آشنایی با انواع و نحوه کار گواهی‌نامه‌های SSL در ویندوز سرور 2019

زمانی که شرکتی تصمیم می‌گیرد گواهی SSL را از یکی از توزیع‌کنندگان عمومی خریداری کند، یک فرآیند تأیید اعتبار دقیق انجام می‌شود تا ارائه‌دهنده گواهی‌نامه اطمینان حاصل کند شخصی که درخواست دریافت گواهینامه را ارائه کرده، دقیقا همان فردی است که ادعا می‌کند و شرکت او در کارهای قانونی به فعالیت اشتغال دارد. شرکت‌های عمومی توزیع‌کننده گواهی‌نامه‌های SSL بر مبنای این مکانیزم امنیتی گواهینامه‌های SSL را صادر می‌کنند.
گواهی‌نامه‌هایی که از سوی این شرکت‌ها صادر می‌شوند معتبر هستند و نیازی نیست زمانی‌که از گواهی‌نامه‌های فوق برای سایت خود استفاده می‌کنید، کار خاصی را در رابطه با عملکرد وب‌سایت روی اینترنت انجام دهید.

برای مطالعه قسمت قبل **آموزش رایگان ویندوز سرور 2019** اینجا کلیک کنید.

انتشار گواهینامه SSL از یک سرور CA که خودتان ساخته‌اید و درون شبکه در حال اجرا است، امکان‌پذیر است، اما در این حالت لازم است به چند نکته مهم دقت کنید که ممکن است کار را پیچیده کنند، زیرا گواهی‌نامه‌ای که از سوی سرور CA شما انتشار پیدا می‌کند ممکن است از سوی همه کامپیوترها به عنوان یک گواهی‌نامه قابل اعتماد شناخته نشود. اگر در نظر دارید مجوز SSL خود را برای استفاده در یک وب سایت عمومی منتشر کنید، باید حداقل بخشی از PKI داخلی خود را که با نام خدمات صدور، ابطال و انتشار گواهی‌نامه‌ها (CLR) سرنام Certificate Revocation List شناخته می‌شود را به اینترنت منتقل کنید. هر زمان که یک مؤلفه درون شبکه‌ای را به اینترنت منتقل کنید، یک ریسک امنیتی به وجود می‌آورید، بنابراین زمانی این‌کار را انجام دهید که واقعا مجبور هستید. دلیل دومی که به‌کارگیری گواهینامه‌های SSL شخصی در وب‌سایت‌های عمومی را با دشواری همراه می‌سازد این است که فقط کامپیوترهای عضو دامنه شما می‌دانند که چگونه باید به این گواهی SSL اعتماد کنند. بنابراین، اگر یک کاربر لپ‌تاپ شرکت را به خانه خود بیاورد و از آن برای دسترسی به صفحه ورود به ایمیل خود استفاده کند، بدون مشکل به صفحه مربوطه دسترسی خواهد داشت، اما اگر کاربر سعی کند به همان صفحه ورود به ایمیل از کامپیوتر خانگی خود که بخشی از دامنه یا شبکه سازمان نیست دسترسی پیدا کند، یک پیام هشدار مرتبط با گواهینامه‌ها دریافت می‌کند که برای دستیابی به وب‌سایت باید یکسری کارهای خاص را انجام دهد. شما هرگز نباید کاربران سازمان خود را ترغیب کنید که یک چنین خطری را قبول کرده و از طریق یك پیام هشداردهی گواهی‌نامه اقدام به باز کردن سایت‌ها کنند، زیرا پیامد این کار فاجعه‌آمیز است، حتا اگر گواهی که آن‌ها روی آن کلیك می‌کنند، توسط CA خود شما صادر شده باشد. این یک اصل مهم است که هرگز خطر را قبول نکنیم.

این مشکل را می‌توان با خرید یک گواهینامه SSL از یکی از شرکت‌های عمومی صادرکننده گواهی‌نامه‌ها برطرف کرد، بنابراین خرید این نوع گواهینامه‌ها رویکرد متداولی است و توصیه می‌شود در وب‌سایت‌های عمومی از یک چنین گواهی‌نامه‌های SSL استفاده کنید. برای وب‌سایت‌هایی که به‌طور کامل درون شبکه هستند داستان متفاوت است،

زیرا با اینترنت سر و کار ندارند و مشکلات امنیتی آن‌ها به راحتی به فضای ناامن اینترنت ورود پیدا نمی‌کند. شما می‌توانید از سرور CA داخلی خود برای صدور گواهینامه SSL برای وب‌سایت‌های داخلی استفاده کنید و نیازی به پرداخت هزینه‌های مربوط به خرید گواهی‌نامه برای این مدل وب‌سایت‌ها نیست.

