، ممکن است در لحظه، احساس خوبی ایجاد کند، اما بعداً می‌تواند برای‌تان دردسرساز شود.

پیش از ترک شغل، از خود پرسید: «امنیت مالی من چگونه است؟ قدم بعدی چیست؟». اگر پروژه بزرگی در سر می‌پرورانید؛ مثلاً قصد کارآفرینی و راه‌اندازی یک استارت‌آپ را دارید، فکر کنید چگونه اطمینان حاصل خواهید کرد که دیگران دچار مشکل نمی‌شوند؟ مطمئن شوید ترک کار برای‌تان به یک عادت قدیمی و ناپسند تبدیل نشده است و برای ترک کار، حتماً نقشه خروج مشخص ترسیم کنید. یک ترک شغل برنامه‌ریزی شده می‌تواند پایه و اساس موفقیت بعدی شما باشد.

۴ چه چیزی به دست می‌آورم و چه چیزی از دست می‌دهم؟

هر تصمیمی با نوعی بده بستان همراه است. بهتر است پیش از آن که تسلیم شوید و نامه استعفا را به رئیس بدهید، جوانب مثبت و منفی تصمیم‌تان را با دقت بسنجید. با ترک شغل، از چه چیزهایی فاصله می‌گیرید؟ ثبات؟ روابط؟ رشد کاری؟ و در مقابل، چه چیزهایی به دست می‌آورید؟ آزادی؟ آرامش خاطر؟ فضایی برای دنبال کردن اهداف بهتر؟

افتاده‌اید و این رفتن چه کمکی به شما خواهد کرد؟ اگر بمانید، چه اتفاقی ممکن است رخ دهد؟ اغلب اوقات نوشتن، باعث شفافیت ذهن و تصمیم‌گیری بهتر می‌شود.

۲ آیا همه راه‌های منطقی را امتحان کرده‌اید؟

ترک محل کار، بدون تلاش برای اصلاح شرایط، مانند رها کردن ماشینی است که سوخت آن تمام شده، در حالی که یک پمپ بنزین درست در همان نزدیکی قرار دارد. اگر تلاش کرده‌اید و نتیجه نگرفته‌اید؛ از خود پرسید: «آیا واقعاً تمام تلاشم را کرده‌ام؟» شاید لازم باشد یکبار دیگر شرایط کاری، راه‌حل‌های موجود و حتی امکان دریافت راهنمایی از دیگران را بررسی و آزمایش کنید. گاهی اوقات، آن چه غیرممکن به نظر می‌رسد؛ تنها به یک نگاه تازه یا دیدگاه متفاوت نیاز دارد. ناراحتی را با غیرممکن بودن، اشتباه نگیرید. رشد اغلب با ناراحتی همراه است. مهم این است که مطمئن شوید همه راه‌ها را آزموده‌اید تا پس از ترک کار، به سرعت پشیمان نشوید.

۳ استراتژی خروج من چیست؟

هر ترک شغل موفق، با برنامه‌ریزی همراه



گامی رو به جلو شود، نه صرفاً فاصله گرفتن از شرایط فعلی.

۶ آیا با «هیئت مدیره زندگی تان» مشورت کرده اید؟

اینجا منظور، هیئت مدیره محل کار نیست؛ بلکه جمع کوچکی از قابل اعتمادترین افراد زندگی شخصی شماست؛ اعضای خانواده، دوستان صمیمی، مربی یا همکاری که هم صادق است و هم از شرایط کاری شما کاملاً مطلع است. پیش از تصمیم به ترک شغل؛ با این افراد مشورت کرده و نظرشان را جویا شوید. این افراد اغلب، زاویه دیدی دارند که شما به دلیل نزدیکی بیش از حد به موقعیت شغلی، ممکن است نبینید.

البته هدف از این مشورت، تعیین تکلیف برای شما نیست، بلکه کمک به دیدن تصویر کامل و سنجیده تر تصمیم است. با افرادی مشورت کنید که حقیقت را می گویند؛ نه فقط حرف هایی که خوشایندتان است. و در نهایت، فراموش نکنید صدای درونی تان را هم بشنوید؛ همان حس غریزی که اغلب، مسیر درست را می شناسد.

۷ چه زمان بندیی برای ترک شغل در نظر دارید؟

گاهی مسئله این نیست که استعفا بدهید یا نه؛ بلکه این که چه زمانی این کار را انجام

مناسب تر را رقم می زند. هنگامی که در یک بستر درست، کارتان را ترک می کنید؛ پایان راه نیست بلکه آغاز مسیری بهتر خواهد بود.



ترک شغل زمانی درست است که دلیل واقعی تان را بشناسید، همه راه های اصلاح شرایط را آزموده باشید و با استراتژی خروج، زمان بندی و مشورت مناسب اقدام کنید. این تصمیم باید حرکتی آگاهانه به سوی رشد باشد، نه صرفاً فرار از ناراحتی.

دهید، اهمیت دارد.

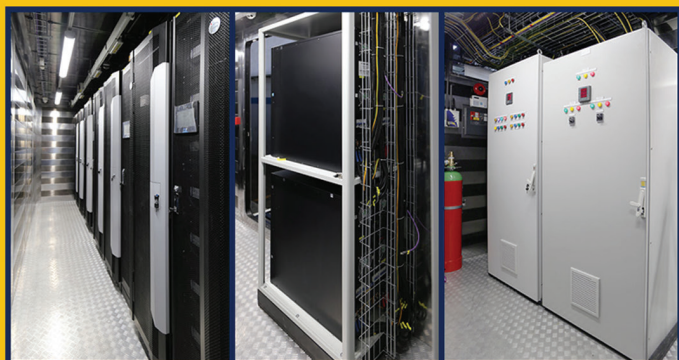
زمان تصمیم گیری شما، می تواند تفاوت های زیادی ایجاد کند. مثلاً، اگر پیش از پیدا کردن شغل جدید، استعفا دهید؛ ممکن است با فشارهای مالی روبرو شوید. یا اگر پیش از تحویل کامل پروژه ای ترک کار کنید؛ ممکن است به اعتبار خود لطمه زده و حقوق و مزایای کامل خود را از دست بدهید. خروج از شرکت در زمان مناسب، نه فقط تصمیمی هوشمندانه نیست؛ بلکه یک تصمیم استراتژیک است. به تاثیرات زنجیره ای زمان بندی خود دقت کنید: آیا پیش از رفتن، باید به نقاط عطف کلیدی برسید؟ آیا افراد مهمی باید از این موضوع مطلع شوند؟ برای همه چیز، برنامه ریزی و زمان بندی دقیق داشته باشید.

نتیجه گیری

خروج از یک شغل و یک سازمان، فاجعه نیست و گاهی می تواند شجاعانه ترین و هوشمندانه ترین اقدامی باشد که می توانید انجام دهید. مهم این است که این تصمیم را ساده نگیرید و حتماً پیش از ترک کار، زمان کافی برای تأمل و بررسی همه جوانب آن صرف کنید. مطمئن شوید که در مسیر درستی گام برمی دارید و خروج شما به معنای شکست نیست؛ بلکه انتخاب های بهتر، زندگی آرام تر و باکیفیت تر و رسیدن به موقعیت های شغلی



این مرکز داده
قابل حمل است



دلایل ساخت مرکز داده سیار:

- کمبود فضای فیزیکی
- برنامه‌ریزی برای استمرار کسب و کار
- محدودیت ساختمانی برای تأسیس مرکز داده ثابت
- نیاز به راه‌اندازی مرکز داده در کمترین زمان
- امکان انتقال سریع مرکز داده در شرایط فورس مازور



تلفن گویا: ۹۱۰۷۲۳۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
ایران: ۰۰۲۰۷۴۹۶۶
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

دیتاسنترهای هوش مصنوعی؛ هدف جنگ‌های آینده!

بمب‌ها روی اهداف جدید قفل شدند



منبع: cybernews.com

مترجم: میلاد شادفر

مقاله فنی

اشاره

هوش مصنوعی معادلات قدرت در جهان را دگرگون کرده است. در دنیای امروز، هر کشوری که در حوزه‌ی هوش مصنوعی قدرتمندتر و پیشروتر باشد؛ می‌تواند به قدرت مطلق تبدیل شود. اما این واقعیت، یک سوال نگران‌کننده را در دل خود پنهان کرده است: «آیا حملات فیزیکی در آینده، برای مثال، جنگ جهانی سوم، روی دیتاسنترهای AI متمرکز خواهند شد؟». به زبان ساده‌تر، «آیا در رقابت تسلیحاتی دیجیتالی آینده، مراکز داده یک هدف حیاتی محسوب شده و مورد هدف موشک‌ها و جنگنده‌ها و بمب‌ها قرار می‌گیرند؟»

اخیرا، «اریک اشمیت»، مدیرعامل سابق گوگل در یکی از سخنرانی‌های TED و در نقش یک توسعه‌دهنده سرکش هوش مصنوعی، به صراحت گفت: «انتخاب بعدی من چیست؟ مراکز داده‌ی شما را بمباران کنم؟»

شاید این جمله، در نگاه اول خیلی افراطی یا نمایشی باشد، اما با افزایش تنش‌های سیاسی نظامی در سراسر جهان، هیچ چیز در رقابت تسلیحاتی هوش مصنوعی، غیرممکن نیست! دنیای آینده ممکن است شاهد جنگ‌هایی باشد که نه برای تصرف خاک، بلکه برای نابودی مغزهای دیجیتالی قدرت‌ها یعنی دیتاسنترهای هوش مصنوعی شکل می‌گیرند.

جنگ‌های سایبری، فیزیکی می‌شوند

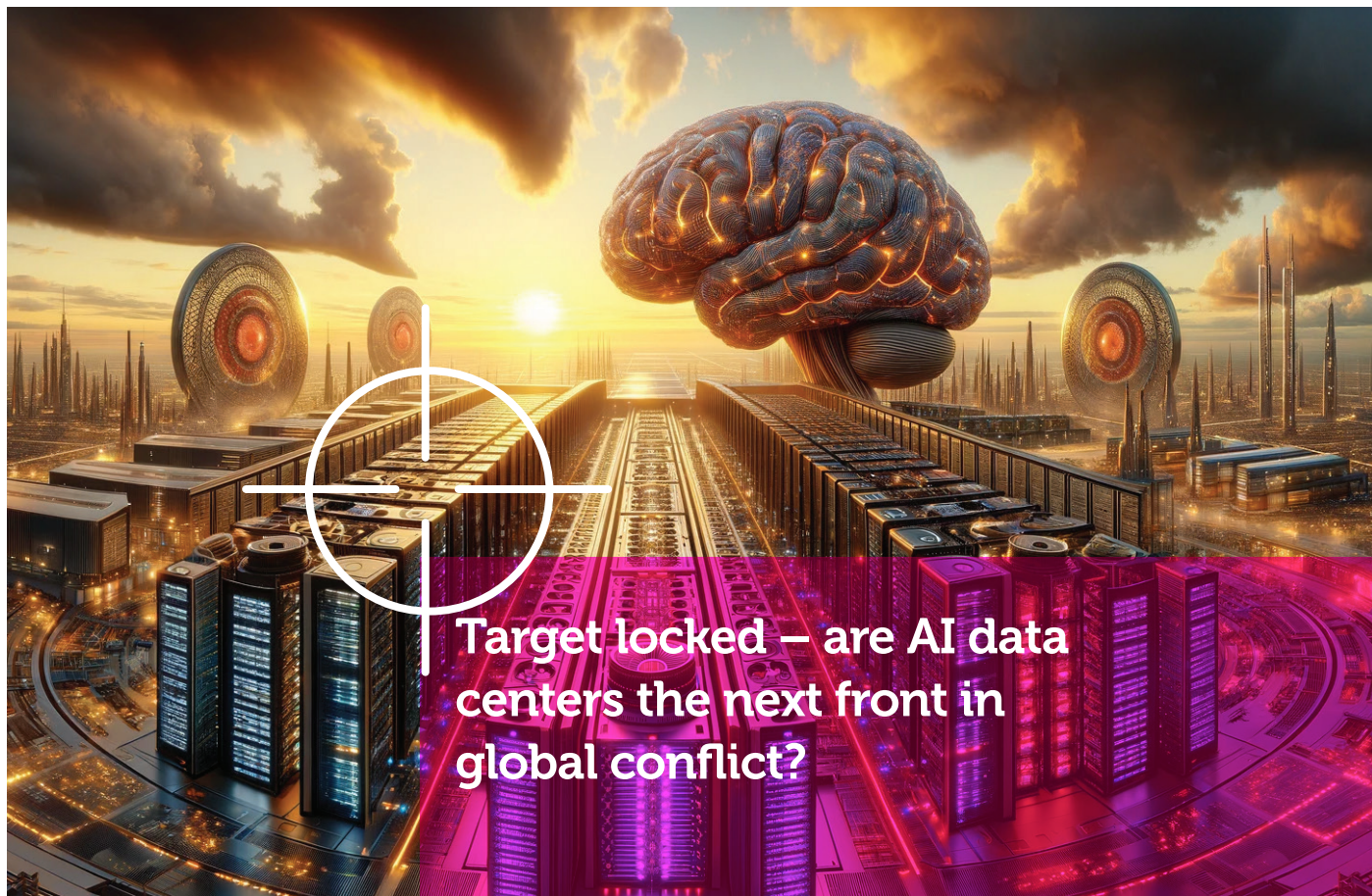
ساخت و استقرار دیتاسنترها در فضا برون‌داز آن‌ها را از تهدید بمباران‌های فیزیکی در امان دارند.

