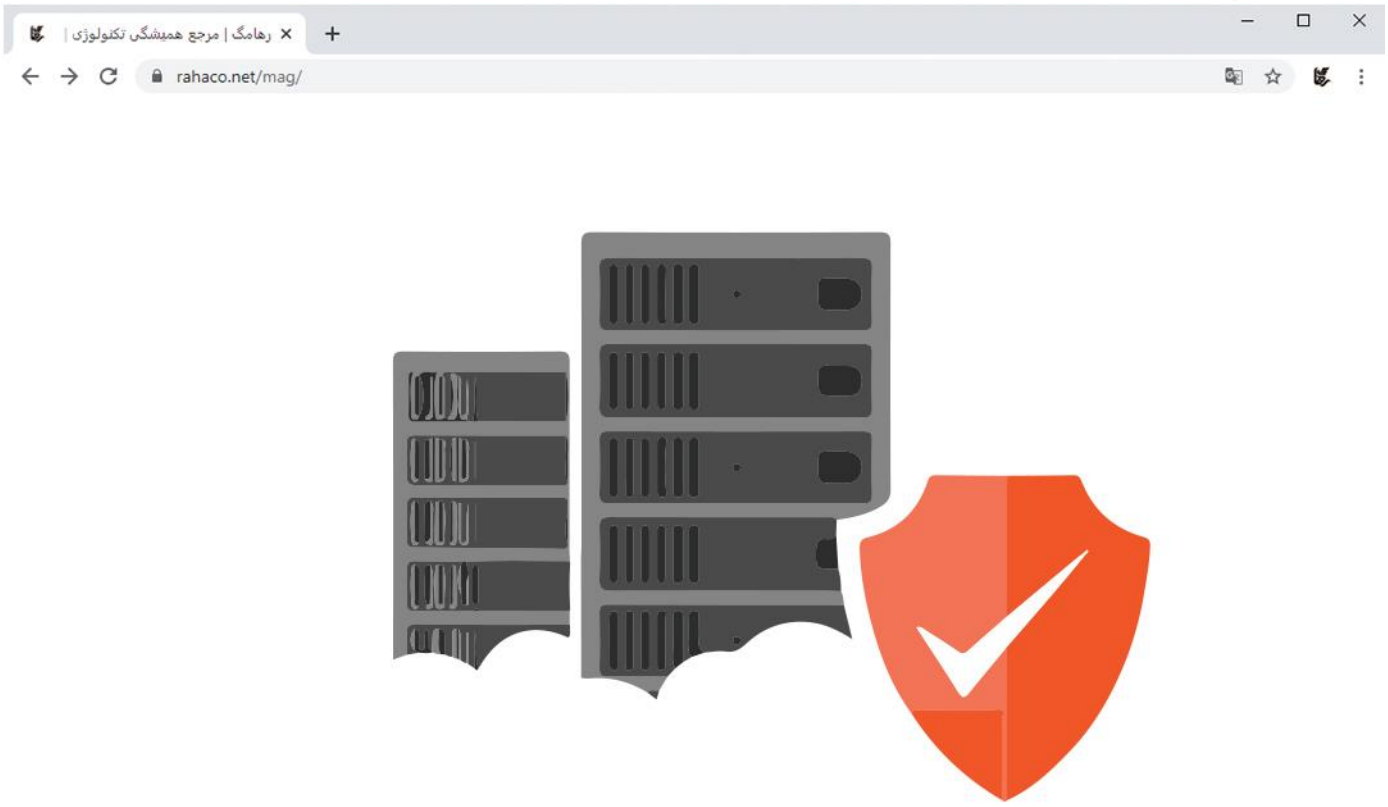
چگونه امنیت دیتاسنتر فراهم می‌شود؟

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



rahaco.net/mag

فهرست

تصور کنید یک جعبه پر از شمش‌های طلا دارید و باید به بهترین شکل از آن محافظت کنید. آیا جعبه را در یک فضای باز و نا امن رها می‌کنید یا با قفل و کلید آن را در جایی مطمئن پنهان می‌کنید؟ داستان دیتاسنتر نیز همین است: یک معدن طلا پر از اطلاعات! سرورهاو کامپیوترهایی که داده‌های ارزشمند شما را پردازش، توزیع و ذخیره می‌کنند در دیتاسنتر قرار دارند. بنابراین یکی از عناصر حیاتی زیرساخت دیجیتال سازمان شما، مرکز داده است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

امنیت دیتاسنتر ترکیبی از سیاست‌ها، فرآیندها، استراتژی‌ها و فناوری‌هایی است که آن را از حملات سایبری و سایر تهدیدات مجازی ایمن می‌کند. متاسفانه وقتی صحبت از امنیت مرکز داده می‌شود، بسیاری از شرکت‌ها حداقل‌ها را در مورد امنیت آن رعایت می‌کنند. استانداردهای امنیت دیتاسنتر چیست؟ و چرا باید این استانداردها در سازمان‌ها رعایت شود؟ در ادامه به شما میگوییم که چرا.

