بهترین زمان برای بازبینی برنامه‌های بازیابی پس از فاجعه

چگونه ویروس کرونا می‌تواند به بهبود سیستم بازیابی پس از فاجعه مراکز داده کمک کند

ویروس کووید 19 بخش قابل توجهی از کارمندان را مجبور به خانه‌نشینی و کار از راه دور کرده است. بر همین اساس برخی از کارشناسان اعلام کرده‌اند، اکنون بهترین زمان برای بازبینی برنامه‌های بازیابی پس از فاجعه و برطرف کردن کاستی‌ها است.

سیستم‌های تهیه نسخه پشتیبان و بازیابی فاجعه اغلب مورد توجه قرار ندارند و بودجه لازم برای آن‌ها اختصاص پیدا نمی‌کند، به همین دلیل ممکن است؛ سازمان‌ها در برابر یک حمله سایبری به راحتی قربانی شوند، اما ویروس کووید 19 می‌تواند به بهبود این اوضاع کمک کند.

سازمان‌های بزرگ فرآیندهای مشخصی را در قالب یک استراتژی بازیابی آماده می‌کنند و در این مقطع زمانی نیز قرار نیست کار خاصی در این زمینه انجام شود، اما نگرانی از بابت شیوع گسترده‌تر ویروس کرونا باعث شده تا برخی از سازمان‌ها به فکر تهیه هرچه سریع‌تر این برنامه باشند و برخی نیز برنامه‌های موجود را بازبینی کرده‌اند تا خط‌مشی‌های بلندمدت در آن لحاظ شود.

آماده ورود تجهیزات سیار باشید

اغلب کارمندان سازمان‌ها و شرکت‌ها از مدت‌ها قبل تجهیزات سیار خود همچون لپ‌تاپ‌ها و دستگاه‌های تلفن همراه را به محل کار می‌آورند و به شبکه‌های ارتباطی سازمان متصل می‌شدند، اما اکنون شرایطی ویژه‌ای پیش آمده که نیروی کار مجبور است از دستگاه‌های سیار برای انجام کارهای خود استفاده کند. نکته‌ای که برخی از سازمان‌ها به آن توجهی ندارند این است که انجام فعالیت‌های تجاری توسط کارمندان از هر مکانی به معنای آن نیست که زیرساخت‌های ارتباطی سازمان آماده است تا پذیرای چنین شرایطی باشد. به عبارت دقیق‌تر، برقراری یک تعامل چهره به چهره با مشتریان برای کسب‌وکار شما ضروری است.

اگر شرکت شما در رویارویی با همه‌گیری ویروس کرونا، کارمندان را به ماندن در خانه ترغیب می‌کند، بخش قابل توجهی از نیروی کار ممکن است برای مدت زمان طولانی در خانه کار کند. از منظر محافظت از داده‌ها؛ این امر به‌طور قابل توجهی ممکن است باعث نقض مالکیت معنوی شود و حتا خطر دسترسی غیر مجاز به داده‌ها را افزایش می‌دهد. اگر سازوکار ارتباطی شرکت شما به گونه‌ای است که داده‌ها روی فایل‌سرورها یا سیستم‌های مشابه ذخیره‌سازی می‌شوند، این احتمال وجود دارد که کارمندان از راه دور به راحتی نتوانند به این سامانه‌ها متصل شوند. در سویی دیگر، این احتمال وجود دارد تا داده‌های مهم شرکتی به‌طور مستقیم روی لپ‌تاپ‌های کارمندان ذخیره‌سازی شود که این امر مشکل ذخیره‌سازی غیر متمرکز داده‌ها را به همراه خواهد آورد.

به همین دلیل لازم است تا خط‌مشی‌های شرکت در قبال محافظت از اطلاعات ذخیره شده روی لپ‌تاپ‌ها و دستگاه‌های تلفن همراه بررسی شود. در حالی که بیشتر متخصصان تهیه نسخه پشتیبان و بازیابی برای دستگاه‌های سیار را پیشنهاد می‌کنند، اما بسیاری از شرکت‌ها در این خصوص اقدام خاصی انجام نمی‌دهند. به نظر می‌رسد اکنون زمان خوبی برای انجام این کار باشد.

دلیل اصلی عدم ساخت نسخه پشتیبان از اطلاعاتی که روی لپ‌تاپ‌ها ذخیره می‌شود این است که فرآیند تهیه نسخه پشتیبان باعث کند شدن انجام کارها می‌شود و هزینه زیادی نیز به همراه دارد. برای حل این مشکل باید به سراغ نرم‌افزارهای اختصاصی برویم که اجازه می‌دهند از اطلاعات موجود روی لپ‌تاپ‌ها و دستگاه‌های همراه نسخه پشتیبان تهیه کرد.