اما تا آن زمان، اگر کشوری بخواهد تاسیسات کلیدی هوش مصنوعی دشمن را از کار بیندازد؛ چه خواهد شد؟

یک متخصص امنیت شبکه با سابقه همکاری با سازمان‌های نظامی، که اکنون ریاست بخش امنیت سایبری موسسه FTI Consulting را بر عهده دارد؛ پیش‌بینی می‌کند: «به احتمال زیاد، تا ۵ سال آینده، دیتاسنترها هدف حملات فیزیکی قرار خواهند گرفت.» ممکن است چنین حملاتی در ابتدا با

در حال حاضر، رقابت برای تبدیل شدن به قدرت اول هوش مصنوعی در جهان، همه چیز را در بر می‌گیرد؛ از موتورهای جست‌وجو گرفته تا پهپادها و سیستم‌های خودران. در این میان، مراکز داده نقش حیاتی و بی‌بدیلی در پیشبرد این اهداف ایفا می‌کنند. بدون دیتاسنترهای قدرتمند مبتنی بر هوش مصنوعی، هیچ کشوری نمی‌تواند در این رقابت یا جنگ نرم حضور موثری داشته باشد. «اریک اشمیت» در همان سخنرانی TED، پیشنهاد می‌دهد که کشورها باید به سمت

هوش مصنوعی در حال بازتعریف معادلات قدرت جهانی است و کشورها برای سلطه، به مراکز داده AI تکیه دارند. با افزایش تنش‌های ژئوپلیتیکی، این مراکز می‌توانند به اهداف نظامی تبدیل شوند. حملات آینده شاید نه برای خاک، بلکه برای نابودی مغزهای دیجیتالی یعنی دیتاسنترها باشد.



Target locked – are AI data centers the next front in global conflict?

سرویس‌های مهم بانکی، مالی و نظامی را از کار بیندازد و حتی باعث قطع اینترنت شود. تاثیر چنین حمله‌ای، در برخی شرایط، می‌تواند بسیار مخرب‌تر از نابودی یک پالایشگاه نفت یا نیروگاه برق باشد.

اما در مقابل این اهمیت حیاتی، کارشناسان هشدار می‌دهند که بسیاری از دیتاسنترها همچنان فاقد اصول اولیه امنیت فیزیکی هستند. در بسیاری موارد، تنها یک موشک می‌تواند کل یک دیتاسنتر را از کار بیندازد، آن هم در حالی که هیچ دیتاسنتر پشتیبان دومی وجود ندارد یا پیش‌بینی‌های لازم برای تامین برق اضطراری، بازیابی فوری اطلاعات، و تعمیر سرورها و تجهیزات آسیب دیده، انجام نشده است.

در نتیجه‌ی سیاست‌های نادرست حکمرانی، دیتاسنترها اغلب در برج‌ها و ساختمان‌های مهم دولتی ساخته شده‌اند و در بهترین حالت، در زیرزمین طبقه منفی یک یا دو یک سازمان، مستقر هستند.

اگر آن ساختمان چه به عمد و چه به‌طور تصادفی هدف حمله فیزیکی قرار گیرد؛ نه تنها زیرساخت و دیتاسنتر آسیب می‌بیند، بلکه کل ساختمان نیز ممکن است فرو بریزد.

با گسترش رقابت جهانی در حوزه هوش مصنوعی، مراکز داده به زیرساختی حیاتی و در عین حال آسیب‌پذیر تبدیل شده‌اند که ممکن است در آینده هدف حملات فیزیکی قرار گیرند. نابودی یک دیتاسنتر می‌تواند اثراتی فراتر از حمله به پالایشگاه یا نیروگاه داشته باشد، اما بسیاری از آن‌ها هنوز فاقد امنیت کافی هستند.

شدت پایین‌تری آغاز شوند (مانند خرابکاری عمدی توسط یک کارمند، آتش‌سوزی عمدی یا حوادث پنهان) تا از درگیری‌های مستقیم نظامی جلوگیری شود. اما در نهایت، از کار انداختن دیتاسنترها با هدف کند کردن پیشرفت‌های هوش مصنوعی رقیب، یک هدف استراتژیک برای بسیاری از کشورها خواهد بود.

مراکز داده = منطقه خطر

امروزه، مراکز داده‌ی متمرکز و پرمصرف، جزو زیرساخت‌های حیاتی هر کشور به‌شمار می‌روند و به همین دلیل، به راحتی می‌توانند به اهداف فیزیکی حملات تبدیل شوند.

هدف قرار دادن یک مرکز داده، فقط به معنای کند کردن روند رشد فناوری یا توسعه‌ی هوش مصنوعی نیست؛ بلکه می‌تواند زیرساخت‌های ارتباطی و داده‌ای را مختل کند.



از این رو، در جنگ‌های آینده، دیتاسنترها به خطرناک‌ترین مناطق تبدیل خواهند شد؛ به طوری که شاید در یک پادگان نظامی یا برج نگهبانی، امنیت بیشتری نسبت به اتاق سرورها داشته باشید.

اگر یک دیتاسنتر هوش مصنوعی خاموش شود؛ چه اتفاقی می‌افتد؟

اگر به هر روشی، اعم از حمله فیزیکی، سایبری یا عملیات خرابکارانه یک ابرقدرت موفق شود یک دیتاسنتر هوش مصنوعی را از کار بیندازد یا نابود کند؛ پیامدهای سنگینی در پی خواهد داشت. مستقیم‌ترین نتیجه این اتفاق، توقف یا تعویق چند ماهه در فرآیند آموزش مدل‌های یادگیری زبان بزرگ (مانند ChatGPT) خواهد بود. اما ماجرا فقط به همین جا ختم نمی‌شود؛ بلکه دامنه‌ی تأثیرات، لایه‌لایه و عمیق‌تر می‌شود: از کار افتادن سیستم‌های مالی و بانکی، اختلال در دولت الکترونیک، توقف سرویس‌های خدماتی آنلاین، اختلال در خدمات لجستیکی، و حتی فلج شدن سامانه‌های هوش مصنوعی نظامی از جمله پیامدهای جدی آن است.

این موج تخریب دیتاسنترها می‌تواند به سرعت گسترش یابد و منجر به از دست رفتن اعتماد سرمایه‌گذاران، فرار نیروی انسانی متخصص، شکست پروژه‌های استراتژی، تشدید حملات سایبری و ایجاد اختلالات گسترده در شبکه و اینترنت شود.

کارشناس امنیت شبکه ما در این زمینه هشدار می‌دهد: «یک حمله فیزیکی به مراکز داده بزرگ هوش مصنوعی، تأثیر بسیار مخربی بر توسعه برنامه‌های AI خواهد داشت. برای مثال، آموزش مداوم یک مدل زبانی (LLM) را به تأخیر می‌اندازد و خدمات مبتنی

بر هوش مصنوعی رافلج می‌کند؛ ضمن این‌که موجی از نگرانی‌های گسترده در حوزه‌ی امنیت ملی به وجود می‌آورد.»

فایروال‌ها کافی نیستند

آنچه امروز به روشنی دیده می‌شود؛ این است که مراکز داده‌ی هوش مصنوعی به زیرساخت‌هایی حیاتی و استراتژیک تبدیل شده‌اند، اما همچنان از حفاظت‌های فیزیکی سطح بالا، برخوردار نیستند. چه این مراکز داده در زیرزمین ساخته شده باشند و چه در سطح زمین، نیاز به بازنگری و تقویت جدی در حوزه‌ی مقاوم‌سازی دیتاسنترها در برابر حملات فیزیکی آینده و همچنین حملات سایبری نسل جدید، به شدت احساس می‌شود. این هشدار را کارشناسان امنیت شبکه درباره دیتاسنترهای ایالات متحده مطرح کرده‌اند؛ چه برسد به دیتاسنترهایی که در سایر کشورها ساخته می‌شوند مراکزی که معمولاً از نظر معماری، طراحی‌های امنیتی و زیرساخت‌های فیزیکی، در سطحی به مراتب ضعیف‌تر قرار دارند.

در دنیایی که محاسبات و الگوریتم‌ها به ابزاری برای قدرت تبدیل شده‌اند؛ حفاظت و امنیت به اندازه‌ی نوآوری، اهمیت پیدا کرده‌اند و نیازمند سرمایه‌گذاری، برنامه‌ریزی، و ارتقای دائمی هستند.

چند سال پیش، یک تحلیل‌گر مسایل امنیت و حریم خصوصی در اینترنت، پیش‌بینی عجیبی ارائه داد: «به‌زودی باید به جای فایروال‌ها و سیستم‌های شناسایی و مسدودسازی حملات DDoS، برای هر شبکه یک تیربار یا ضدهوایی در نظر گرفت». در آن دوران، بسیاری از رسانه‌ها این ایده را اغراق‌آمیز دانستند، اما امروز، با تشدید تهدیدات سایبری و فیزیکی، این پرسش جدی‌تر از همیشه مطرح می‌شود:

«آیا دیتاسنترها در یکی از ۷ لایه‌ی امنیتی خود نیازمند تجهیزاتی مانند ضدهوایی، سامانه ضدپهپاد، موشک‌انداز، گیت‌های ضدنفوذ و رادار هستند؟»

شاید پاسخ این سؤال در گذشته منفی بود، اما امروز — در عصر رقابت‌های تسلیحاتی دیجیتال و جنگ‌های هیبریدی — باید آن را با جدیت بررسی کرد. فایروال‌ها دیگر کافی نیستند.

نتیجه‌گیری

جنگ‌های آینده ممکن است بیش از آن‌که انسانی باشند، داده‌محور و مبتنی بر تصمیم‌گیری‌های هوش مصنوعی باشند. در چنین شرایطی، حمله به منابع پردازش و ذخیره‌سازی داده (دیتاسنترها) بسیار منطقی‌تر و موثرتر از حمله به تجهیزات نظامی سنتی خواهد بود. دیتاسنترهای بزرگ هوش مصنوعی، در واقع مغز دیجیتال یک کشور محسوب می‌شوند. نابودی یا اختلال در عملکرد آن‌ها می‌تواند هوش مصنوعی نظامی، امنیتی یا اقتصادی کشور را از کار بیندازد؛ دسترسی به داده‌های حیاتی را قطع کند و الگوریتم‌ها و مدل‌های حساس را نابود یا حتی فاش کند. در آینده‌ای نه‌چندان دور، دیتاسنترها به اهداف نظامی و استراتژیک تبدیل خواهند شد. از این رو، حفاظت از آن‌ها، باید به اندازه‌ی حفاظت از پایگاه‌های نظامی مهم تلقی شود. ساخت دیتاسنترهایی با ویژگی‌هایی مانند مقاومت بالا، طراحی توزیع‌شده، استقرار زیرزمینی و توان مقابله با بمب‌های الکترومغناطیسی (EMP) و حملات موشکی، دیگر یک انتخاب نیست؛ بلکه یک ضرورت در سطح امنیت ملی است.

نکته ها و گفته ها

- اگر می خواهید شجاعان را بیابید، کسانی را جستجو کنید که قادر به بخشودن هستند و اگر می خواهید قهرمانان را بیابید، کسانی را بجویید که قادرند در مقابل نفرت عشق بورزند. (بهاگاوادگیتا)
- شما هم می توانید هر کاری را که دوست دارید، بکنید؛ اگر فقط باور کنید که می توانید. (جک کانفیلد)
- زندگی یک بوم نقاشی است که در آن از پاک کن خبری نیست. (جک کانفیلد)
- مردم از من می پرسند چه زمان قصد بازنشستگی دارم. من به آنها می گویم هم اکنون هم بازنشسته هستم. من آن چیزی را که سرگرم انجامش هستم کار نمی دانم. (نورمن برودسکی)
- هر چیزی که می آفرینید، نتیجه تصمیم هایی است که گرفته اید و از راه تصمیم هایی که می گیرید، آزادی تان را به دست می آورید. (دان کارلن)
- مرا برای دزدیدن تکه نانی به زندان انداختند و پانزده سال در آنجا نان مجانی خوردم! این دیگر چه دنیایی است؟ (ویکتور هوگو)
- در زندگی هر وقت به دو راهی رسیدم می دانستم کدام راه را انتخاب کنم و همیشه اشتباه بود به خاطر اینکه راه ساده تر را انتخاب کردم (آل پاچینو)
- غمگین نشو وقتی کسی تلاشت را نمی بیند و هنرت را درک نمی کند. طلوع خورشید منظره ای تماشایی است اما بیشتر مردم همیشه آن موقع صبح خواب هستند. (جن لنون)
- مهمترین اصل انسانیت است: اگر کسی از من کمکی بخواهد، یعنی من هنوز روی زمین ارزش دارم. (پائولو کوئیلو)
- افراد با یکدیگر متفاوت هستند؛ هر قدر در مورد اینکه دیگران کاری را بهتر از شما انجام می دهند غرولند کنید، هیچ تأثیر مثبتی در تغییر فردی شما نخواهد داشت. (وین دایر)
- کسی که خواب باشد را اگر صدا کنیم بیدار می شود. اما هستند کسانی که خود را به خواب زده اند و با هیچ صدایی بیدار نمی شوند. (علی شریعتی)

اگر به رئیس مان دروغ گفتیم و او متوجه شد؛ چه باید کرد؟

۴ اقدام مهم پس از فاش شدن دروغ

منبع: fastcompany.com



✍ مترجم: کیوان کمالی

اشاره

عدم صداقت در محل کار می تواند به روابط حرفه ای و اعتبار شما آسیب بزند. اگر این عدم صداقت نسبت به رئیس تان رخ داد؛ با خطرات بیشتری روبرو خواهید شد. بهترین کار این است که هرگز به رئیس تان دروغ نگویید، اما اگر این اتفاق افتاد؛ اقداماتی وجود دارد که می تواند به کاهش آسیب کمک کند. در این مقاله یک برنامه ۴ مرحله ای ارائه شده است که در آن به مدیریت بحران و حفظ شغل پس از فاش شدن دروغ، پرداخته ایم.

مقاله مدیریتی

است که احتمالاً همکاران تمایلی به همکاری با شما نخواهند داشت یا ایده های خود را با شما به اشتراک نمی گذارند.

