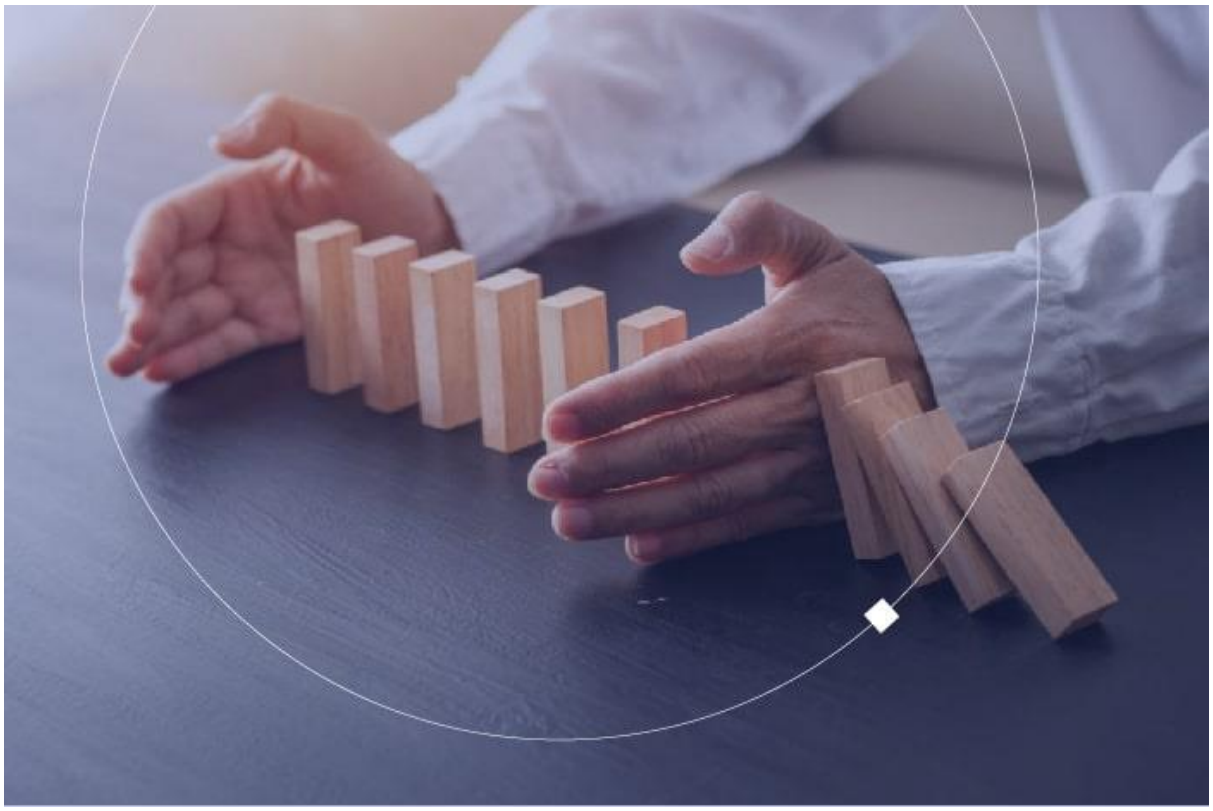
چگونه از پایگاه داده خود در مقابل باج افزارها دفاع کنیم؟



سوالی که اغلب بعد از مواجهه با باج‌افزارها پیش می‌آید این است که باید چه کاری می‌کردیم و نکردیم که این اتفاق افتاد؟

برای شفافیت بیشتر، بهتر است اول به این سوال پاسخ بدهیم که Ransomware یا همان باج‌افزار چیست؟

فردی را در نظر بگیرید که به واسطه‌ی ضعف امنیتی‌مان، به اطلاعات محرمانه‌ی ما دسترسی پیدا کرده و از ما می‌خواهد به او پولی بدهیم که در ازای آن، اطلاعات ما را افشاء نکند. در واقع او از ما باج می‌خواهد. پس خود آن فرد نیز «باج‌گیر» به حساب می‌آید. اما اینکار را با چاقو و اسلحه و امثالهم انجام نمی‌دهد بلکه با استفاده از دانش نرم‌افزاری خود این کار را می‌کند؛ نرم‌افزارِ او برای اجرای این کار «باج‌افزار» نام دارد.

