محافظت از فایل های پشتیبان در مقابل باج افزارها

شرکت مهندسی تحقیق و توسعه ارتباط پانا

PANA

October, 2020

Ver. 1.0

WWW.PANACO.IR

چگونه می توان از نسخه های پشتیبان شرکت در برابر باج افزار محافظت کرد

پشتیبان گیری یک بخش اساسی از هر برنامه بازیابی و نجات از فاجعه باج افزار است. در صورتی که سازمانی توسط باج افزار در معرض آسیب قرار گیرد، می تواند به راحتی با استفاده از نسخه پشتیبان تهیه شده، سیستم را بدون پرداخت یک سنت، بازیابی کند.

فقط یک مشکل وجود دارد: فایل های پشتیبان اغلب از آسیب باج افزار در امان نیستند. حملات باج افزار که به طور فزاینده ای پیشرفته هستند، شامل مکانیزم هایی هستند که برای جستجو و رمزگذاری پشتیبان هایی که چه به صورت محلی و چه در ابر (cloud) ذخیره می شوند طراحی شده اند. و اگر فایل های پشتیبان یک شرکت رمزگذاری شود، ممکن است چاره ای جز پرداخت باج نباشد!!

در این متن به شما نشان خواهیم داد که باج افزار چگونه می تواند بر پشتیبان گیری شرکت تأثیر بگذارد و چگونه می توان نسخه پشتیبان را ایمن تهیه و امن نگه داشت.

باج افزار چگونه پشتیبان ها را رمزگذاری می کند؟

روش های زیادی وجود دارد که باج افزار می تواند سیستم را آلوده کند، از جمله پیوست های ایمیل، لینک های مخرب، حمله به درایو ، حملات RDP ، ابزارهای MSP و سایر نرم افزارهای ثالث (third party). هنگامی که یک نقطه پایانی (Endpoint) آلوده شد، به طور بالقوه و در کوتاه زمان می تواند به پشتیبان گیری های موجود در دستگاه هایی که از طریق پروتکل های استاندارد قابل دسترسی برای نوشتن هستند، مانند دستگاه های NAS، سرویس های ابری نصب شده محلی و دستگاه های متصل به USB ، گسترش یابد.

چند روش برای انجام این کار وجود دارد:

- **گسترش از طریق شبکه**

بسیاری از صاحبان مشاغل کوچک ارزش پشتیبان گیری را درک می کنند، اما ممکن است منابع یا تخصص لازم برای ایجاد و حفظ یک استراتژی مداوم و کامل را نداشته باشند. در عوض، ممکن است رویکردی موقت را در پیش گیرند، که ممکن است شامل کپی دستی فایل های مهم در یک هارد خارجی یا تهیه خودکار پشتیبان های منظم در یک فایل سرور متصل به شبکه باشد.

پشتیبان گیری محلی مهم است، اما وقتی تنها راهکار پشتیبان گیری باشد، راه حل موثری نیست. بسیاری از انواع باج افزارها قادر به گسترش جانبی در سایر رایانه ها و درایوهای شناخته شده در شبکه هستند. اگر سیستم آلوده

شود، احتمال زیادی وجود دارد که باج افزار در سراسر شبکه پخش شود و درایوی که نسخه پشتیبان سازمان در آن نگهداری می شود هم رمزگذاری شود.

- **همگام سازی با فضای ذخیره سازی ابری**

فضای ذخیره سازی ابری با رعایت همه شرایط و جوانب مربوطه، یک روش مناسب برای ذخیره فایل ها است، اما یک روش موثر برای حفظ فایل های پشتیبان نیست خصوصاً در مورد باج افزارها

بسیاری از سرویس های ذخیره سازی ابر مانند Dropbox، OneDrive و Google Drive به طور خودکار فایل های محلی را با فایل های ذخیره شده در cloud همگام سازی (synchronize) می کنند. اگر سازمان با باج افزار روبرو شود و فایل های موجود در شبکه شما رمزگذاری شوند، فایل های ذخیره شده در کلاود هم به دلیل همگام سازی خودکار، رمزگذاری می شوند.

برخی از ارائه دهندگان خدمات ذخیره سازی ابری نسخه فایل را ارائه می دهند، به این معنی که چندین نسخه از فایل را نگه می دارد. اگر فایل های شرکت شما رمزگذاری شده باشد، می توانید آنها را به نسخه قبلی و رمزگذاری نشده برگردانید. با این حال، این ویژگی توسط همه ارائه دهندگان فضای ذخیره سازی ابر پشتیبانی نمی شود و ممکن است به طور پیش فرض فعال نباشد.