چرا افراد در محل کار دروغ می گویند؟

مردم معمولاً در محل کار به همان دلایلی دروغ می گویند که در خارج از محل کار دروغ می گویند: «برای بهتر به نظر رسیدن». مورین می گوید: «رایج است که افراد درباره یک اشتباه یا مسئله ای که می تواند آن ها را به دردسر بیندازد، دروغ بگویند. همچنین دروغ گفتن در مورد دستاوردها برای تحت تأثیر قرار دادن دیگران نیز امری متداول است.»

چرا صادق بودن در محل کار اهمیت زیادی دارد؟

به طور کلی، علاوه بر دلایل اخلاقی برای دروغ نگفتن، همه افراد ترجیح می دهند با همکارانی کار کنند که قابل اعتماد باشند. بنابراین عضویت در یک تیم به معنای راستگو بودن نیز هست. همکاران شما می خواهند در کار با شما احساس راحتی و امنیت داشته باشند. «ایمی مورین»، روان درمانگر ساکن فلوریدا و نویسنده کتاب «۱۳ کاری که افراد با ذهن قوی انجام نمی دهند»، توضیح می دهد: «اگر دروغ بگویید، ممکن است همکاران تان نگران شوند که ممکن است کاری انجام دهید که به آن ها آسیب برساند. مثلاً ممکن است اعتبارشان را زیر سوال ببرید؛ ایده های شان را بدزدید یا وجهه شرکت را تضعیف کنید.» او همچنین خاطرنشان می کند که یکی دیگر از پیامدهای شناخته شدن به عنوان فردی دروغگو این

آیا دروغ گویی در محل کار خوب است یا شما را دچار مشکلات می کند؟



What should you do if you get caught lying to your boss?

اگر به رئیس خود دروغ گفتید؛ چه باید بکنید؟

به محض اینکه دروغی از دهانتان خارج شد یا ایمیلی حاوی اطلاعات نادرست ارسال کردید؛ زمان آن رسیده است که بپذیرید کاری که انجام داده‌اید، اشتباه بوده و باید سریعاً برای جبران آن اقدام کنید.

در چنین شرایطی، مسئولیت‌پذیری مهم‌ترین کار است. مورین می‌گوید: «نزد رئیس برو و نشان بده که می‌خواهی موضوعی را روشن کنی.» مثلاً می‌توانید بگویید: «می‌خواهم مکالمه‌ای که قبلاً داشتیم را شفاف کنم. من به‌طور ضمنی گفتم که هرگز ایمیل را ندیده‌ام. من آن را دیدم، اما پاسخی ندادم. نمی‌خواستم غیرمسئول به نظر برسم و این کار من اشتباه بود.»

مورین توضیح می‌دهد: وقتی رئیس‌تان ببیند که می‌توانید پاسخ‌گو باشید و تمایل دارید صادقانه رفتار کنید؛ این موضوع می‌تواند در حفظ اعتماد آینده بسیار مؤثر باشد. اما اگر نتوانید به سرعت مسئولیت کار خود را بپذیرید و رئیس‌تان پیش از اعتراف شما، به دروغ پی ببرد؛ مورین چند گام برای مدیریت وضعیت

- پیشنهاد می‌کند:
- حقیقت را بپذیرید.
- مسئولیت بپذیرید.
- عذرخواهی کنید.
- پیشنهاد جبران بدهید.

با پیش‌قدم شدن، نشان می‌دهید که مایل به پاسخ‌گویی هستید و تلاش می‌کنید وضعیت را اصلاح کنید. لازم است درباره آن چه گفته‌اید روراست باشید و سپس واقعیت را بیان کنید. مورین مثالی ارائه می‌دهد: «می‌خواهم موضوعی را روشن کنم. قبلاً گفتم که سال گذشته یک میلیون دلار کالا فروخته‌ام. در حقیقت باید اعتراف می‌کردم که این کار را به تنهایی انجام نداده‌ام. بلکه این تیم من بود که این مقدار را فروخت.»

یک رویکرد حرفه‌ای دیگر، عذرخواهی صمیمانه است. مورین می‌گوید: «و اگر کاری

هست که می‌توانید برای جبران انجام دهید، آن را پیشنهاد کنید.» نشان دادن حسن نیت نیز گامی مثبت در این مسیر است. برای مثال، می‌توانید بگویید: «من یک ایمیل پیگیری ارسال می‌کنم و توضیح می‌دهم که این اشتباه از جانب شما نبوده است.»

پذیرش کامل مسئولیت (بدون بهانه تراشی)

اولین واکنش مهم، پذیرفتن اشتباه به‌طور مستقیم است. جملاتی مثل «شرایط سخت بود» یا «من مجبور شدم» معمولاً نوعی فرار از مسئولیت را نشان می‌دهد. بهتر است کوتاه، شفاف و مستقیم بگویید: «این تصمیم اشتباه من بود و بابتش عذرخواهی می‌کنم.» مدیر و همکاران باید بدانند چرا این اتفاق افتاده است، اما توضیح شما باید خلاصه و صادقانه باشد. هدف شفاف‌سازی است نه



توجیه. از گفتن جزئیات غیرضروری یا نامرتبط که ممکن است حس «پیچاندن» یا طفره رفتن ایجاد کند؛ پرهیز کنید. به قول معروف، یک توضیح کوتاه بدهید و وارد دفاعیه طولانی نشوید.

مسئولیت‌پذیری فقط در مرحله اعتراف کافی نیست و باید نشان دهید که به دنبال تغییر رفتار و جبران خسارت هستید. این روند را نیز باید در طولانی مدت ادامه دهید تا حس ثبات و اطمینان در ذهن رئیس‌تان شکل بگیرد. اعتماد با یک عذرخواهی ساده باز نمی‌گردد؛ بلکه باید در طول زمان و با رفتارهای کوچک اما مداوم ترمیم شود.

برای بازسازی اعتماد با مدیرتان چه اقداماتی باید انجام دهید؟

درک کنید که بازسازی اعتماد، یک فرآیند زمان‌بر است. بنابراین باید در تعاملات خود با مدیر و همکاران، صداقت را به عنوان اولویت اصلی قرار دهید.

به تعهدات، زمان‌بندی‌ها و وظایفی که به شما محول شده؛ پایبند باشید. از وعده‌های غیرواقعی پرهیز کنید و حتی در کوچک‌ترین مسایل نیز سعی کنید شفاف‌سازی داشته باشید تا از بروز سوءتفاهم‌ها جلوگیری شود. به خاطر داشته باشید که در این شرایط، رابطه شما شکننده است و کوچک‌ترین خطای سهوی یا اطلاعات نادرست می‌تواند اعتماد را دوباره تخریب کند.

«نیکولت لینزا»، درمانگر در LifeStance Health در شهر اوهایو، می‌گوید: «کلید بازسازی اعتماد، ثبات در راستگویی و شفافیت است.

اعمال، بلندتر از کلمات صحبت می‌کنند، بنابراین با نشان دادن اخلاق کاری فوی و ایفای نقش یک عضو فعال در تیم، می‌توانید در مسیر خوبی برای بازگرداندن اعتماد قرار بگیرید.»

مسئولیت‌پذیری نیز بخشی از رشد و موفقیت شما است. لینزا می‌گوید: «مهم است نشان دهید که درک کرده‌اید دروغ شما چه اثری بر دیگران و فرهنگ سازمان داشته است. این رویکرد، لحنی ایجاد می‌کند که نشان می‌دهد با درس گرفتن از اشتباه، آماده حرکت رو به جلو هستید.»



چرا صداقت در محیط کار حیاتی است، چرا افراد ممکن است به رئیس خود دروغ بگویند و در صورت وقوع، چه اقداماتی برای پذیرش، عذرخواهی، جبران و بازسازی اعتماد باید انجام شود. همچنین بر اهمیت ثبات در راستگویی، مسئولیت‌پذیری و یادگیری از اشتباه برای رشد حرفه‌ای تأکید دارد.

همچنین جلب اعتماد همکاران می‌تواند در جمع‌های غیررسمی (ناهار، گفت‌وگوهای کوتاه) سریع‌تر اتفاق بیفتد. رفتار دوستانه، گوش دادن فعال و کمک داوطلبانه می‌تواند

حس «بازگشت» شما را تقویت کند.

در نهایت، باید نشان دهید مکانیزمی برای جلوگیری از تکرار ایجاد کرده‌اید؛ اقداماتی مانند ثبت دقیق داده‌ها، مشورت گرفتن قبل از تصمیم‌های حساس، یا شفاف‌سازی فرآیندها، پیام مهمی منتقل می‌کند: این که دروغ‌گویی شما یک لغزش بوده، نه یک عادت.

در صورت بخشیده شدن، چه اقداماتی را می‌توانید به رئیس خود پیشنهاد دهید؟

مورین، روان‌درمانگر، پیشنهاد می‌کند با مدیر خود در مورد نحوه پیشرفت صحبت کنید. مورین می‌گوید: «حتی اگر لازم باشد هر هفته به یک سرپرست اجازه دهید کار شما را بررسی کند، یا این که روزانه شکست‌ها و نقاط ضعف را گزارش دهید. بهتر است برنامه‌ای مشخص تدوین کنید تا روند رشد و پیشرفت شما قابل مشاهده باشد.»

اگر به دلیل دروغ‌گویی اخراج شوید؛ چه اتفاقی می‌افتد؟

در این شرایط، مهم‌ترین کار این است که تجربه را به عنوان یک درس زندگی بپذیرید و مسئولیت کامل آن را بر عهده بگیرید. مورین می‌کند: «به دام وسوسه سرزنش دیگران برای اعمال خود نیفتید. اشتباهات را تحلیل کنید، درس‌ها را استخراج کنید و سپس به این فکر کنید که در موقعیت‌های مشابه در آینده، چگونه می‌توانید شرایط را به گونه‌ای متفاوت و بهتر مدیریت کنید.»

چگونه خطرات ایمنی محل کار دیتاسنترها را کاهش دهیم؟

ایمنی محیط‌های مرکز داده برای نیروی انسانی، حتی از ایمنی تجهیزات و دیتاها مهم‌تر است

منبع: datacenterknowledge.com



مترجم: علی رضا گنجی

مقاله فنی

اشاره

وقتی متخصصان مرکز داده درباره مدیریت خطرات (risk management) صحبت می‌کنند؛ اغلب تمرکزشان بر محافظت از سرورها و زیرساخت‌های فناوری اطلاعات است. به هر حال، مراکز داده ساخته شدند تا کمترین قطعی و بالاترین امنیت برای دارایی‌های دیجیتالی را داشته باشند؛ اما ایمنی محل کار نیز به همان اندازه مهم و حیاتی است. انسان‌ها نیز به اندازه سخت‌افزارها، در محیط‌های دیتاسنتر با خطرات قابل توجهی روبرو هستند. از خطرات الکتریکی و برق‌گرفتگی تا سیستم‌های اطفای حریق، گرمای شدید و سروصداها. دیتاسنترها، چالش‌های ایمنی محیط کار منحصربه‌فردی دارند باید مورد توجه کارفرمایان و اپراتورها قرار گیرند و تمام نکات لازم برای محافظت از کارمندان و پیمان‌کاران صورت گیرد. این مقاله به بررسی خطرات کلیدی مطرح در محیط کار مراکز داده پرداخته و راه‌کارهایی برای کاهش آن‌ها ارائه می‌کند.

مراکز داده و ایمنی محل کار

محیط‌ها باشند و بخشی دیگر از نیروی انسانی، وظیفه تعمیر و نگهداری فضا و ساختار فیزیکی محیط دیتاسنتر را برعهده دارند. بنابراین، اپراتورهای مراکز داده وظیفه دارند محیط کار این افراد را امن نگه دارند. تضمین ایمنی مراکز داده نه تنها یک کار درست است؛ بلکه در بسیاری از کشورها از جمله ایالات متحده، یک الزام از سوی اداره ایمنی و بهداشت شغلی موسوم به OSHA است. بسیاری از ممیزی‌ها و مجوزهای دیتاسنترها صادر نمی‌شود تا اینکه قوانین ایمنی محیط کار در آن‌ها کاملاً رعایت و با استانداردهای رایج، منطبق باشد.

عمده تهدیدات ایمنی محیط کار دیتاسنترها به این شرح است:

اگرچه حضور نیروی انسانی در داخل اکثر مراکز داده، محدود و موقتی و برای بازه‌ای کوتاه است ولی نمی‌توان از این مسئله چشم‌پوشی کرد که تکنسین‌ها و مهندسان مراکز داده، بخشی از زمان کاری خود را محل تجهیزات و تاسیسات طی می‌کنند. آن‌ها وظایف فیزیکی مانند راه‌اندازی سرورها و وصل کردن کابل‌ها را انجام می‌دهند و نمی‌توان این کارها را از راه دور انجام داد.

افزون بر این، تکنسین‌های دیگری هم به دلایل مختلف، وارد محیط اصلی مراکز داده می‌شوند؛ برخی باید سیستم‌های سرمایشی را بازرسی و تجهیزات HVAC جدید را نصب و راه‌اندازی کنند تا سرورها همیشه خنک بمانند. متخصصان و کارمندان امنیت شبکه باید دنبال رفع تهدیدات فیزیکی در این

ایمنی کارکنان در مراکز داده به‌اندازه حفاظت از تجهیزات حیاتی است؛ چراکه خطراتی چون برق‌گرفتگی، گرما و سروصدا، جان انسان‌ها را تهدید می‌کنند. این مقاله راهکارهایی برای کاهش این خطرات محیطی ارائه می‌دهد.