البته راهکارهای جایگزینی نیز وجود دارند که سازمان‌ها و افراد را از تهیه نسخه پشتیبان بی‌نیاز می‌کنند. یکی از این راهکارها به‌کارگیری سامانه‌های ذخیره‌سازی و ارتباطی متمرکز همچون آفیس 365 یا G-Suite است. البته برای استفاده از این نرم‌افزارها کارمندان باید آموزش‌های لازم را دریافت کنند تا امکان ذخیره‌سازی دقیق و درست اطلاعات فراهم شود.

از داده‌های SaaS محافظت کنید

هرچه بیشتر از محصولات SaaS شبیه به Office 365 یا G-Suite استفاده می‌کنید، دوست دارید اطمینان حاصل کنید که داده‌های ذخیره شده در فضای ابری به شکل ایمنی محافظت می‌شوند. برای بهره‌مندی از مدل‌های مختلف ارائه خدمات ابری SaaS لازم است تا مفاد قرارداد ارائه‌دهنده خدمات را به دقت بررسی کنید تا ببینید در صورت بروز مشکل، خدمات پشتیبانی و بازیابی آن‌ها در چه وضعیتی قرار دارد. دقت کنید اغلب ارائه‌دهندگان خدمات SaaS پیشنهاد خاصی در این زمینه ارائه نمی‌کنند.

بهتر است در ارتباط با یکسری ویژگی‌های مهم همچون بازیابی ایمیل‌های حذف شده از یک سرویس و پشتیبان‌گیری و بازیابی که به‌نام قاعده 3-2-1 شهرت دارد غافل نشوید. برخی از ارائه‌دهندگان خدمات هیچ سرویس پشتیبانی در این زمینه ارائه نمی‌کنند و تنها یک یکسری قابلیت‌های ساده ارائه می‌کنند. در این حالت اگر یک اتفاق جدی برای حساب‌کاربری رخ دهد، بیشتر فروشندگان SaaS قادر به بازیابی اطلاعات نیستند و با توجه به این‌که در توافق‌نامه خدمات به چنین موضوعی اشاره نشده هیچ تعهدی در این زمینه نخواهند داشت.

مطلب پیشنهادی

سرمقاله شماره 177 ماهنامه شبکه
BYOD، داده‌های سازمان، ابزارهای کارکنان

به فکر تهیه نسخه پشتیبان در فضای ابری باشید

اگر اتفاق بدی رخ دهد و کارکنان فناوری اطلاعات قادر به مدیریت فیزیکی مرکز داده‌ها نباشند، این احتمال وجود دارد که شرکت شما در پاسخ‌گویی به یک فاجعه با مشکل جدی روبرو شود. بیشتر سیستم‌های سنتی نیاز به حضور فیزیکی و جابجایی دارند.

سرویس‌های بازیابی در برابر بلایایی که مبتنی بر ابر هستند به شکل خودکار و تمام وقت در دسترس قرار دارند. اگر زیرساخت ارتباطی شما به شکل ترکیبی یا به‌طور کامل بر مبنای فضای ابری استوار شده، این شانس را دارید تا در زمان بروز یک مشکل جدی در زیرساخت ارتباطی بدون نیاز به حضور فیزیکی مشکل را برطرف کنید، زیرا همه چیز در فضای ابری و از هر مکانی قابل مدیریت هستند. تنها کاری که باید انجام دهید بازگرداندن داده‌ها از فضای ابری به زیرساخت‌ها ارتباطی است. یک سیستم DR کاملاً خودکار نیز راهی عالی برای مقابله با خرابی‌ها و به ویژه حملات باج‌افزاری است. حملاتی که این روزها به‌فور رخ می‌دهند.

وحشت نکنید

طراحی و پیاده‌سازی سیستم پشتیبان و DR کار پیچیده‌ای نیست، اما اجازه می‌دهد در بدترین شرایط به شکل مدیریت شده همه چیز را به حالت اولیه خود بازگردانید و خدمات کاربردی را همچون گذشته در اختیار مردم قرار دهید تا سودآوری کسب‌وکارتان لطمه نخورد.

تاریخ انتشار:

15 فروردین 1399

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16752/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%88%DB%8C%D8%B1%D9%88%D8%B3-%DA%A9%D8%B1%D9%88%D9%86%D8%A7-%D9%85%DB%8C%E2%80%8C%D8%AA%D9%88%D8%A7%D9%86%D8%AF-%D8%A8%D9%87-%D8%A8%D9%87%D8%A8%D9%88%D8%AF-%D8%B3%DB%8C%D8%B3%D8%AA%D9%85-%D8%A8%D8%A7%D8%B2%DB%8C%D8%A7%D8%A8%DB%8C-%D9%BE%D8%B3-%D8%A7%D8%B2-%D9%81%D8%A7%D8%AC%D8%B9%D9%87-

%D9%85%D8%B1%D8%A7%DA%A9%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87