چرا امنیت دیتاسنتر اهمیت دارد؟

تمام دارایی‌های اطلاعاتی و مالکیت معنوی در مرکز داده قرار دارند. به همین دلیل اینجا کانون اصلی تمام حملات هدفمند است و بنابراین به سطح بالایی از امنیت نیاز دارند. مراکز داده حاوی صدها تا هزاران سرور فیزیکی و مجازی است که بر اساس نوع برنامه، دسته بندی داده‌ها و روش‌های دیگر تقسیم بندی می‌شوند. بدیهی است که مدیریت و کنترل دسترسی به منابع بسیار دشوار است و استفاده از قوانین امنیتی مناسب برای دیتاسنتر این کار را امکانپذیر می‌کند.

چالش‌های امنیت دیتاسنتر

گرافیک امنیت مرکز داده: نمونه‌ای از یک ابزار امنیتی مبتنی بر بیومتریک اسکنر اثر انگشت است که می‌توانید از آن برای محدود کردن دسترسی به مرکز داده استفاده کنید. جای تعجب نیست که داده‌های مهم یک شرکت برای دیگران اهمیت داشته باشد. این اطلاعات ارزشمند عامل اصلی موفقیت یا شکست کسب و کارها خواهد بود. اطلاعات اختصاصی مانند مالکیت معنوی و اسرار تجاری و همچنین اطلاعات شخصی و مالی مشتریان، نمونه‌هایی از انواع داده‌هایی هستند که در دیتاسنتر یافت می‌شوند.

دسترسی افراد متفرقه به مرکز داده آسیب‌های زیر را به دنبال دارد:

آسیب به شهرت و از دست دادن اعتماد مشتری. اگر اقدامات لازم را برای محافظت از داده‌های مشتریان خود (یا حتی مالکیت معنوی خود) انجام ندهید، چرا آن‌ها باید به شما اعتماد کنند؟

جریمه‌های عدم رعایت قوانین و مقررات. قوانین کلیدی وجود دارند که الزامات امنیتی مرکز داده را در خود جای داده اند.

زیان مالی. از کار افتادن دیتاسنتر یک نگرانی بزرگ برای مشاغل است و می تواند منجر به خسارات قابل توجهی شود.

اهمیت امنیت مرکز داده را نمی‌توان نادیده گرفت و این باید برای هر کسب‌وکاری در اولویت باشد. پس نیازی به گفتن نیست که اگر هر یک از این اطلاعات حیاتی به دست افراد نادرست برسد، با مشکلات زیادی مواجه خواهید شد. به همین دلیل است که باید از بهترین روش‌های امنیت مرکز داده باخبر باشید و آن‌ها را در زیرساخت سازمان خود پیاده سازی کنید.

سه نیاز حیاتی در امنیت دیتاسنتر

قدرت دید

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

هنگام ایمن سازی مرکز داده عوامل مختلفی از جمله: دیدگاه کاربران، دستگاه‌ها، شبکه‌ها، برنامه‌ها، حجم کاری و فرآیندها دخیل هستند. قدرت دید، تشخیص مشکلات را آسان کرده و حمله را در سریع‌ترین زمان ممکن شناسایی می‌کند. همچنین شناسایی افرادی که در تلاش برای سرقت داده‌های حساس یا اختلال در عملیات هستند با این ویژگی بسیار آسان می‌شود. علاوه بر این، نظارت فرایند بهبود پس از حادثه را بهبود می‌بخشد که این خود می‌تواند میزان نقض سیستم را آشکار کند و مشخص کند چه اطلاعاتی به سرقت رفته است.