How to Manage Data Center Workplace Safety Risks



۱- خطرات الکتریکی

مراکز داده مقدار زیادی برق مصرف می‌کنند که از طریق شبکه‌ای پیچیده از کابل‌ها، پل‌های توزیع برق، پریزها و باتری‌ها به تجهیزات الکترونیکی و رک‌ها می‌رسد. در اینجا، کابل‌های عایق‌بندی نشده، اتصالات برقی شل یا نیم سوز شده که می‌توانند منجر به جرقه و آتش‌سوزی شوند؛ خطرانی ایجاد می‌کنند که ممکن است به کارمندان آسیب وارد کند. با توجه به اینکه ولتاژ بالایی از طریق خطوط برق دیتاسنتر جریان است؛ یک شوک الکتریکی می‌تواند تأثیری فاجعه‌بار داشته باشد.

۲- خطرات زمین خوردن کارمندان

محیط‌های مرکز داده به گونه‌ای هستند که خطرات افتادن، پرت شدن و زمین خوردن کارگران زیاد است. در غالب دیتاسنترها، بخش

عظیمی از کابل‌های شبکه و برق از بالای رک‌ها و تجهیزات الکتریکی عبور کرده و کار و مدیریت آن‌ها، خطرات بالقوه‌ای مانند زمین خوردن را ایجاد می‌کند؛ موضوعی که موسسه OSHA نیز تمرکز کلیدی روی آن دارد.

۳- گرمای بیش از حد

مراکز داده به دلیل تولید حرارت بسیار زیاد توسط تجهیزات الکترونیکی، غالباً محیط‌های بسیار گرمی هستند. اگرچه، سیستم‌های سرمایشی در این محیط‌ها نصب شده و سعی می‌شود دما در یک بازه استاندارد و عادی نگه داشته شود تا تجهیزات فناوری اطلاعات خوب کار کنند اما همیشه کل محیط دیتاسنتر

خنک نیست. این موضوع برای سیستم‌های سرمایشی پیشرفته مانند فناوری جدید directtochip که سعی می‌کند درون سرور خنک باشد و گرما را از داخل سرور به بیرون هدایت می‌کند؛ برای کارمندان دیتاسنتر چالش برانگیز می‌شود و معمولاً در محیطی بسیار گرم باید کارهای فنی و تعمیر و نگهداری را انجام بدهند. در نتیجه، محیط‌های گرم مراکز داده می‌توانند یک خطر برای افرادی باشند که به مدت طولانی باید در آنجا کار کنند.

۴- اجسام سنگین

یک سرور زیاد سنگین نیست ولی وقتی چند سرور را درون یک رک جاسازی می‌کنید؛ این

کار نه تنها مدیریت کابل‌های در آینده را ساده‌تر می‌کند؛ بلکه از پخش شدن کابل‌ها و زمینه‌سازی بروز حوادثی مانند جرقه زدن، بریدگی، زمین خوردن نیروی انسانی و ... جلوگیری می‌کند.

۳- هنگام طراحی سیستم سرمایشی، فقط به فکر سرورها و رک‌ها نباشید و دمای محیط دیتاسنتر را هم در نظر بگیرید تا فضا و دمای مناسب کار طولانی‌مدت چند ساعته فراهم باشد.

۴- اگر دمای اتاق سرور باید بالاتر از ۸۰ درجه فارنهایت باشد؛ اطمینان حاصل کنید تکنسین‌های دیتاسنتری که می‌خواهند برای طولانی‌مدت در آن جا کار کنند؛ تمام نکات ایمنی گفته شده در استانداردها و قوانین کار را رعایت می‌کنند.

۵- دستورالعمل‌هایی برای جابه‌جایی و کار با اجسام سنگین و همچنین مدیریت آن‌ها تدوین و به کارمندان آموزش دهید تا از هرگونه سقوط جلوگیری شود.

۶- اطمینان حاصل کنید رک‌های سرور به کف یا به دیوار و همچنین در صورت نیاز به یکدیگر متصل شدند و کاملاً محکم هستند؛ به طوری که خطر سقوط ندارند.

۷- کارمندانی که دائماً در میان رک‌ها و سرورها مشغول کار هستند؛ باید از هدفون‌های بزرگ گوشی استفاده کنند؛ هدفون‌هایی که قابلیت نویز کنسلینگ دارند و می‌توانند مقداری از نویز آلودگی صوتی محیط را کاهش دهند.

۸- محیط اصلی مرکز داده باید دارای تهویه و فیلتراسیون مناسب باشد؛ استفاده از سیستم‌های تهویه مطبوع با فیلترهای HEPA یا فیلترهای صنعتی با قابلیت جذب ذرات ریز و گرد و غبار در این زمینه بسیار کمک‌کننده است.

۹- برنامه مدونی برای جلوگیری از ورود گردوغبار به داخل مرکز داده داشته باشید. اجرای برنامه نظافت منظم برای کف کاذب، سقف، رک‌ها و مسیرهای کابل‌کشی ضروری است و استفاده از جاروبرقی‌های صنعتی با فیلتر مناسب برای جلوگیری از پراکنده شدن ذرات در هوا نیز توصیه می‌شود.

نتیجه‌گیری

هرچقدر روی ایمنی کارمندان در محیط کار، سرمایه‌گذاری کنید؛ به ویژه در محیط‌هایی مانند دیتاسنترها که خطرات بالقوه‌ای با درجه بالا مطرح است؛ هم خیالتان آسوده خواهد بود که اتفاق غیرمنتظره‌ای رخ نمی‌دهد و هم خود تکنسین دیتاسنتر شما با شوق و اطمینان و انگیزه بالاتری، فعالیت خواهد کرد.

کاذب یا روی فیلترها ممکن است مشکلات آلرژیک یا تنفسی ایجاد کند.

همچنین، شیفتهای شبانه، آماده‌باش دائمی و نیاز به پاسخ سریع در زمان قطعی، باعث استرس زیاد و فرسودگی شغلی می‌شود. در برخی دیتاسنترها، شاهد خطرات دیگری مانند ورود افراد غیرمجاز به داخل این محیط‌ها و حمله به کارمندان دیتاسنتر برای خرابکاری یا نفوذ به شبکه بودیم.

چگونه خطرات محیط‌های مرکز داده را مدیریت و کاهش دهیم؟

اگرچه این طور به نظر می‌رسد که تهدیدات زیادی در محیط‌های دیتاسنتر برای کارگران و نیروی فنی وجود دارد ولی خوش‌بختانه، مدیریت همه آن‌ها نسبتاً ساده است. برای به حداقل رساندن خطرات ایمنی محل کار، اپراتورهای مرکز داده باید بهترین شیوه‌ها را در نظر بگیرند:

۱- باید سیستم‌های الکتریکی به طور مرتب بازرسی شوند تا کابل‌ها و تجهیزات معیوب و از کار افتاده‌ای که می‌توانند به کارمندان آسیب برسانند؛ شناسایی و رفع شوند.

۲- کابل‌ها را سازماندهی کنید. انجام این

رک چند صد پوند وزن خواهد داشت. باتری‌ها، یوپی‌اس‌ها، واحدهای سرمایش و برخی دیگر از قطعات و تجهیزاتی که در دیتاسنترها می‌بینیم؛ سنگین وزن هستند و جابه‌جایی آن‌ها می‌تواند برای کارمندان خطرناک باشد. همچنین، اگر یک رک بیش از حد سنگین شده یا نصب و پیکربندی فیزیکی درستی نداشته باشد؛ خطر افتادن آن روی کارمندی که مشغول تعمیر یا تعویض یک سرور آن یا رک کنار دستی است؛ وجود دارد.

۵- آلودگی صوتی

صدای مداوم فن‌ها، تجهیزات سرمایشی و سرورها می‌تواند باعث آسیب شنوایی در بلندمدت برای کارمندان شود یا باعث خستگی ذهنی آن‌ها گردد. مراکز داده به محیط‌های با آلودگی صوتی بالا، مشهور هستند و گریزی از این امر نیست اما باید خود نیروی انسانی و مدیریت مرکز داده، تأثیرات این خبر همیشگی را کاهش دهند.

۶- ریسک‌های تنفسی، استرس و فرسودگی روانی و ...

فهرست خطرات ایمنی محیط دیتاسنترها طولانی است. نشأت گازهای خنک‌کننده یا مواد شیمیایی خاص می‌تواند برای سیستم تنفسی مضر باشد. گرد و غبار انباشته در کف

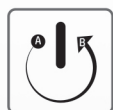


کار در مراکز داده با خطراتی چون برق‌گرفتگی، گرمای شدید، سقوط اجسام سنگین، آلودگی صوتی و مشکلات تنفسی همراه است. این محیط‌ها همچنین استرس‌زا هستند و نیاز به تدابیر ایمنی جدی برای حفاظت از کارکنان دارند.

ipoWVER[®]

TPD-916M

ATS (Automatic Transfer Switch PDU) Power Distribution Unit



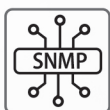
Auto Switch
Power ON (16m/S)



12 IEC60320
C-13



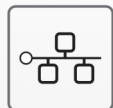
04 IEC60320
C-19



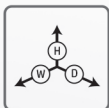
SNMP Protocol



Control Input &
Output Voltage



NET: Ethernet Port



483x90x220
Set Dimensions
(mm)



Customize



7 Segment
Display

سریع و بی وقفه
همواره متصل!!

نسل هوشمند پیل های
توزیع برق داخل رک

“
The fastest
recorded rate is about 80 beats
per second Hummingbird
”



مشخصات فنی:

- دارای ۱۲ پریز IEC60320 / C-13 و ۴ پریز IEC60320 / C-19 به منظور سهولت و قابلیت کارکرد با انواع دستگاهها
- مجهز به سیستم ارت، قابلیت انتقال جریان ۱۰ آمپر از هر پریز C-13 و 16 آمپر از هر پریز C-19 و ۳۲ آمپر به صورت کلی
- قابلیت تعویض منبع برق A و B به صورت خودکار و دستی در بازه زمانی مجاز (حدود ۱۶ میلی ثانیه)
- تنظیم بازه مورد نظر از لحاظ کل جریان و ولتاژ ورودی
- امکان نصب کارت SNMP



تلفن گویا: ۹۱۰۷۲۳۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
اپراتور: ۰۰۹۴۷۲۰۰
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

هنر تصمیم‌گیری در بحران؛ چگونه کسب‌وکارمان را در طوفان‌ها نجات دهیم!

۵ تصمیم‌گیری حیاتی که رهبران کسب‌وکارها باید در دل بحران‌ها اتخاذ کنند



منبع: inc.com

✍ مترجم: نرگس روحانی

اشاره

مقاله مدیریتی

در دنیای پرشتاب و به‌شدت متغیر امروز، وقوع بحران دیگر یک احتمال دور از ذهن نیست؛ بلکه بخشی جدایی‌ناپذیر از واقعیت محیط کسب‌وکار است. از جنگ‌ها و بلایای طبیعی گرفته تا حملات سایبری، بحران‌های اقتصادی، کمبود منابع یا حتی قطع دسترسی به زیرساخت‌های حیاتی مانند اینترنت، همگی می‌توانند سازمان‌ها را به‌طور مستقیم و شدید تحت تأثیر قرار دهند. ما به تازگی نمونه‌ای واقعی از این بحران را تجربه کردیم: جنگ ۱۲ روزه ایران در خرداد ماه! بحرانی که ناگهانی، شوکه‌آور و ضربه‌زننده بر پیکره صنعت IT و زیست بوم فناوری کشور فرود آمد و در دل خود ده‌ها بحران دیگر را نیز به همراه داشت؛ از قطعی اینترنت و اختلال در دسترسی به هاست، سرور و دیتاسترها گرفته تا تعطیلی کسب‌وکارها، هک سایت‌ها و موج گسترده حملات سایبری، سرقت اطلاعات کاربران، از کار افتادن سرویس‌های آنلاین مهم و حیاتی، اختلالات GPS و بدتر اینکه هیچ‌کس نمی‌دانست این وضعیت تا چه زمانی ادامه خواهد داشت! در چنین شرایطی، آن‌چه یک سازمان را از فروپاشی نجات می‌دهد یا برعکس به سمت سقوط می‌کشاند؛ تصمیمات مدیران در لحظات بحرانی است. تصمیم‌گیری درست می‌تواند سازمان را حتی در میانه بحران به سمت فرصت‌های تازه هدایت کند، در حالی که تصمیمات شتاب‌زده یا انفعالی، آسیب‌ها را چند برابر خواهد کرد. در این مقاله، به مهم‌ترین تصمیماتی می‌پردازیم که رهبران کسب‌وکار باید در شرایط ناپایدار، غیرقطعی، غیرقابل پیش‌بینی و غیرعادی اتخاذ کنند.

دارد: حفظ حیات سازمان در کنار جستجوی

مسیرهای جدید برای رشد. تعطیلی، عدم تصمیم‌گیری یا انتظار برای پایان یافتن بحران، هنری نیست که یک مدیر کسب‌وکار از خود نشان بدهد. مدیران برای چنین لحظاتی آموزش دیده‌اند، مهارت کسب کردند، و مسئولیت پذیرفته‌اند. نگاه تمام کارکنان یک سازمان به تصمیم رئیس است و اگر رئیس خودش نداند سازمان دقیقاً در چه وضعیتی قرار دارد و چه اقداماتی باید انجام دهد؛ موجی از سردرگمی، ناامیدی و شکست

۱- اولویت‌بندی بین بقا و رشد

در دل بحران‌های بزرگ، اولین پرسش هر مدیری در سازمان‌ها این است: «اکنون باید برای بقا بجنگیم یا برای رشد برنامه‌ریزی کنیم؟»

- در مرحله شوک و تهدید فوری (مانند حمله سایبری یا قطع اینترنت)، تمرکز اصلی باید بر حفظ عملیات حیاتی، جلوگیری از گسترش آسیب و تأمین نیازهای فوری مشتریان باشد.
- در بحران‌های بلندمدت (مانند رکود اقتصادی یا جنگ)، رویکردی ترکیبی ضرورت



نجات سازمان‌ها در بحران‌های شدید، وابسته به تصمیم‌های درست و به‌موقع مدیران است.



