چرا یک استراتژی چند ابری برای محافظت از داده‌های سازمانی ضروری است

امروزه سازمان‌ها از تواناییهای ابر چه به عنوان بخشی از زیرساخت آنها، یا برای میزبانی اپلیکیشنها و یا به عنوان یک پلتفرم به خوبی آگاه هستند. ابر عمومی نیز به مرور در حال فراگیر شدن است. اما نکته جالب توجه در مورد استفاده سازمان‌ها از ابر چگونگی ایجاد تنوع در پیاده سازی این خدمات توسط آنها است. نظرسنجیها نشان میدهند شرکتها به دنبال آن هستند تا به جای استفاده از یک خدمات دهنده از چند ابر عمومی استفاده کنند. اما پرسش اینجا است که چرا توجهات تا به این اندازه به سمت خدمات چند ابری متمرکز شده است؟

طبق نظرسنجی انجام شده توسط Group Voice of the Enterprise 451 مشخص شده است که تا سال 2020 عمده بار کاری در یک سازمان به واسطه فراگیر شدن استفاده از IaaS, SaaS و PaaS به ابر عمومی منتقل خواهد شد.

اما نکته جالب توجه در مورد استفاده سازمان‌ها از ابر چگونگی ایجاد تنوع در پیاده سازی این خدمات توسط آنها است. RightScale نیز یک نظرسنجی در این مورد برگذار کرده است که نشان می‌دهد شرکت‌ها به دنبال آن هستند تا به جای استفاده از یک خدمات دهنده از چند ابر عمومی استفاده کنند. اما پرسش اینجا است که چرا توجهات تا به این اندازه به سمت خدمات چند ابری متمرکز شده است؟ پاسخ این است که با حق انتخاب‌های گوناگون سازمان‌ها می‌توانند همچنان که خطرات را به حداقل می‌رسانند، در عین حال می‌توانند سریع باقی بمانند و علاوه بر افزایش نوآوری هزینه‌ها را نیز بهینه سازی کنند.

چرا ایجاد تنوع ضروری است

با وجودی که خدمات دهندگان ابر عمومی مثل آمازون، گوگل و مایکروسافت خدمات قدرتمند و قابل اعتمادی را ارائه می‌دهند، اما بعضی اوقات در اختیار داشتن چند ابر و خدمات دهنده ضروری به نظر می‌رسد. این‌طور نیست که ممکن است این تامین کنندگان خدمات ابری با مشکل جدی مواجه شوند، اما اگر چنین اتفاقی رخ دهد، عواقب بزرگی به همراه خواهد داشت. شرکت‌های بزرگ بدون دسترسی به اپلیکیشن‌ها، سرورها و از همه مهمتر داده‌های خود با خسارات جبران ناپذیری مواجه خواهند شد.

از دسترس خارج شدن خدمات ابری که نمونه‌ای از آن اوایل امسال رخ داد و باعث شد در چندین ناحیه سرویس آمازون قطع شود و قطع شدن خدمات Microsoft Azure که اخیرا اتفاق افتاد، یک واقعیت کلیدی را آشکار می‌کند که خیلی از مدیران و گروه‌های فناوری اطلاعات آن را نادیده می‌گیرد: تنها و تنها این خود سازمان‌ها هستند که در برابر محافظت از داده‌های خود مسئولند. فراهم کنندگان خدمات ابر عمومی مسئولیتی برای داده‌های شما برعهده ندارند. اگر چه ممکن است توافقنامه سطح خدمات (SLA) 99.99 درصد باشد، اما آنها تنها برای دسترسی به شبکه و دوام زیرساخت هستند نه داده‌های مشتری و در دسترس بودن این داده‌ها. از داده تحت آنچه که اغلب به عنوان مدل مسئولیت مشترک نامیده می‌شود محافظت می‌شود.

هر کدام از فراهم کنندگان خدمات ابری از یک مدل مسئولیت مشترک متفاوت پیروی می‌کنند، بنابراین مهم است که مسئولان بخش فناوری اطلاعات سازمان‌ها جزئیات و مشخصات قراردادهای خود را به دقت مطالعه کنند. در توافق نامه آمازون مسئولیت‌های کاربر به وضوح مشخص شده و آمده است که این شرکت مسئولیتی در قبال امنیت هر نوع محتوا یا هر نوع تغییر یا از دست رفتن داده برعهده ندارد. توافق نامه مسئولیت مشترک مایکروسافت نیز کمی متفاوت است. آنها اعلام کرده‌اند که استفاده از IaaS و PaaS شامل مسئولیت حفاظت از داده نمی‌شود. اما خدمات SaaS مایکروسافت ضمانت دسترسی به داده را (تنها برای 30 تا 60 روز) پوشش می‌دهد.