تقسیم بندی

فرایند تقسیم بندی با محدود کردن مرکز داده، دامنه حمله را کاهش می‌دهد. تقسیم بندی یک ابزار مهم برای سرورهاست. تقسیم‌بندی برای محافظت از برای سیستم‌های قدیمی که دیگر به‌روزرسانی ارائه نمی‌دهند بسیار حیاتی است.

بسیاری از حملات بر روی دسترسی مستقیم به دیتاسنتر تاثیر می‌گذارند. این حملات از طریق آسیب پذیری‌های برنامه، پورت‌های ناامن یا حملات (DoS) برای انجام می‌شوند. حملات DoS سیستم را از کار می اندازد و به مهاجم اجازه می‌دهد تا کنترل ادمین را به دست آورده و کدهای مخرب را برای ادامه حمله نصب کند.

تهدیدات پیشرفته برای برخی از صنایع مانند: شرکت‌های آب و برق به بخشی از کار آن‌ها تبدیل شده است. تقریبا 100 درصد مواقع دفاع در برابر این نوع حملات غیرممکن است، اما تقسیم بندی ابزار ارزشمندی برای کاهش سرعت هکر و زمان دادن به تیم‌های امنیتی برای شناسایی حمله و نحوه پاسخ به آن‌هاست.

حفاظت در مقابل تهدیدات

دیتاسنتر باید از برنامه‌ها و داده‌ها در برابر تهدیدات پیچیده و حملات محافظت کند. همه سازمان‌ها در معرض خطر حمله قرار دارند در بیشتر مواقع از آن بی اطلاع هستند. امنیت مرکز داده مدرن به یک چالش برای تیم‌های امنیتی تبدیل شده است. اطلاعات مهم در مراکز داده فیزیکی و محیط های ابری در حال حرکتند. به همین دلیل است که سیاست‌های امنیتی این مکان‌ها باید به طور مداوم تغییر کنند.

برنامه‌های کاربردی موبایل و وب سطح حمله را افزایش می‌دهند و راه‌های جدیدی برای بهره برداری ایجاد می‌کنند. از سوی دیگر ممکن است کارمندان ناخواسته داده های مهم سازمان را به خطر بیاندازند. این روزها هکرها با روش‌های جدید می‌توانند به یک سرور یا سرورهای داخل مرکز داده دسترسی "مجاز" داشته باشد. شما می‌توانید با به کارگیری محصولات امنیتی جامع و یکپارچه، اختلالات و تاثیرات ناشی از نقض داده‌ها را کاهش دهید. این امر حفاظت، شناسایی و کاهش تهدیدات را بسیار ساده می‌کند.

چگونه از مرکز داده محافظت کنیم؟

هر سال، کسب‌وکارها متحمل ضررهای قابل توجهی می‌شوند و ممکن است سرمایه، مشتریان و شهرت خود را در طی حملات سایبری از دست بدهند. بنابراین عجیب نیست که تقریبا بخش‌های مختلف سازمان، از اتاق هیئت مدیره گرفته تا اتاق سرور

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

حول محور امنیت بچرخند. امنیت زیرساخت دیتاسنتر و فناوری اطلاعات همیشه یک نگرانی بزرگ برای مشاغل بوده است و اکنون حرکت به سمت پلتفرم‌های ابری در دستور کار شرکت‌های بزرگ و کوچک قرار گرفته است.

برای حفظ امنیت مرکز داده، کسب و کارها باید از سیستم‌های مجازی و فیزیکی استفاده کنند. علاوه بر حفاظت از دارایی‌های محاسباتی سازمان، اقدامات امنیتی ویژه شبکه باید برای جلوگیری از نفوذ حملات بدافزار و سایر تهدیدها در مرکز داده اعمال شود. این راهکارهای امنیتی همیشه بخش مهمی از طراحی و معماری مرکز داده بوده‌اند. دیتاسنتر اکوسیستم پیچیده‌ای است و حفاظت از آن مستلزم آن است که الزامات امنیتی هر قسمت به طور جداگانه در نظر گرفته شود. در این قسمت برخی از الزامات امنیت دیتاسنتر را شرح می‌دهیم.