Critical Decisions Leaders Must Make for Business

برای نمونه، مقایسه کنید: در اجرای یک بانک‌های پاساگرد و سپه، حتی چند روز پس از اختلال، هیچ اطلاع‌رسانی شفافی وجود نداشت. در مقابل، صرافی رمزارز نوبیتکس از همان ساعات نخست حمله سایبری با اطلاعیه‌های روشن، به موقع و حمایت‌گرانه، اعتماد و آرامش کاربران خود را حفظ کرد. تصمیم‌گیری: یک طرح ارتباطات بحران داشته باشید تا همه بدانند در صورت بروز حادثه، چه کسی سخنگوی سازمان است، پیام‌ها از چه کانال‌هایی منتشر می‌شوند، چه اطلاعاتی باید در اختیار کارکنان و مشتریان قرار گیرد و گفتن چه اطلاعاتی ضروری نیست!

۴- تأمین امنیت سایبری و حفاظت از داده‌ها

در شرایطی مانند حمله هکری یا نشت اطلاعات، زمان برای تصمیم‌گیری بسیار محدود است. مدیر سازمان باید بدون تأخیر روی موارد زیر اقدام کند:

- فعال‌سازی تیم واکنش سریع امنیتی
- محدود یا مسدود کردن دسترسی‌های حیاتی
- اطلاع‌رسانی شفاف و فوری به کاربران یا مشتریان آسیب‌دیده
- همکاری مستقیم با مراجع قانونی و نهادهای مرتبط

در جنگ اخیر به همگان ثابت شد حملات سایبری خطرناک‌تر از آن چیزی هستند که

آن‌ها کار و برنامه‌ریزی شده، شاید در نگاه اول صرفه‌جویی به نظر برسند، اما تصمیماتی پایدار برای عبور از بحران‌های مالی موقت نیستند. و در طولانی‌مدت آسیب‌های جبران‌ناپذیری به سازمان وارد می‌کنند که مهم‌ترین آن، کاهش اعتماد و انگیزه در میان کارکنان است.

تصمیم‌گیری: یک نقشه مالی اضطراری داشته باشید که نشان دهد حتی در بدترین سناریو، سازمان چگونه می‌تواند به حیات خود ادامه دهد.

۳- ایجاد شفافیت و ارتباطات مؤثر

در دل بحران، شایعات و ابهام می‌توانند حتی مخرب‌تر از خود بحران عمل کنند. اگر کارمندان، مشتریان یا شرکا از واقعیت بی‌اطلاع بمانند، اعتماد به سازمان فرو می‌ریزد. بنابراین مدیر یک سازمان باید تصمیم بگیرد:

- چه اطلاعاتی، در چه زمانی و با چه سطحی از جزئیات به چه کسانی منتقل شود
- کانال‌های اصلی ارتباطی سازمان در بحران چه باشند (برای مثال، اگر اینترنت قطع است، از پیامک یا تماس تلفن استفاده شود)
- چگونه پیام‌ها هم‌امیدبخش و هم واقع‌گرایانه باشند

در روحیه کارمندان شکل خواهد گرفت. تصمیم‌گیری: پیش از هر اقدامی، تشخیص دهید سازمان در کدام مرحله از بحران قرار دارد و بر اساس آن، استراتژی‌های کوتاه‌مدت و بلندمدت را هم‌زمان طراحی کنید.

۲- مدیریت جریان نقدی و منابع مالی

بحران‌ها معمولاً با کاهش درآمد، افزایش هزینه‌های پیش‌بینی‌نشده یا ترکیبی از هر دو همراهند.

مدیران باید بدون تعارف و با شفافیت، وضعیت نقدینگی شرکت را بررسی کنند و سراغ تصمیمات حیاتی اما ضامن پایداری مالی شرکت بروند. برای نمونه:

- حذف یا تعلیق پروژه‌های غیرضروری
- مذاکره مجدد با تأمین‌کنندگان برای شرایط پرداخت بهتر
- یافتن منابع مالی جایگزین (وام اضطراری، جذب سرمایه‌گذار جدید)
- ایجاد ذخیره نقدی برای ماه‌های آینده

اما اقداماتی مانند تعدیل شتاب‌زده نیروها، به تأخیر انداختن پرداخت حقوق و مزایا، یا کنار گذاشتن پروژه‌هایی که ماه‌ها برای

در این زمان می‌تواند سال‌ها تلاش برای جلب اعتماد را نابود کند. مدیر باید تصمیم بگیرد:

- در مواجهه با مشتریان ناراضی یا آسیب‌دیده چه رویکردی داشته باشد
- چطور مسئولیت‌پذیری سازمان را نشان دهد
- چگونه با اقدامات مثبت (مانند کمک به جامعه) تصویر برند را تقویت کند
- تصمیم کلیدی: هر تصمیم باید اعتبار بلندمدت برند را حفظ کند، حتی اگر هزینه کوتاه‌مدت داشته باشد.

۱۰- آماده‌سازی سازمان برای بحران‌های آینده

هر بحران، فرصتی برای یادگیری است. رهبران موفق پس از عبور از بحران، فرایندها را مرور و نقاط ضعف را اصلاح می‌کنند:

- مستندسازی تجربه‌ها
- بازنگری در برنامه‌های پشتیبان و اضطراری
- آموزش تیم برای واکنش بهتر در بحران‌های بعدی

تصمیم کلیدی: تبدیل بحران به فرصتی برای یادگیری سازمانی.

نتیجه‌گیری

تصمیم‌گیری در بحران مانند حرکت روی طناب باریک است؛ هر گام باید سنجیده، سریع و منعطف باشد. مدیران موفق باید هم تصویر بزرگ را ببینند و هم به جزئیات حیاتی توجه کنند. ترکیب سه عنصر کلیدی: عقلانیت (تصمیم‌گیری مبتنی بر داده‌ها)، انسانیت (حمایت از کارکنان و مشتریان) و جسارت (حرکت به سمت راهکارهای جدید) همان چیزی است که می‌تواند سازمان را نه تنها از بحران عبور دهد، بلکه قوی‌تر از قبل سازد.

فرصت‌های تازه‌ای برای رشد یا نوآوری هم به همراه دارند. ممکن است مردم یا دولت به محصولات بیشتری نیاز پیدا کنند؛ یا مواد اولیه کمیاب شود و سازمان ناچار باشد برای تامین یا جایگزینی آن‌ها، راه‌حل‌های خلاقانه بیابد. تصمیم کلیدی: ایجاد انعطاف‌پذیری در زنجیره تامین و مدل کسب‌وکار، به گونه‌ای که بقا و رشد سازمان، تنها به یک مسیر، وابسته نباشد.

۷- استفاده از داده و سناریوسازی

در شرایط غیرقابل پیش‌بینی، تصمیم‌گیری نباید صرفاً بر پایه حدس و احساس انجام شود. مدیر کسب‌وکار باید:

- داده‌های موجود را جمع‌آوری و تحلیل کند (مانند آمار فروش، رفتار مشتریان، میزان هزینه‌ها)
- چند سناریوی متفاوت طراحی کند (بدبینانه، محتاطانه، خوش‌بینانه)
- برای هر سناریو، مجموعه‌ای از اقدامات مشخص و عملی در نظر بگیرد

تصمیم کلیدی: تکیه بر تصمیم‌گیری مبتنی بر شواهد و داده‌ها، به جای واکنش‌های احساسی یا شتاب‌زده.

۸- سرعت در تصمیم‌گیری، همراه با انعطاف

یکی از خطرات رایج در بحران‌ها، تعلل بیش از حد است. تأخیر می‌تواند فرصت‌ها را از بین ببرد و خسارت را افزایش دهد. از سوی دیگر، تصمیمات عجولانه بدون اطلاعات کافی نیز پرخطر هستند. مدیر موفق در بحران کسی است که:

- در کمترین زمان ممکن اطلاعات کافی را جمع‌آوری کند
- تصمیم بگیرد و آن را اجرا کند
- در صورت تغییر شرایط، آماده اصلاح تصمیم باشد

برخی از مدیران از ترس تصمیم غلط، ترجیح می‌دهند هیچ تصمیمی نگیرند؛ در حالی که تأخیر در تصمیم‌گیری خود می‌تواند بدترین تصمیم باشد. تصمیم کلیدی: پیدا کردن تعادل بین سرعت و دقت.

۹- حفظ اعتبار و اعتماد برند

بحران‌ها زمان‌هایی هستند که برند شما زیر ذره‌بین مردم قرار می‌گیرد. یک تصمیم اشتباه

تصور می‌شود و می‌تواند ویرانگر و مخرب برای کل کسب‌وکار باشند. اهمیت زیادی دارد که سازمان‌ها از پیش برای چنین شرایطی آماده باشند، از پشتیبان‌گیری و افزونگی سیستم‌ها گرفته تا شبیه‌سازی سناریوهای حمله. اما در لحظه بحران، آنچه حیاتی است تصمیم سریع برای بازگرداندن سرویس‌ها یا بازایی اطلاعات از دست رفته است.

تصمیم کلیدی: داشتن یک پروتکل پاسخ به حادثه سایبری و تمرین منظم آن، تا در لحظه بحران هیچ زمانی هدر نرود و واکنش سازمان دقیق، سریع و هماهنگ باشد.

۵- حفظ و تقویت روحیه تیم

بحران‌هایی مانند جنگ یا رکود شدید، فشار روانی سنگینی بر کارکنان تحمیل می‌کنند. اگر به انگیزه و امنیت روانی آن‌ها توجه نشود، می‌تواند باعث ریزش نیروی کلیدی و فروپاشی ساختار سازمان شود. مدیر سازمان باید آگاهانه تصمیم بگیرد که:

- چطور به کارکنان اطمینان دهد که سازمان در کنار آن‌هاست و برای حمایت از آن‌ها تلاش می‌کند
- چه تغییراتی در ساعات کاری یا روش کار (مانند دورکاری) ضروری است
- چه اقدامات حمایتی (از مشاوره روان‌شناسی تا حمایت مالی) امکان‌پذیر است
- در صورت تعطیلی دفتر کار یا اختلال در اینترنت و موبایل، ارتباطات کاری چگونه ادامه پیدا کنند
- تصمیم کلیدی: انتخاب رویکردی انسان‌محور حتی در اوج فشار کاری، تا کارکنان بدانند در سخت‌ترین لحظه‌ها تنها نیستند.

۶- تنوع بخشی به زنجیره تامین و مدل درآمدی

در بحران‌هایی مانند کمبود مواد اولیه یا قطع واردات، وابستگی به یک تأمین‌کننده یا یک بازار می‌تواند برای سازمان مرگ‌آور باشد. بنابراین مدیران باید تصمیم بگیرند که:

- تأمین‌کنندگان جایگزین پیدا کنند (حتی اگر هزینه بیشتری داشته باشند)
- مدل کسب‌وکار متناسب با شرایط تغییر کند (برای نمونه، فروش آنلاین در صورت بسته بودن فروشگاه‌ها)
- محصولات یا خدمات جدیدی معرفی کنند که نیاز فوری بازار را پوشش دهند

بسیاری از بحران‌ها، علاوه بر تهدید،



در دل بحران، مدیران باید میان بقا و رشد تعادل برقرار کرده، با تصمیم‌های سریع، داده‌محور و انسان‌محور سازمان را هدایت کنند.

ترکیب عقلانیت، شفافیت و حمایت از کارکنان و مشتریان، کلید عبور از بحران و تقویت برند است.

استاندارد زیر ساخت مراکز داده TIA 942 (Data Center) (بخش نهم)

منبع: TIA Standard / TIA942

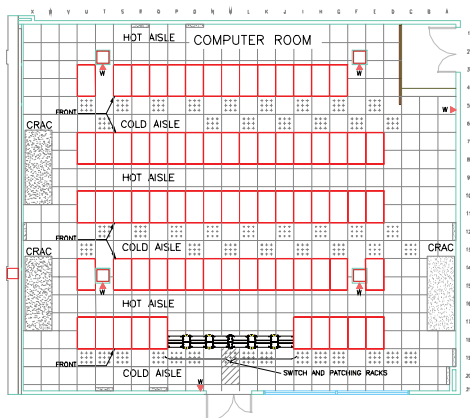


مترجم: فرزانه شوقی لیسار

ضمیمه (ح) کتاب در این
شماره تقدیم شما می شود

ح: مثال طراحی یک مرکز داده کوچک

یک طرح نمونه برای یک مرکز داده کوچک در زیر نشان داده شده است. این نمونه از مرکز داده، به اندازه‌ای کوچک است که می‌توان آن را با MDA و بدون نیاز به HDA، پشتیبانی کرد.

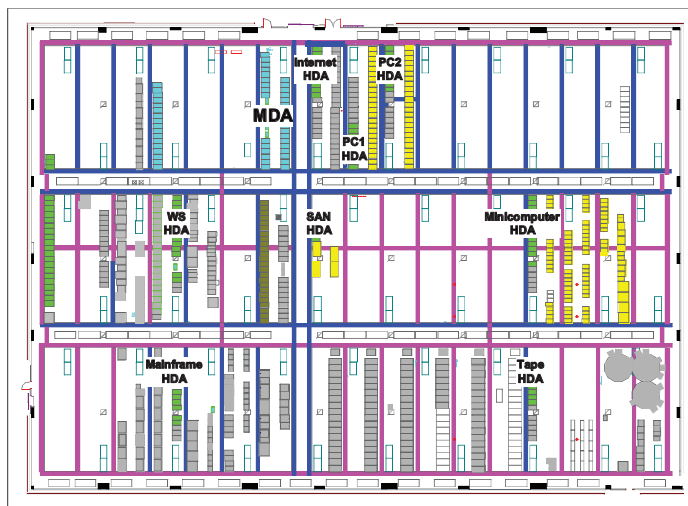


ضمائم

ضمیمه (ح): مثال‌هایی برای طراحی مرکز داده

این ضمیمه تنها جنبه آموزشی دارد و بخشی از این استاندارد نیست

کاذب در درون سینی‌های کابل سبکی شکل جا داده شده‌اند. در بعضی جاها که حجم کابل‌ها زیاد است و برای این‌که مانع جریان هوا نشوند، سینی‌های کابل به صورت دو طبقه نصب می‌شود. شکل زیر اتاق کامپیوتر طبقه دوم را همراه با سینی‌های کابل نشان می‌دهد.