- **حذف نقاط بازیابی سیستم**

System Restore، ابزار بازیابی داخلی Windows ، به مدیر اجازه می دهد تغییرات اخیر سیستم عامل را معکوس کند و می تواند برای برگرداندن درایورها و فایل های سیستم به نسخه های قبلی مفید باشد. متأسفانه، System Restore کپی فایل های شخصی ، از جمله اسناد، عکس ها و فیلم ها را ذخیره نمی کند، به این معنی که نمی توان از آن برای انجام فرایند معکوس رمزگذاری استفاده کرد.

حتی اگر System Restore بتواند به بازگرداندن فایل های شخصی کمک کند، بسیاری از انواع باج افزارها - از جمله WannaCry، Cryptolocker و Locky - برای شناسایی و حذف عمدی نسخه های Shadow و Image های احتمالی از سیستم، با استفاده از دستورات خط فرمان طراحی شده اند.

راهکارهای مقابله:

- **استفاده از یک روش چند لایه بهترین راه برای محافظت از نسخه های پشتیبان در برابر باج افزار است.**

پشتیبان گیری محلی سریع و کارآمد است و هر زمان که لازم باشد به راحتی قابل دسترسی است. با این حال، همانطور که در بالا ذکر شد، پشتیبان گیری محلی در برابر باج افزار، که به طور بالقوه می تواند در سراسر شبکه گسترش یابد، آسیب پذیر است.

در حالی که راه حل های ذخیره سازی خارج از سایت به طور کلی کندتر و مطمئن تر هستند، آنها از شبکه شرکت جدا هستند و بنابراین قابل اطمینان تر هستند. استفاده از ترکیبی از پشتیبان گیری محلی و خارج از سایت بهترین حالت را ایجاد می کند.

با در نظر گرفتن این موضوع، ساده ترین راه برای تهیه نسخه پشتیبان در مقابل باج افزار، اجرای قانون ۳-۲-۱ است که تعیین می کند یک کسب و کار باید:

- ✓ حداقل سه نسخه از فایل های مهم را نگه دارد.
- ✓ نسخه های پشتیبان حداقل باید در دو نوع رسانه ذخیره سازی مختلف ذخیره شوند.
- ✓ حداقل یک نسخه در خارج از شبکه نگهداری شود.

به یاد داشته باشید که همیشه برای همه سیستم های پشتیبان (و هر چیز دیگری مشابه این موضوع) از نام کاربری و گذرواژه های منحصر به فرد استفاده کنید.

- **چرا حداقل سه نسخه پشتیبان:**

هرچه سیستم پشتیبان قوی تر باشد، خطر از دست دادن داده ها کمتر است. شرکت ها و سازمان ها باید حداقل سه نسخه از داده های خود را حفظ کنند. اگر یک نسخه به دلیل باج افزار، سرقت، خطای فنی یا بلایای طبیعی از بین برود، مدیران مشاغل می توانند اطمینان داشته باشند که نسخه های دیگری نیز برای استفاده مجدد وجود دارد.

- **چرا حداقل دو نسخه را در رسانه های ذخیره سازی مختلف ذخیره کنیم:**

همه دستگاه ها دیر یا زود خراب می شوند. متنوع سازی فضای ذخیره سازی، خطر شکست همزمان بازیابی نسخه پشتیبان را به حداقل می رساند. هنگام ذخیره سازی و پشتیبان گیری به صورت محلی، حداقل از دو نوع مختلف حافظه ذخیره سازی مانند درایو محلی، فایل سرور، دستگاه NAS یا Tape Driveتا استفاده کنید.

- **چرا حداقل یک نسخه در خارج از سایت ذخیره کنیم:**

برای حداکثر حفاظت، حداقل یک نسخه از نسخه های پشتیبان باید کاملاً از شبکه جدا شده و ترجیحاً به صورت آفلاین ذخیره شود، جایی که از باج افزار در امان خواهد بود.