مدل‌های مختلفی از گواهینامه‌های SSL وجود دارد که می‌توانید از یک CA عمومی خریداری کنید که اطلاعات مربوطه درون وب‌سایت‌های توزیع‌کنندگان درج شده است. البته یک اصل کلی وجود دارد که هرچه بیشتر هزینه کنید، گواهی شما ایمن‌تر است. مدل‌های مختلف گواهی‌نامه‌ها به نحوه تایید اعتبار درخواست‌کننده گواهی‌نامه از سوی ارائه‌دهنده گواهی‌نامه اشاره دارند، جایی که مباحث امنیتی حرف اول را می‌زنند. به‌طور مثال، شرکت ارائه‌دهنده گواهی‌نامه تضمین می‌کند که وقتی به صفحه‌ای که توسط گواهینامه آن‌ها تایید شده دسترسی پیدا می‌کنید این گواهی به شرکت حقیقی که صاحب آن صفحه وب است تخصیص داده شده است.

به غیر از مرحله اعتبارسنجی که هنگام خرید گواهینامه می‌توانید انتخاب کنید، گزینه دیگری نیز وجود دارد که باید در مورد آن تصمیم بگیرید که در ارتباط با جنبه فنی و مدلی است که گواهینامه بر پایه آن کار می‌کند. در هنگام خرید گواهینامه، نوع‌های مختلف بر مبنای نام‌گذاری‌هایی که برایشان تعریف شده شناخته می‌شوند. اجازه دهید سه مورد از گواهی‌های SSL پر کاربرد را بررسی کنیم.

گواهی‌های تک نامی

گواهی‌نامه‌های تک نامی ارزان‌ترین و متداول‌ترین مسیری است که برای خرید گواهینامه برای یک وب‌سایت شخصی در اختیارتان قرار دارد. یک گواهی تک نامی از اطلاعات یک نام DNS انفرادی برای برقراری امنیت استفاده می‌کند. زمانی‌که وب‌سایت جدیدی در پورتالی شبیه به portal.contoso.com راه‌اندازی کردید و در نظر دارید این وب‌سایت با استفاده از HTTPS از ترافیک میان کلاینت و سرور محافظت کند از طریق یک گواهی SSL که روی وب‌سایت نصب می‌شود قادر به انجام این‌کار هستید. زمانی‌که درخواستی برای گواهی‌نامه جدید برای مرجع صدور گواهینامه ارسال می‌کنید باید نام خاص portal.contoso.com را در قسمت نام مشترک در فرم درخواست وارد کنید. این نام DNS انفرادی تنها نامی است که می‌تواند توسط این گواهینامه محافظت و تأیید شود.

گواهینامه Subject Alternative Name

گواهینامه (SAN) سرنام Subject Alternative Name به‌طور کلی هزینه‌ای کمی بیشتر از گواهینامه‌های تک نامی‌دارد، زیرا قابلیت‌های بیشتری ارائه می‌دهد. هنگام درخواست گواهینامه SAN، شما می‌توانید چند نام DNS را تعریف کنید تا گواهی‌نامه از آن‌ها محافظت کند. پس از صدور، گواهینامه SAN حاوی یک نام DNS اصلی است که به‌طور معمول نام اصلی وب‌سایت است و درون آن ویژگی‌های گواهی و نام‌های DNS دیگری را که در طی درخواست خود مشخص کرده‌اید پیدا می‌کنید. این گواهینامه منفرد را می‌توان در یک وب‌سرور نصب کرد و برای اعتبارسنجی ترافیک برای هر یک از نام‌های DNS موجود در گواهی از آن استفاده کرد. یک مثال ساده از یک گواهی‌نامه SAN زمانی است که سرور Lync سرنام Skype for Business را پیکربندی می‌کنید. Lync از نام‌های DNS مختلفی استفاده می‌کند، اما تمامی نام‌ها درون دامنه DNS یکسانی قرار دارند. در زمان به‌کارگیری گواهی‌نامه‌های SAN دقت کنید که نام شما باید بخشی از همان دامنه یا زیر دامنه باشد. در اینجا نمونه‌ای از نام‌هایی را مشاهده می‌کنید که ممکن است در یک گواهینامه SAN مرتبط با Lync وجود داشته باشند.

- Lync.contoso.com (the primary one)
- Lyncdiscover.contoso.com
- Meet.contoso.com
- Dialin.contoso.com
- Admin.contoso.com

این وب‌سایت‌ها/سرویس‌های مختلفی که توسط Lync استفاده می‌شوند در ادامه توسط یک یا چند سرور پیاده‌سازی می‌شوند و می‌توانید از گواهینامه یکسان SAN در تمامی آن سرورها استفاده کنید تا ترافیکی که به سمت هر یک از این نام‌های DNS هدایت می‌شوند، اعتبارسنجی شوند.