شکل (ضمیمه ۲۱) نمونه مرکز داده شرکت

کابل‌کشی دیتا و مخابرات در راهروهای «گرم» پشت رک‌های سرور انجام شده است. کابل‌کشی الکتریکی در راهروهای «سرد» در جلوی رک‌های سرور کشیده شده است. هر دو نوع کابل‌کشی برق و دیتا، راهروهای اصلی در جهت شرقی غربی را دنبال می‌کنند اما برای حفظ فواصل لازم بین این دو نوع کابل، از مسیرهای مستقلی انجام خواهند شد.

مکان قرارگیری اتاق ورودی در طبقه اول و MDA در طبقه دوم به دقت انتخاب شده است. به طوری که مدارات T1 و T3 می‌توانند در هر جایی از اتاق کامپیوتر روی تجهیزات مربوطه سربندی شوند. رک‌های سرورهای rackmount، کابل‌کشی استاندارد شامل فیبر Multimode و کابل 6Cat دارند. اگر این استانداردها را انجام شود، مدیریت آن‌ها قدری ساده‌تر خواهد بود.

در این مرکز داده به دلیل این تنوع گسترده انواع کابل‌کشی برای رک‌های ایستاده، امکان پیاده‌سازی یک پیکربندی استاندارد برای پریزهای منطقه‌ای یا zone outlet وجود ندارد.

ح ۳: مثال طراحی یک مرکز داده اینترنت

در این مثال، مرکز داده اینترنت دارای یک طبقه تقریباً ۹۵۰۰ متر مربعی به همراه یک اتاق کامپیوتر در حدود ۶۴۰۰ متر مربع است این نمونه‌ای از یک مرکز داده است که در آن، HDAها به جای این که بر اساس نوع سیستم‌هایی که نگهداری می‌کنند متمایز شوند، بر اساس نواحی تحت پوششان تفکیک می‌شوند. شکل زیر، نقشه چیدمان مرکز داده را همراه با سینی‌های کابل نشان می‌دهد. رک‌های MDA و HDA نشان داده شده‌اند ولی رک‌های مشتری در شکل نمایان نیستند.

شکل (ضمیمه ۲۰) نقشه اتاق کامپیوتر با نمایش راهروهای گرم و سرد

این اتاق کامپیوتر، فضایی در حدود ۱۸۰ متر مربع و ۷۳ رک سرور در EDAها و شش رک نیز در MDA دارد. شش رک MDA، شش رکی هستند که با عنوان SWITCH AND PATCHING RACKS در پایین شکل نشان داده شده‌اند.

الزامی برای قراردادن MDA در مرکز اتاق کامپیوتر وجود نداشت، چون در اینجا محدودیت مسافت مطرح نیست. در هر حال، با قراردادن MDA در مرکز اتاق می‌توان طول و حجم کابل راهروهای عمود بر راهروهای رک را کاهش داد.

MDA برای کابل‌کشی افقی به EDA از HC استفاده می‌کند. در یک مرکز داده که حجم بالایی کابل‌کشی به رک تجهیزات دارد، ممکن است لازم باشد که برای کاهش ازدحام کابل‌های نزدیک MDA، از HDA استفاده شود.

ردیف‌های رک با جهت جریان هوای زیر کف که به وسیله واحدهای تهویه مطبوع اتاق کامپیوتر (CRAC) ایجاد می‌شود، همسو هستند. هر CRAC روبروی راهروهای «گرم» قرار گرفته است تا اجازه دهد که هوای موثرتری به هر واحد CRAC برگردد.

تشکیل راهروهای «گرم» و «سرد» به صورت یکی در میان، به سبب نحوه چیدمان رک‌های سرور ایجاد شده است.

کابل‌های دیتا در راهروهای «گرم» درون سینی‌های کابل سبکی شکل و کابل‌های برق نیز، در زیر کف کاذب در راهروهای «سرد» قرار می‌گیرند.

برای کنترل دسترسی و آلودگی اتاق کامپیوتر از NOC (NOC) در شکل نمایان نیست (جدا است).

ح ۲: مثال طراحی یک مرکز داده شرکتی

مثال زیر برای یک مرکز داده میزبان وب یا اینترنت است که کامپیوتر و تجهیزات ارتباطی مربوط به وب سایت چندین شرکت را در خود جای داده است.

مرکز داده شرکتی در این مثال، دو طبقه دارد که هر کدام تقریباً ۴۱۴۰ متر مربع هستند. این مرکز داده، نمونه‌ای از مرکز داده با چندین HDA است که هر کدام بر اساس نوع سیستم‌هایی که نگهداری می‌کند از دیگری متمایز می‌شود. به خاطر حجم کابل‌کشی‌های انجام شده برای PCهای سرور، این سیستم‌ها توسط دو HDA سرویس داده می‌شوند و هر ناحیه فقط ۲۴ رک سرور را پشتیبانی می‌کند هفت HDA اضافه برای نگهداری رکهای سرور اضافه طراحی شده است بنابراین HDA فقط برای تفکیک نواحی بر اساس نوع عملیات آنها استفاده نمی‌شود بلکه از دحام کابل در هر HDA را نیز کاهش می‌دهد. هر HDA برای نگهداری حداکثر ۲۰۰۰ کابل CAT6 طراحی شده است.

اولین طبقه شامل اتاق‌های الکتریکی، مکانیکی، انبارها، جایگاه بارگیری، اتاق حراست، دفتر پذیرش، مرکز عملیات (NOC) و اتاق ورودی است.

اتاق کامپیوتر در طبقه دوم قرار دارد و به طور کامل با کف کاذب پوشیده شده است. همه کابل‌کشی‌های دیتا و مخابرات در زیر کف

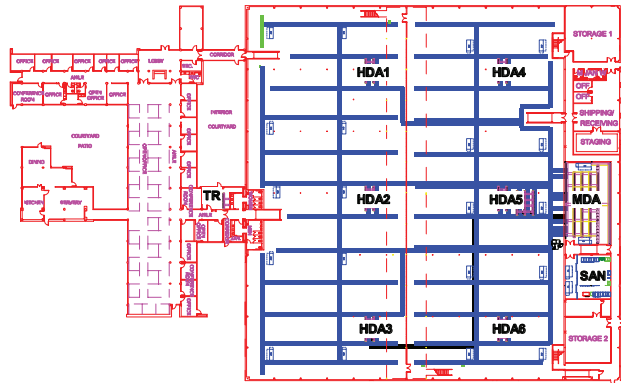
ضمیمه «ط»:

نام کتب و مراجع

این ضمیمه جنبه آموزشی داشته و بخشی از این استاندارد نیست.

این ضمیمه حاوی اطلاعات مربوط به استادی است که با این استاندارد مربوط هستند یا در متن استاندارد به آن‌ها اشاره شده است. بسیاری از این اسناد در حال چاپ هستند و به وسیله سازمان‌های استاندارد بین‌المللی یا ملی پشتیبانی و توزیع می‌شوند. این اسناد را می‌توان از طریق تماس با مرکز مؤسسات استاندارد یا نمایندگان منتصب آن‌ها بدست آورد. قانون الکتریکی کاربردی در ایالات متحده آمریکا NEC است.

- ANSI/IEEE C21997, National Electrical Safety Code
- ANSI/NFPA702002, National Electrical Code
- ANSI/NFPA752003, Standard for the protection of information technology equipment
- ANSI T1.336, Engineering requirements for a universal telecommunications frame
- ANSI/TIA/EIA568B.12001, Commercial Building Telecommunications Cabling Standard
- ANSI/TIA/EIA568B.12001, Commercial Building Telecommunications Cabling Standard Part 2: Balanced TwistedPair Cabling Components
- ANSI/TIA/EIA568B.32000, Optical Fiber Cabling Components
- ANSI/TIA569A1993, Commercial Building Standard for Telecommunications Pathways and Spaces.
- ANSI/TIA/EIA606A2002, Administration Standard for the Telecommunication Infrastructure of Commercial Buildings
- ANSI/TIA/EIAJSTD6072001, Commercial Building Grounding (Earthing) and Bonding Requirments for Telecommunications
- ANSI/TIA7581999. Customerowned Outside Plant Telecommunications Cabling Standard
- ASHREA, Thermal Guideline for Data Processing Environments
- ASTM B53990, Measuring Contact Resistance of Electrical Connections (Static Contacts)
- BICSI Telecommunications Distribution Methods Manual
- BICSI Cabling Installation Manual
- BICSI Customerowned Outside Plant Methods Manual
- BOMA Building Owners Management Association, International Codes & Issues, July2000



شکل (ضمیمه ۲۲) نمونه مرکز داده اینترنت

عملیات اتاق ورودی و crossconnect اصلی با هم ادغام شده و در MDA انجام می‌شود. این ناحیه ۵۰ رک سرویس‌دهنده مخابراتی و ۲۰ رک مربوط به فضای crossconnect اصلی را در خود جای می‌دهد. این اتاق توسط دو PDU اختصاصی، دو واحد تهویه مطبوع اختصاصی اتاق کامپیوتر، پشتیبانی می‌شود و روی کف کاذب قرار دارد. MDA در یک اتاق اختصاصی با یک ورودی مجزا قرار گرفته است که به سرویس‌دهندگان مخابراتی اجازه می‌دهد که بدون نیاز به ورود به قسمت مربوط به مشتریان در اتاق کامپیوتر، اصلی کار خود را در این اتاق انجام دهند.

مکان قرارگیری MDA و HDAها طوری طراحی شده است که طول مدارات T1 و T3 به هر رک در اتاق کامپیوتر که وصل شود، از حد مجاز بیشتر نشود.

Tape libraryهای خودکار سرورهای ذخیره سازی و تجهیزات کنترلی مربوط به سرویس‌های ذخیره، در یک اتاق SAN اختصاصی در مجاورت MDA قرار دارند. این تجهیزات به وسیله مالک مرکز داده تهیه و مدیریت نمی‌شوند، بلکه گروه سومی (غیر از مالک مرکز داده و تولیدکننده تجهیزات) آن را انجام می‌دهند. این فضای مستقل، به گروه متخصصین ذخیره‌سازی این امکان را می‌دهد که بدون نیاز به ورود به اتاق کامپیوتر اصلی، تجهیزاتشان را مدیریت کنند. اتاق کامپیوتر حاوی ۴۳۰۰ رک مشتری است. فضای مربوط به مشتریان توسط شش HDA پشتیبانی می‌شود تا حجم کابلی که در سینی‌های کابل زیر کف قرار می‌گیرد کمتر شود. هر HDA تقریباً ظرفیت مناسب برای ۲۰۰۰ اتصال زوج سیم دارد. این HDAها در مرکز این فضا قرار می‌گیرند تا طول کابل‌ها کاهش یابد. کابل‌کشی از HDAها به رک‌های مشتری استاندارد است تا مدیریت ساده‌تر شود. در هر حال، ممکن است در صورت نیاز کابل‌کشی اضافه به رک‌های مشتری انجام شود.

کابل‌کشی دیتا و مخابرات به نواحی ذخیره‌سازی و اتاق مونتاز در قسمت شرقی اتاق کامپیوتر، از MDA و به دفاتر غربی اتاق کامپیوتر نیز از اتاق مخابرات (TR) انجام می‌شود.

- CABAContinental Automated Buildings Association,
- Federal Communications Commision (FCC) Washington D.C., «The Code of Federal Regulations, FCC 47 CFR 68»
- Federal Telecommunications Recommendation 10901997, Commercial Building Telecommunications Cabling Standard, by National Communications System (NCS)
- IBC, International Building Code
- ICC, International Code Council
- IEEE Std. 142, Recommended Practice for Grounding of Industrial and Commercial Power Systems
- IEEE Std. 446, Recommended Practice for Eemergency and Standby Power System for Industrial and Commercial Applications
- IEEE Std. 1100, Recommended Practice for Powering and Grounding Electronic Equipment
- IEEE 802.32002 (also known as ANSI/IEEE Std. 802.32002 or ISO 88023: 2002 (E), Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifictions
- IEEE 802.41990, Standard for Local Area Network Token Passing Bus Access Method, Physical Layer Specification,
- IEEE 802.51998, Token Ring Access Method and Physical Layer Specifications IEEE 802.71989 (R1997) IEEE Recommended Practices for Broadband Local Area Networks (ANSI)
- IEEE Standard 5181982, Guide for the installation of electrical equipment to minimize electrical noise to controllers of external sources
- IFMA International Facility Management Association Ergonomics for Facility Managers, June 2000
- NFPA 72, National Fire Alarm Code, 1999
- NFPA 2001, Standard on clean agent fire extinguishing systems, 2000 Edition
- NEC, National Eelectrical Code, article 725, Class 1, Class 2 and Class 3 Remote Control, Signaling and PowerLimited Circuits
- NEC, National Eelectrical Code, article 760, Fire Alarm System.
- NEMA VE 22001, cable tray installation guidelines
- Society of Cable Television Engineers, Inc., Document #IPSP001, Flecible RF Coaxial Drop Cable Specification
- TIA/EIA TSB31B, FCC 47 CFR 68, Rationale and Measurement Guidelines
- ANSI/TIA/EIA485A1998, Electrical Characteristics of Generators and Receivers for USE in Balanced Digital Multipoint Systems
- TIA/EIATSB891998, Application Guidelines for TIA/

EIA 485 A

- UL 444/CSAC22.2 No. 21494, Communications Cables
- The Uptime Institute White Paper, Alternating Cold and Hot Aisles Provides More Reliable Cooling for Server Farms
- The Uptime Institute White Paper, Industry Standard Tier Classifications Define Site Infrastructure Performance
- The Uptime Institute White Paper, Fault Tolerant Power Compliance Specification

برای کسب اطلاعات مرجع می‌توانید با سازمان‌های زیر تماس حاصل کنید.