چند گزینه مختلف برای ذخیره فایل های پشتیبان شرکت در خارج از سایت وجود دارد. سیستم های Tape ممکن است یک راه حل تا حدودی منسوخ به نظر برسد، اما به لطف مقرون به صرفه بودن، مقیاس پذیری و پایداری بایگانی، همچنان یک گزینه محبوب هستند. سیستم های پشتیبان نواری معمولاً به هیچ شبکه ای متصل نیستند و بنابراین نمی توانند تحت تأثیر باج افزار قرار بگیرند.

خدمات پشتیبان گیری ابری راه حل مدرن تری را برای ایجاد و نگهداری پشتیبان های خارج از سایت ارائه می دهند. سرورهای پشتیبان گیری ابری در شرایطی که از امنیت و نظارت بر آنها اطمینان باشد که معمولاً شامل کنترل های محیطی، منابع تغذیه پشتیبان، سیستم های مهار آتش و ... است می توانند راهکاهای جایگزینی بخصوص برای سازمان ها و شرکتهای کوچک و متوسط باشند. اگر باج افزار یا یک فاجعه محلی نسخه پشتیبان محلی شرکت شما را از بین ببرد، می توانید از نسخه پشتیبان cloud برای راه اندازی مجدد استفاده کنید.

مقایسه ذخیره سازی ابری و پشتیبان گیری ابری

توجه به این نکته مهم است که خدمات ذخیره سازی ابری و خدمات پشتیبان گیری ابری متفاوت هستند. سرویس های ذخیره سازی ابری دقیقاً به همین منظور طراحی شده اند: تنها ذخیره فایل ها. این ابزار ممکن است نسخه های ترتیبی فایل را ارائه ندهند که این موضوع استفاده از آن را در مواقع خطر مشکل ساز و سازمان را در برابر باج افزار آسیب پذیر می کند و معمولاً به شما اجازه نمی دهند ساختار و ترتیب قبلی فایل خود را حفظ کنید، به این معنی که اگر شما به بازیابی سیستم خود نیاز داشته باشید تنها آخرین نسخه که احتمالا تحت تاثیر باج افزار قرار گرفته در اختیار شما خواهد بود، در این حالت برای پیشگیری از این موضوع باید تمام داده های خود را دستی سازماندهی کنید

از طرف دیگر، خدمات پشتیبان گیری ابری با در نظر گرفتن شرایط حملات و تداوم فعالیت سازمان پس از حادثه ساخته می شوند. این ابزارها به سازمان امکان می دهند ساختار سیستم فایل خود را حفظ کند و معمولاً دارای ویژگی های مفیدی مانند ویرایش فایل، گزارش وضعیت، گزینه های برنامه ریزی و روش های رمزگذاری بهتر برای انتقال داده ها هستند. وقتی نوبت به ضد باج افزار می رسد ، استفاده از نسخه پشتیبان ، انتخاب برتر است.

مدیریت دسترسی کاربران

صرف نظر از رسانه ذخیره سازی که سازمان برای استفاده انتخاب می کند، مهم این است که دسترسی به فایل ها فقط به افرادی که تایید شده و لازم است محدود شود. این شامل انتخاب دقیق افرادی است که دارای اعتبار ورود به سیستم برای سرورها و خدمات پشتیبان گیری هستند و همچنین ایجاد محدودیت زیاد برای دسترسی فیزیکی به نسخه پشتیبان تهیه شده برای نگهداری در خارج از سایت.. محدود کردن دسترسی به پشتیبان گیری به کاهش

سطح حمله باج افزار کمک می کند و احتمال نابودی اطلاعات حساس شرکت به دلیل اشتباهات را به حداقل می رساند.

کاهش اثرات باج افزار

استراتژی پشتیبان گیری قوی یک عنصر مهم برای کاهش اثرات باج افزار است.

با این حال، مانند هر داده ای، پشتیبان گیری نیز می تواند تحت تأثیر باج افزار قرار گیرد. استفاده از ترکیبی از نسخه پشتیبان محلی و خارج از سایت به سازمان در کاهش خطر باج افزار کمک می کند و سازمان را در موقعیت برنده قرار می دهد تا در صورت بروز حمله، زمان خرابی را به حداقل و فرایند بازگشت به حالت عادی را به سریعترین حالت برسانید.

- در صورت نیاز به توضیحات بیشتر با همکاران ما در دپارتمان فنی پانا تماس بگیرید، همکاران ما با افتخار آماده پاسخگویی خواهند بود.

www.panaco.ir
02188876142 | 02188873951
03136691964 | 03195017415