امنیت دیتاسنتر به صورت فیزیکی

امنیت فیزیکی مرکز داده و اجزای آن برای ایمن نگه داشتن داده‌ها بسیار مهم است. مرکز داده باید برای مقابله با انواع چالش‌های فیزیکی، از حملات تروریستی و حوادث صنعتی گرفته تا بلایای طبیعی طراحی شود. افزایش امنیت فیزیکی اقدامات مختلفی را در برمیگیرد. این اقدامات شامل دیوارهای ضخیم و در و پنجره کمتر، افزایش قدرت دوربین مدار بسته و حفاظت در برابر آتش می‌باشند. هنگام ساخت مرکز داده، تمرکز اصلی باید روی انتخاب مکان مناسب باشد. گاهی مکان‌های خاص خطرات امنیتی جدی به همراه دارند که می‌تواند باعث قطع سرویس یا خرابی کامل شود. این مکان‌ها شامل:

- نیروگاه‌ها
- مناطق روی گسل زلزله
- مناطقی که هواپیماها هنگام فرود از آن عبور می‌کنند
- مکان‌های نزدیک به تاسیسات شیمیایی
- مناطق مستعد آتش سوزی فصلی
- مکان‌های در معرض سیل

علاوه بر این‌ها، استفاده از دیوارهای ضخیم نیز یک لایه امنیتی فیزیکی ایجاد خواهد کرد. دیوارهای ضخیم می‌توانند به جلوگیری از بلایای طبیعی و حتی انفجارها کمک کنند تا امنیت فیزیکی مرکز داده حفظ شود.

امنیت مجازی

این روزها فناوری مجازی سازی در مرکز داده بسیار رایج شده است. با این فناوری سیستم زیرساخت کسب و کارها مجازی می‌شود. با استفاده از آن مدیران میتوانند امنیت مرکز داده را از راه دور مدیریت کنند. در حالی که استفاده از نرم‌افزار و راهکارهای ابری انعطاف‌پذیری بیشتری را برای مدیران فراهم می‌کند، اما ممکن است زیرساخت دیتاسنتر را در معرض تهدیدات سایبری قرار دهد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

محدود کردن دسترسی

تیم امنیت دیتاسنتر باید مراقب افرادی باشد که وارد مرکز داده می‌شوند، از خدمه و کارکنان داخلیIT گرفته تا بازدیدکنندگان. دسترسی به این منطقه حساس باید محدود شود و تمام ورودی و خروجی‌ها ردیابی شوند. تنها در این صورت است که افراد غیرمجاز از اتاق‌های حساس سرور دور می‌مانند.

امنیت داده‌های مهم

هدف از امنیت مرکز داده انجام اقداماتی برای حفظ داده‌های خصوصی و مهم است. این اقدامات شامل بکاپ و بازیابی داده‌ها، رمزگذاری داده حین انتقال فایل‌ها، اجرای مقررات حفظ حریم خصوصی داده‌ها و نظارت بر ترافیک می‌باشد.

امنیت شبکه

اولین لایه امنیت شبکه با نصب فایروال‌ها صورت می‌پذیرد و این کار با نظارت بر ترافیک داخلی شبکه امکانپذیر خواهد شد. این اقدامات برای شناسایی و کاهش هرگونه تهدیدی که ممکن است فایروال را دور زده باشد، انجام می‌شود.

امنیت سرور

با مجازی سازی، امنیت سرور پیچیده‌تر و چالش برانگیزتر شده است. پیروی از استانداردها برای اطمینان از امنیت کامل سرور با نظارت 7×24 و تشخیص نفوذ ضروری است. این راهکار جامع امنیتی از تمام زیرساخت‌های سرور مجازی و فیزیکی و همچنین تمام برنامه‌های کاربردی مبتنی بر وب محافظت می‌کند. تمام مشاغل در سراسر دنیا دیر یا زود با یک تهدید واقعی روبرو می‌شوند. مهاجمان سایبری اکنون هر شرکتی را بدون در نظر گرفتن اندازه یا حوزه فعالیت آن هدف قرار می‌دهند و این حملات روز به روز پیچیده‌تر می‌شوند.

نتیجه گیری

مراکز داده در راس این حملات قرار دارند. البته آن‌ها به خوبی از گستردگی مشکل آگاه هستند و به همان اندازه راه‌های نوآورانه‌ای را برای محافظت از کسب و کار خود ابداع می‌کنند. امنیت دیتاسنتر مستلزم اقدامات گسترده‌ای برای نظارت و محافظت از آن در طول شبانه روز، هم به صورت فیزیکی و هم مجازی است. مهم‌تر از همه، سرمایه گذاری در یک برنامه آموزشی امنیت مرکز داده به سازمان شما در حفظ یک محیط امن و پایدار کمک خواهد کرد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net