اصلی‌ترین آسیبی که باج‌افزارها به وجود می‌آورند این است که مجبورمان می‌کنند قید تمام اطلاعات خود را بزنیم و بعد از آن ناچاریم که تمام داده‌های‌مان را از «پایگاه داده» حذف کنیم و از ابتدا نصب و راه‌اندازی اطلاعات را انجام دهیم. پس اصلی‌ترین موردی که باید از آن محافظت بشود، پایگاه داده است.

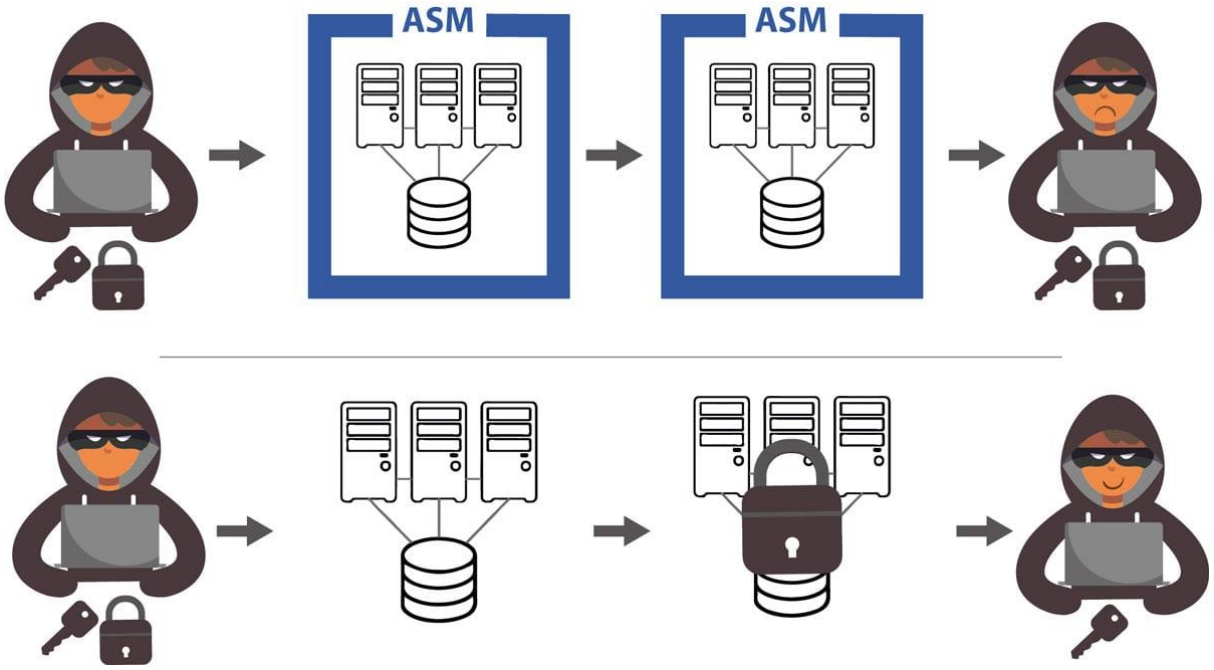
مشخص است که تنها چاره در این شرایط، بالاتر بردن امنیت اطلاعاتمان است ولی برای اینکه بفهیمم که چه کاری بهترین کار در جهت مقابله با نفوذ باج‌افزار است، باید ابتدا متوجه بشویم که «باج‌گیر»ها، از چه طریقی اقدام به آنالیز و بررسی سیستم ما می‌کنند.