چگونه باید خدمات چند ابری را آماده سازی و مدیریت کرد

هدف هر سازمانی این است که با معرفی شیوه‌های هوشمندانه مدیریت داده و فرآیند محافظت را تحت کنترل داشته و خدمات خود را بدون وقفه از طریق ابر ارائه کند. اولین قدم این است که اطمینان حاصل شود داده‌ها که بخشی حیاتی از یک کسب و کار کارآمد محسوب می‌شوند همیشه در دسترس باشند.

شرکت‌ها دیگر نمی‌توانند از روش قدیمی پشتیبان گیری روزانه از داده روی نوار یا ابر استفاده کنند. با افزایش سرعت تولید و تغییر داده خیلی از سازمان‌ها نیاز دارند تا هر دقیقه از داده‌های خود محافظت کنند. یکی از عوارض جانبی استفاده از استراتژی چند منطقه‌ای، چند مرکز داده و چند ابری بودن این است که داده‌های شما همه جا از ابرهای گوناگون و پایگاه‌های داده مختلف تا دستگاه‌های مختلف حضور دارند و این می‌تواند نگرانی‌های زیادی را به همراه داشته باشد.

مشکل اینجا است که بدون مدیریت هوشمندانه داده برای این خدمات چند ابری، گروه‌های فناوری اطلاعات سازمان‌ها امکان ردگیری مکان و نحوه محافظت از داده‌های خود را از دست می‌دهند. روش ایده‌ال برای محافظت داده در سرویس‌های چند ابری شامل پنج مرحله اصلی است:

پشتیبان گیری - به نظر کار ساده‌ای است، اما خیلی از سازمان‌ها برای فراهم کردن یک سیستم پشتیبان گیری قابل اطمینان که امکان بازیابی سریع داده در زمان قطعی، حملات و از بین رفتن داده را فراهم کند با چالش مواجه هستند. استفاده از APIها برای فراهم کردن امکان یکپارچه سازی عمیق با اپلیکیشن و زیرساخت‌ها برای مدیریت و حفاظت از داده ضروری است.

تجمیع - نکته کلیدی در این مرحله به کارگیری یک پلتفرم واحد و توسعه پذیر برای ارائه دسترسی است تا اطمینان حاصل شود که از تمام داده‌های حیاتی در یک محیط چند ابری با چند پایگاه داده محافظت می‌شود.

مشاهده و دسترسی - گروه‌ها باید قادر باشند تا به طور واضح و شفاف محیط‌های ذخیره و نگهداری از داده‌های خود را تحت نظر داشته و مدیریت کنند. چنین اقدامی سازمان‌ها را قادر می‌سازد برای بهینه سازی ظرفیت برنامه‌های خود و تحت نظر گرفتن منابع کنترل و دقت بیشتری داشته باشند.

تنظیم و ارکستراسیون - هدف از این مرحله این است که داده‌ها به طور یکپارچه به بهترین موقعیت مکانی در محیط‌های چند ابری منتقل شوند تا از تداوم کسب و کار، انطباق، امنیت و استفاده بهینه از منابع برای عملیات تجاری اطمینان حاصل شود.

اتوماسیون - این مرحله نهایی داده‌ها را قادر می‌سازد تا با یادگیری نحوه پشتیبان گیری و مهاجرت به یک موقعیت مکانی ایده‌ال از نظر نیازهای تجاری، خود را به طور خودکار مدیریت کنند و به این شکل بتوانند از خود در زمان فعالیت غیرعادی محافظت کنند.

همین حالا ایجاد تنوع را شروع کنید

سازمان‌ها به یک پلتفرم توسعه پذیر نیاز دارند تا بتوانند پیچیدگی‌های محیط‌های چند ابری را اداره کنند. با ایجاد تنوع در محافظت از داده توسط خدمات ابر عمومی گوناگون، سازمان‌ها می‌توانند اطمینان حاصل کنند که محافظت از داده‌های آنها دقیق‌تر و بهتر انجام می‌شود. اما با این حال همچنان موضوع مهم و حیاتی مربوط به مراکز داده

شخصی و نحوه مدیریت آنها است تا اطمینان حاصل شود که مسئولیت اصلی محافظت از داده بر عهده مالک سازمان است نه ارائه دهنده خدمات ابری.

منبع:
datacenterknowledge
تاریخ انتشار:
28 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/14180/%DA%86%D8%B1%D8%A7-%DB%8C%DA%A9-%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%DA%98%DB%8C-%DA%86%D9%86%D8%AF-%D8%A7%D8%A8%D8%B1%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86%DB%8C-%D8%B6%D8%B1%D9%88%D8%B1%DB%8C-%D8%A7%D8%B3%D8%AA