• ANSI

- » American National Standards Institute
- » 11 W 42 St.
- » New York, NY 10032
- » USA
- » (212) 6424900
- » www.ansi.org

• ASHRAE

- » American Society of Heating, Refrigeration and Air conditioning Engineers
- » 1791 Tullie Circle, NE
- » Atlanta, GA 30329
- » 18005274723
- » (400) 6368400
- » www.ashrac.org

• ASTM

- » American Society for Testing and Materials (ASTM)
- » 100 Barr Harbor Drive
- » West Conshohocken, PA 194282959
- » USA
- » (610) 8329500
- » www.astm.org

• BICSI

- » Building Industry Consulting Service International (BICSI)
- » 8610 Hidden River Parkway
- » Tampa, FL 336371000
- » USA
- » (800) 2427405
- » www.bicsi.org

• CSA

- » Canadian Standards Association International (CSA)
- » 178 Rexdale Blvd.

- » Etobicoke, (Toronto), Ontario
- » Canada M9W 1R3
- » (416) 7474000
- » **www.csainternational.org**

• EIA

- » Electrical Industries Alliance (EIA)
- » 2500 Wilson Blvd., Suite 400 Arlington, VA 222013836
- » USA
- » (703) 9077500
- » **www.cia.org**

• FCC

- » Federal Communications Commission (FCC)
- » Washington, D.C. 20554
- » USA
- » (301) 7251585
- » **www.fcc.org**

• Federal and Military Specifications

- » National Communications System (NCS)
- » Technology and Standards Division
- » 701 South Court House Road Arlington, VA 222042198
- » USA
- » (703) 6076200
- » **www.ncs.gov**

• International Code Council (ICC)

• International Building Code (IBC)

- » 5203 Leesburg Pike, Suite 600
- » Falls Church, VA 22041
- » 7039314533
- » **www.iccsafe.org**

• IEC

- » International Electrotechnical Commission (IEC)
- » Sales Department
- » PO Box 131
- » 3 rue de Varembe
- » 1211 Geneva 20
- » Switzerland
- » +41 22 919 02 11
- » **www.iec.ch**

• IEEE

- » The Institute of Electrical and Electronic Engineers, Inc (IEEE)
- » IEEE Service Center
- » 445 Hoes Ln., PO Box 1331
- » Piscataway, NJ 08855 1331
- » USA
- » (732) 9810060
- » **www.ieee.org**

• IPC

- » The Institute for Interconnecting and Packaging Electronic Circuits
- » 2215 Sanders Rd.
- » NorthBROOK, IL 600626135
- » USA
- » (847) 5099700
- » **www.ipc.org**

• ISO

- » International Organization for Standardization (ISO)
- » 1, Rue de Varembe
- » Case Postale 56
- » CH1211 Geneva 20
- » Switzerland
- » +41 22 74 901 11
- » **www.iso.ch**

• NEMA

- » National Electrical Manufacturers Association (NEMA) 1300 N.
- » 17th Street, Suit 1847
- » Rosslyn, VA 22209
- » USA
- » (703) 8413200
- » **www.nema.org**

• NFPA

- » National Fire Protection Association (NFPA)
- » Batterymarch Park
- » Quincy, MA 022699101
- » USA
- » (617) 7703000
- » **www.nfpa.org**

• SCTE

- » Society of Cable Telecommunications Engineers (SCTE)
- » 140 Philips Rd.
- » Exton, PA 193411318

- » USA
- » (800) 5425040
- » **www.scte.org**

- **Telcorida Technologies (Formerly: Bellcore)**
- **Telcorida Technologies Customer Service**

- » 8 Corporate Place Room 3C 183
- » Piscataway, NJ 088544157
- » USA
- » (800) 5212673
- » **www.telcorida.com**

- **The Uptime Institute, Inc.**

- » 1347 Tano Ridge Road
- » Santa Fe, NM 87506
- » USA
- » (505) 9863900
- » **www.upsite.com**

- **TIA**

- » Telecommunication Industry Association (TIA)
- » 2500 Wilson Blvd., Suite 300
- » Arlington, VA 222013836
- » USA
- » (703) 9077700
- » **www.tiaonline.org**

- **UL**

- » Underwriters Laboratories, Inc. (UL)
- » 333 Pfingsten Road
- » Northbrook, IL 600622096
- » USA
- » (847) 2728800
- » **www.ul.com**



Fiber Optic - MPO Data Center Solution

**سرعتی فضایی
در مسیر ویژه!!**

-بالا رفتن سرعت انتقال
-بالا رفتن سرعت نصب
-کم شدن حجم کابل کشی

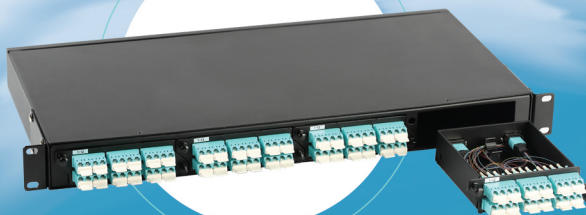
10G 40G

real-high-speed

Fiber Optic MPO



F.O. MPO Cassette



F.O. Patch Panel



F.O. MPO Trunk



تلفن گویا: ۹۱۰۷۲۲۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
اپراتور: ۰۰ ۶۶۹۴۷۲۰۰
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

چگونه از سرورهای خود در برابر حملات جنگی محافظت کنیم؟

ترفندهایی برای افزایش امنیت فیزیکی سرورهای مدرن امروزی و وظایف کاربران

منبع: hexatronicdatacenter.com

✍ مترجم: بهرام غلامی



اشاره

جنگ ۱۲ روزه اخیر ایران، تصورات بسیاری از ما درباره تهدیدات سایبری و فیزیکی و آسیب‌های ناشی از حملات جنگی را تغییر داد. دیدیم که عملاً ممکن است یک روز صبح از خواب بیدار شویم و بفهمیم برق شهر بر اثر حمله سایبری یا اصابت موشک و پهپاد، قطع شده است؛ اینترنت نداریم و دفتر محل کارمان در یک ساختمان معروف و مستحکم شهر، به تلی از خاکستر تبدیل شده است. اکنون، چه باید کرد؟ چگونه به اطلاعات ذخیره شده روی سرورهای سوخته و نابود شده، دسترسی پیدا کنیم؟ چگونه دیتاهای حیاتی مردم را بازیابی و سرویس‌های گذشته را زنده کنیم؟ آیا در این شرایط که نه اینترنت عادی در دسترس است و نه امکان حضور فیزیکی در محل وجود دارد و شاید برق هم نداشته باشیم؛ کاری می‌شود کرد یا همه چیز از بین رفته و باید ماه‌ها قبل و سال‌های قبل، پیش‌بینی چنین روزی را می‌کردیم؟

در این مقاله، به راهکارهایی برای محافظت از سرورهای مدرن امروزی در برابر تهدیدهای جنگی اشاره می‌کنیم و اشاره‌ای هم به نقش کاربران در حفاظت از اطلاعات حیاتی‌شان خواهیم داشت:

مقاله فنی

استفاده از قفس‌های فارادی برای افزایش مقاومت سرورها و مراکز داده

یا ذخیره‌سازی (مانند هارد دیسک‌های پشتیبان)، در آن قرار می‌گیرند. این محفظه آن قدر محکم و مقاوم است که به هیچ وجه اجازه‌ی وارد شدن آسیبی به سرور و سایر تجهیزات را نمی‌دهد؛ نه قابل آتش‌سوزی و اشتعال است؛ و نه به راحتی بر اثر فشار یا ضربه، دچار شکستگی یا خم‌شدگی می‌شود. قفس فارادی میدان‌های الکترومغناطیسی خارجی را دفع یا خنثی می‌کند و همانند یک سپر از نفوذ امواج رادیویی، الکترومغناطیسی و حتی پالس‌های الکترومغناطیسی (EMP) که در حملات جنگی یا انفجارهای اتمی ایجاد

در دنیای امروز، برای حفاظت از سرورهای مهم و حیاتی نظامی و بانکی یا تجهیزات مخابراتی در جنگ‌ها و تهدیدات فیزیکی مانند انفجار، آتش‌سوزی، اصابت موشک، ریزش ساختمان و حتی بمب‌های الکترومغناطیسی (Electromagnetic Pulse - EMP) از راهکاری به نام قفس فارادی (Faraday Cage) استفاده می‌شود. قفس فارادی یک محفظه فلزی ویژه است که سرورها و تجهیزات شبکه

جنگ اخیر نشان داد که زیرساخت‌های دیجیتال چقدر در برابر حملات فیزیکی و سایبری آسیب‌پذیرند. این مقاله راهکارهایی برای محافظت از سرورها و بازیابی اطلاعات در شرایط بحرانی ارائه می‌دهد، همراه با توصیه‌هایی برای آمادگی کاربران.

The Physical Security of Your Data Center: How to Keep Everything Safe



مسلح و ضخیم (گاهی تا ۱ متر) برای مقاومت در برابر موج انفجار و اصابت‌های غیرمستقیم استفاده می‌شود.

سرورهای توزیع شده و راهکاری ابری برای محافظت از داده‌ها

هرچقدر هم که برای مقاومت‌سازی رک‌ها و سرورهای خود در دفترکارتان اقدام کنید؛ باز هم خطر آسیب و از بین رفتن آن‌ها در



برای محافظت از سرورها در برابر تهدیدهای فیزیکی و الکترومغناطیسی، از قفس فارادی استفاده می‌شود؛ محفظه‌ای فلزی که امواج و فشارهای مخرب را دفع می‌کند. این قفس‌ها به صورت رک یا اتاقک‌های عایق‌شده ساخته می‌شوند و تاب‌آوری مراکز داده را افزایش می‌دهند. همچنین، قرار دادن دیتاسنترها در پناهگاه‌های زیرزمینی یا دل کوه‌ها، راهکاری موثر برای مقابله با حملات فیزیکی و بمب‌های EMP است.

فلزی استفاده می‌شود تا این اطمینان حاصل شود که هیچ آسیبی به سرورها نخواهد شد.

دیتاسنترهای زیرزمینی و دور از مناطق شهری و حساس

احتمالاً تصاویری از دیتاسنترهای شرکت‌های بزرگ فناوری دیده‌اید که در دل کوه‌ها، چند ده متر زیرزمین، یا در صحراها و مناطق روستایی دور از شهرها ساخته شده‌اند و این سوال برایتان پیش آمده که چرا باید سرورها در چنین مکان‌هایی، نگهداری شوند؟

فارغ از مباحث مربوط به انرژی، سیستم سرمایشی، یا هزینه‌های احداث، یکی از روش‌های رایج برای محافظت از دیتاسنترها و سرورها در برابر حملات فیزیکی، قرار دادن آن‌ها در پناهگاه‌های زیرزمینی یا در دل کوه‌ها و محیط‌هایی است که به راحتی در دسترس خرابکاری، نفوذ، انفجار یا بمب‌های الکترومغناطیسی نباشند.

ساخت دیتاسنترها در زیرزمین (BunkerStyle Data Center) برای محافظت در برابر انفجار، امواج ضربه‌ای، پرتاب ترکش و تشعشعات، در بسیاری از کشورها رایج است. در این نوع ساخت و ساز، گاه از دیوارهای بتنی

می‌شوند؛ جلوگیری می‌کند.

استفاده از قفس فارادی برای سرورها و تجهیزات شبکه باعث افزایش تاب‌آوری (resilience) مراکز داده در زمان بحران و ایمن‌سازی وسایل حساس در برابر حملات هدفمند رادیویی و الکترونیکی می‌شود.

پیاده‌سازی قفس فارادی در مراکز داده

برای محافظت از سرورها و تجهیزات شبکه در مراکز حیاتی، قفس فارادی به چندین شیوه ساخته و پیاده‌سازی می‌شود. در روش نخست، مجموعه‌ای از اتاقک‌ها یا رک‌های فلزی که به زمین متصل هستند، ساخته شده و تجهیزات شبکه درون آن‌ها قرار می‌گیرند. در روش دیگر، که برای محافظت از تعداد محدودی سرور و تجهیزات ذخیره‌سازی به کار می‌رود؛ رک‌های سروری با درب و جداره‌های فلزی بسیار مقاوم، ضد ضربه و فشار، و مقاوم در برابر بمب‌های الکترومغناطیسی و با رعایت کامل عایق‌بندی‌ها ساخته می‌شوند. در این رک‌ها، از فیلترهای ویژه‌ای برای ورودی کابل‌ها و تجهیزات شبکه استفاده می‌شود. در برخی پیاده‌سازی‌ها، از چندین لایه رسانای

Drills) و آموزش مستمر تیم‌ها برای بازیابی سریع و ایمن خدمات، نباید فراموش شود. در نهایت، استفاده از برنامه‌های حرفه‌ای در حوزه Continuity Planning باید به عنوان یکی از ارکان اصلی مدیریت ریسک و تداوم کسب و کار در دستور کار قرار گیرد.

داده‌های نهادهای امنیتی استفاده می‌شود، چراکه این اطلاعات نیازمند محافظت بالا و دسترسی محدود هستند و نباید به راحتی در معرض خطرات سایبری یا فیزیکی قرار گیرند.