معمولاً اینگونه است که باجگیرها از طریق Data Dictionary، متوجه می‌شوند که آدرس فایل های ذخیره شده ما کجاست و بعد شروع به کد کردن فایل‌ها می کنند و عملاً هیچ اهمیتی هم به پسوند فایل‌ها نمی‌دهند و تر و خشک را با هم «کد» می‌کنند. (کُد کردن همان کار اصلی و مخربی‌ست که باج‌افزارها انجام می‌دهند). در این حالت اگر فایل‌های بکاپ بر روی سرورمان باشند، نسخه‌های پشتیبان ما نیز تحت آسیب قرار خواهند گرفت و ممکن است باج‌افزارها به طور کلی باعث از کار افتادن سیستم و از دست رفتن اطلاعات ما بشوند.

پس اولین قدم و اصلی ترین قدم برای مواجهه با باج‌افزارها این است که کاری کنیم اطلاعات‌مان قابل مشاهده نباشد. اگر به هر طریقی بتوانیم این قدم را برداریم ، تا حد خیلی زیادی از آسیب باجگیری در امان خواهیم ماند. یعنی باید کاری کنیم که باجگیر به راحتی نتواند جزئیات اطلاعات ما را مشاهده کند.

از میان راه‌حل‌هایی که برای پاسخ به این آسیب وجود دارند، راه حلی که کمپانی Oracle ارائه می‌کند، بسیار کارآمد و هوشمندانه به نظر می‌رسد. اوراکل،سرویس مدیریت هوشمند فضای ذخیره‌سازی را تحت عنوان Automatic Storage Management ارائه می‌دهد. و یکی از ویژگی‌های منحصربه‌فرد سرویس ASM این است که از ابتدا، پیکربندی هارددیسک و بلاک‌بندی آن تحت نظارت Oracle انجام

می‌شود و دیگر نحوه‌ی قرارگیری فایل‌های نصبی، قابل مشاهده نیست و از بیرون یک دیسک خام یا به اصطلاح Rawdisk به نظر می‌رسد؛ با این اقدام به یک معنا این Oracle است که مسئولیت امنیت اطلاعات را برعهده گرفته است و این یعنی دست باج‌افزار از اطلاعات دور خواهد ماند و احتمالاً خطری متوجه مجموعه‌ی ما نخواهد بود.



شاید تنها خطری که در این حالت متوجه سیستم ما باشد، این باشد که خودِ نرم‌افزار Oracle که روی سرور ما نصب است کُد بشود که در آن صورت، با پاک کردن و نصب مجدد این نرم‌افزار مشکل حل خواهد شد و کارکرد سیستم به حالت عادی برخواهد گشت.

اما اگر نخواهیم حتی در حد همین پاک کردن و نصب مجدد اوراکل هم سرورمان از دسترس خارج بشود، چاره این است که به Linux مهاجرت کنیم. چرا که باج‌افزارها معمولا در محیط Windows وجود دارند و در لینوکس احتمال ابتلا به باج‌افزار، بسیار بسیار کمتر خواهد بود. چرا که برخلاف ویندوز که ما می‌توانیم در آن فایل های exe را ببینیم، در لینوکس این امکان وجود ندارد و Directory Base بودن لینوکس، عملاً فعالیت باج‌افزارها را بی‌نهایت سخت و در واقع ناممکن می‌کند.

در مجموع، مسئله باید شفاف و روشن باشد و اولویت حفاظت از پایگاه داده برای مجموعه، به طور مستقیم بر انتخاب راهکار مناسب تأثیر می‌گذارد؛ و اگر بر عدم ابتلا به باج‌افزارها متمرکز باشیم، بهتر است در نظر داشته باشیم که چه راهکاری می‌تواند حفاظت بهتری از داده‌ها و بالاخص پایگاه‌داده‌ی ما را در بر داشته باشد و بر اساس آن اقدام کنیم.