وظیفه کاربران برای محافظت از داده‌های حیاتی‌شان چیست؟

این تصور که با بستن یک قرارداد یا خرید یک هاست و سرور از یک شرکت، دیگر هیچ مسئولیتی در قبال محافظت از دارایی‌های دیجیتال و داده‌های حیاتی‌مان حتی در زمان جنگ‌ها و حملات سایبری نداریم؛ کاملاً اشتباه است.

کاربران، مدیران کسب‌وکارها و افرادی که سرویس‌های مهم و اطلاعات حساس دارند؛ باید همیشه یک نسخه از داده‌های خود را به صورت رمزنگاری شده روی هارددیسک‌های قابل حمل یا در سرویس‌های ابری نگهداری کنند و این احتمال را در نظر بگیرند که روزی ممکن است هیچ اثری از دیتاست‌های شرکت سرویس‌دهنده‌شان روی زمین باقی نماند. مدیران هوشمند، نه تنها به صورت هفتگی از اطلاعات سازمانی خود نسخه پشتیبان روی سرویس‌های کلاود خارج از شرکت تهیه می‌کنند؛ بلکه یک نسخه آفلاین را نیز همیشه در خانه نگه می‌دارند. این افراد معمولاً اقدام به خرید هارددیسک‌های ضد ضربه، ضد حریق، و مقاوم در برابر رطوبت می‌کنند، یا از محفظه‌ها و کیف‌های فلزی مخصوص استفاده می‌کنند تا هارددیسک‌ها را در شرایطی کاملاً ایمن نگهداری کنند.

نتیجه‌گیری

اگر می‌خواهید سرویس‌های شما از هرگونه حمله فیزیکی در امان بمانند؛ لازم است علاوه بر رعایت نکات فنی مانند سازه‌های مقاوم، پشتیبان‌گیری آنلاین و آفلاین، سرویس‌های توزیع شده و مسیرهای چندگانه (Multipath) ارتباطی (مانند فیبر نوری، ارتباطات موبایلی و ماهواره‌ای)، تا حد امکان ساختمان‌های شما فاقد نشان‌های مشخص و غیرقابل شناسایی برای هدف‌گیری باشند. در زمان احداث یک دیتاستر، باید سعی شود که موقعیت آن دور از اهداف استراتژیک نظامی و مناطق شهری انتخاب شود و سیستم‌های افزونگی برق و زیرساخت اینترنت به طور کامل در طراحی آن لحاظ شود. همچنین، اجرای منظم سناریوهای تست بحران (Disaster Recovery)

شرایطی مانند جنگ‌ها وجود دارد. حتی اگر خود سرورها آسیب نبینند؛ ممکن است اینترنت و برق ساختمان قطع شود و هیچ راهی برای دسترسی به سرورها و روشن کردن آن‌ها وجود نداشته باشد. بنابراین، در دنیای امروز از راهکارهای ابری و سرویس‌های توزیع شده استفاده می‌شود. در این روش‌ها، تمام داده‌های حیاتی در چندین مرکز داده یا سرور در نقاط مختلف جغرافیایی، پشتیبان‌گیری و نگهداری می‌شوند تا در صورت از بین رفتن سرور شماره ۱ یا ۲، سرور شماره ۳ از راه دور همچنان در دسترس باشد. شرکت‌های بزرگ فناوری از راهکارهای مبتنی بر سرورهای ابری (Cloud Servers) با زیرساخت توزیع شده در کشورهای مختلف بهره می‌برند تا اگر زیرساخت یک کشور از بین رفت؛ همچنان بتوان به داده‌ها و سرویس‌ها دسترسی داشت.

طراحی ماژولار سرورها برای افزایش سرعت تعویض قطعات آسیب دیده در مراکز داده یا اتاق‌های سروری که اهمیت بالایی دارند؛ از طراحی‌های ماژولار (Modular Design) استفاده می‌شود تا در صورت آسیب دیدن یک بخش از سرور، بخش‌های دیگر همچنان فعال باقی بمانند و به کار خود ادامه دهند و بتوان تنها بخش آسیب‌دیده را به سرعت تعویض کرد. طراحی ماژولار اجازه می‌دهد تعمیر و بازسازی سریع قطعات در مراکز داده‌های بحرانی انجام شود و از قطع کامل سرویس جلوگیری شود. برای مثال، وقتی یک حمله سایبری به سرورها شده و خرابی‌های فیزیکی رخ داده است؛ تیم فنی و پشتیبانی، نیازی به خاموش کردن کل سرور ندارد و می‌تواند فقط بخش‌های معیوب را جدا کرده و جایگزین کند.

ذخیره‌سازی سرد اطلاعات برای روزهای بحرانی

یکی دیگر از راهکارهایی که در زمان وقوع جنگ‌ها، مورد توجه قرار می‌گیرد؛ ذخیره‌سازی سرد (Cold Storage) است. در این روش، تمام اطلاعات حیاتی یک شرکت، بنگاه مالی یا نهاد نظامی، روی تجهیزات ذخیره‌سازی آفلاین (مانند هارددیسک‌ها، دیسک‌های نوری یا مغناطیسی) نگهداری می‌شود. این دیسک‌ها نیز در محفظه‌های فلزی و کاملاً ایمن، نگهداری می‌شوند. معمولاً، از این روش برای نگهداری اطلاعات تاریخی، آرشیوهای ملی و

برای مقابله با تهدیدهای جنگی، از سرورهای توزیع شده، پشتیبان‌گیری ابری و طراحی ماژولار استفاده می‌شود تا دسترسی به داده‌ها حفظ شود. ذخیره‌سازی سرد نیز راهکاری برای حفاظت آفلاین از اطلاعات حیاتی است. کاربران و مدیران کسب‌وکار باید مسئولانه از داده‌هایشان پشتیبان‌گیری و آن‌ها را رمزنگاری و ایمن نگه دارند. محل احداث دیتاستر، سیستم‌های افزونگی، و اجرای منظم سناریوهای بازیابی بحران، نقش کلیدی در تداوم خدمات دارند.

حکایت

عاقبت ترس از مرگ

در روزگاران قدیم دو همسایه بودند که همیشه با هم نزاع و دعوا داشتند. یک روز با هم قرار گذاشتند که هر کدام دارویی بسازد و به دیگری بدهد تا یکی بمیرد و دیگری که می ماند لااقل در آسایش زندگی کند!

برای همین سکه‌ای به هوا انداختند و شیر و خط کردند که کدام یکی اول سم را بخورد. قرعه به نام همسایه دوم افتاد. پس همسایه اول به بازار رفت و از عطاری قوی‌ترین سمی که داشت را خرید و به همسایه‌اش داد تا بخورد. همسایه دوم سم را سرکشید و به خانه‌اش رفت. قبلاً به خدمتکارانش گفته بود حوض را برایش از آب گرم پر کنند و یک ظرف دوغ پر نمک هم آماده بگذارند کنار حوض. او همینکه به خانه رسید، ظرف بزرگ دوغ را سرکشید و وارد حوض شد. کمی دست و پا زد و شنا کرد و هر چه خورده بود را برگرداند و پس از آنکه معده‌اش تخلیه و تمیز شد، به اتاق رفت و تخت خوابید. صبح روز بعد

سالم بیدار شد و به سراغ همسایه‌اش رفت و گفت: من جان سالم به در بردم، حالا نوبت من است که سمی بسازم و طبق قرار تو آن را بخوری.

او به بازار رفت و نمذ بزرگی خرید و به خانه برد. خدمتکارانش را هم صدا کرد و به آنها گفت که از حالا فقط کارتان این است که از صبح تا غروب این نمذ را با چوب بکوبید!

همسایه اول هر روز می شنید که مرد همسایه که در تدارک تهیه سم است!! از صبح تا شب مواد سم را می‌کوبد. با هر ضربه و هر صدا که می شنید نگرانی و ترسش بیشتر می‌شد و پیش

خودش به سم مهلکی که داشتند برایش تهیه می‌کردند فکر می‌کرد!

کم کم نگرانی و ترس همه‌ی وجودش را گرفت و آسایشی برایش نماند. شب‌ها ترس، خواب از چشمانش ربوده بود و روزها با هر صدایی که از خانه‌ی همسایه می‌شنید دلهره‌اش بیشتر می‌شد و تشویش سراسر وجودش را می‌گرفت. هر چوبی که بر نمذ کوبیده می‌شد برای او ضربه‌ای بود که در نظرش سم را مهلک‌تر می‌کرد.

روز سوم خبر رسید که او مرده است. او قبل از اینکه سمی بخورد، از ترس مرده بود!!

این داستان حکایت این روزهای برخی از ماست. هر شرایط و بیماری مادامیکه روحیه‌ی ما شاداب و سرزنده باشد قوی نیست. خیلی‌ها مغلوب استرس و نگرانی می‌شوند تا خود بیماری...



لطیفه

کارمند حاضر جواب

کارمندی به دفتر رئیس خود می‌رود و می‌گوید: معنی این چیست؟ شما ۴۰۰ دلار کمتر از چیزی که توافق کرده بودیم به من پرداخت کردید. رئیس پاسخ می‌دهد: خودم می‌دانم، اما ماه

گذشته که ۴۰۰ دلار بیشتر به تو پرداخت کردم هیچ شکایتی نکردی. کارمند با حاضر جوابی پاسخ می‌دهد: درسته، من اشتباه‌های موردی را می‌توانم بپذیرم اما وقتی به صورت عادت شود وظیفه خود می‌دانم به شما گزارش کنم.



کاریکاتور



معما

کدام عدد باید جایگزین علامت سؤال شود؟ (گزینه‌های پاسخ در ردیف پایین قرار دارند.)

۷ ۵ ۸ ۴ ۹ ۳ ؟
۱۱ ۱ ۲ ۱۰

اگر ۵۰۰۰ را بدست آوردید باید بگوییم اشتباه است. جواب ۴۱۰۰ می‌باشد! الان مجدداً با ماشین حساب محاسبه کنید.

جواب معمای بازی و ریاضی:
جواب: ۴۱۰۰

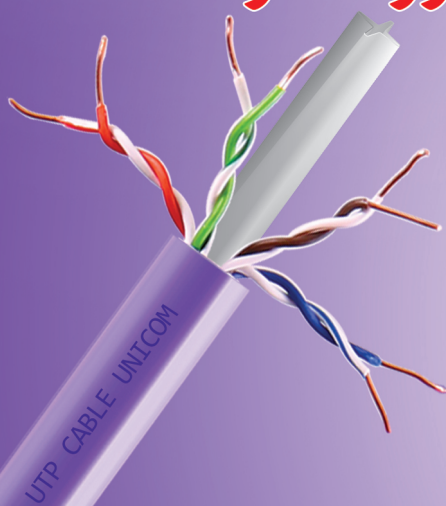




Category 6 Cable

Solid UTP / FTP / S-FTP

همگام با ارائه کابل خارجی،
تولید کابل یونیکام
در کشور آغاز شد!!



- دارای گواهینامه تطابق استاندارد TIA-568 .2D
- دارای گواهینامه تطابق استاندارد ISO/IEC 11801
- تضمین کیفیت HeadRoom حداقل 6db برای کابل‌های UTP
- تضمین تطابق با کلیه اتصالات یونیکام خارجی
- بسته‌بندی در فرقه‌های مطابق استانداردهای بین‌المللی
- حلقه‌های ۵۰۰ متری برای کاهش ضایعات در زمان نصب
- قیمت رقابتی



تلفن گویا: ۹۱۰۷۲۳۲۳
تلفن گویا: ۶۶۹۴۲۳۲۳
دورنگار: ۶۶۹۴۲۳۲۴
info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸
اپراتور: ۶۶۹۴۷۲۰۰
www.tiamnetworks.ir
tiamnetworks
company/tiamnetworks

icool®
Powered by TIAM

TAC6
CONDENSING UNIT

3011CF

با افتخار
ساخت ایران



**اولین و تنها
سیستم سرمایشی
مرکز داده کشور**

دارای استاندارد ملی ایران
به شماره
۱۵۶۲-۱، ۱۵۶۲-۲-۴۰



مشخصات فنی

- مجهز به کویل کندانسوری (U) شکل با فین آلومینیومی
- لوور دار و پوشش ضد خوردگی بلوفین (دارای راندمان بالاتر نسبت به فین های معمولی)
- ساخت کلیه قطعات بدنه از ورق گالوانیزه با پوشش رنگ پودری الکترواستاتیک
- با کیفیت بالا، مقاوم در برابر انواع شرایط محیطی
- ظرفیت واقعی کندانسور ۳۰ کیلووات در شرایط دمای محیطی ۴۲ درجه سانتیگراد
- مجهز به کمپرسور از برندهای معتبر بین المللی (کوپلند)
- به همراه هیتر کمربندی کمپرسور
- مجهز به کنترل خطی دور فن از ۰ تا ۱۰۰ درصد ظرفیت متناسب با شرایط کاری
- سیکل تبرید توسط درایو کنترلی از برند دلتا
- کنترل عملکرد تجهیزات توسط کنترلر مرکزی PLC
- قابلیت ارائه در مناطق حاره ای (T3)
- مجهز به فیلتر درایر از برند دانفوس و جدا کننده روغن از برند کستل
- مجهز به فن کندانسوری از برند زیلاگ
- مجهز به رسیور مایع جهت کارکرد منظم در کلیه فصول سال



Pressure control system



Net weight



Safety Standard of IRAN NO:1562



760x1465x1730 Set Dimensions (mm)



Vibration Less



Cooling design for -15°C to 55°C



Energy saving



R407C



تلفن گویا: ۹۱۰۷۲۳۲۳

تلفن گویا: ۶۶۹۴۲۳۲۳

دورنگار: ۶۶۹۴۲۳۲۴

info@tiamnetworks.ir

تهران، خیابان فاطمی غربی، پلاک ۲۴۸

اپراتور: ۶۶۹۴۷۲۰۰

www.tiamnetworks.ir

tiamnetworks

company/tiamnetworks