گواهینامه‌های Wildcard

گواهی‌نامه سومی که در این مقاله به آن اشاره می‌کنیم گواهی‌نامه Wildcard است. این مدل گواهی‌نامه لاکچری است، زیرا بیشترین قابلیت را دارد و بالاترین انعطاف‌پذیری را در اختیارتان قرار می‌دهد و در عین حال ساده‌ترین مسیر پیاده‌سازی روی بیشتر سرورها را ارائه می‌دهد. نام موجود در یک گواهی Wildcard با کاراکتر ستاره (*) شروع می‌شود. این ستاره به معنی این است که هر چیزی قبل از نام دامنه DNS ظاهر می‌شود، تحت پوشش این گواهینامه است. اگر شما مالک contoso.com هستید و قصد دارید بسیاری از رکوردهای عمومی DNS را که در بیشتر وب‌سایت‌ها و سرورهای مختلف استفاده می‌شوند را تحت پشتیبانی گواهی‌نامه قرار دهید باید یک گواهی‌نامه Wildcard را به شکل *.contoso.com خریداری کنید تا گواهی‌نامه هر آن چیزی که نیازمند محافظت است را شامل شود.

به‌طور معمول، wildcardها را می‌توانید روی وب‌سرورهایی که نیاز دارید نصب کنید. دقت کنید در زمان به‌کارگیری این گواهی‌نامه هیچ محدودیتی در تعداد نام‌های مختلف DNS که این گواهی‌نامه اعتبارسنجی می‌کند وجود ندارد. البته یک استثنا نیز وجود دارد، هنگامی که توافق‌نامه خاصی میان مشتری و مرجع صدور گواهینامه در ارتباط با این گواهی‌نامه‌ها تنظیم می‌شود، ممکن است در قرارداد قید شده باشد که مشتری باید برای هر نمونه گواهی‌نامه‌ای که از آن استفاده می‌کند هزینه مربوطه را پرداخت کند. بنابراین وقتی با مرجع صدور گواهی‌نامه صحبت می‌کنید، حتما مفاد قرارداد را مطالعه کنید. در بیشتر اوقات، یک wildcard به شکل رایگان در تمامی موارد در یک شرکت در دسترس قرار دارد که اجازه می‌دهد از این گواهی‌نامه در ارتباط با سایت‌ها و سرویس‌های مختلفی که روی سرورها میزبانی می‌شوند استفاده کنید. نکته منفی در ارتباط با این گواهینامه قیمت بالای آن‌ها است. اگر برنامه‌های درازمدت روبه‌رشدی دارید خرید این گواهی‌نامه‌ها در طولانی مدت توجیه اقتصادی خواهند داشت. گواهینامه wildcard قابلیت فعال‌سازی پروتکل HTTPS روی دامنه اصلی و تمامی زیردامنه‌ها را امکان‌پذیر می‌کنند. در نتیجه اگر تمایل دارید بخش‌های مختلف وب‌سایت همچون ارتباطات در زیردامنه‌ها امنیت بیشتری داشته باشند و گواهی SSL روی زیردامنه‌ها هم فعال باشد، پیشنهاد می‌کنیم با صرف هزینه کمتر از گواهی Wildcard استفاده کنید تا تمامی دامنه‌های مرتبط با دامنه اصلی را ایمن کنید.

لازم به توضیح است که گواهی‌نامه‌های دیگری همچون SSL DV Standard، SSL OV، SSL EV نیز وجود دارند که در این مقاله به آن‌ها اشاره‌ای نداشتیم.

PKI خود را برنامه‌ریزی کنید

از آن‌جایی که آموزش ما مرتبط با Windows Server 2019 است، در نتیجه سرور مرجع صدور گواهی‌نامه شما باید از جدیدترین سیستم‌عامل روز استفاده کند. همانند سایر قابلیت‌ها در سرور 2019، فرآیند ساخت سرور مرجع صدور گواهی‌نامه در یک شبکه به سادگی نصب یک نقش است. زمانی‌که تصمیم می‌گیرید نقشی به سرور جدید خود اضافه کنید، در اولین گام به سراغ Active Directory Certificate Services یا همان AD CS می‌روید. زمانی‌که نقش فوق را نصب کردید، دو گزینه مهم در اختیارتان قرار می‌گیرد که پیش از ایجاد یک محیط زیرساخت کلید عمومی (PKI) باید اطلاع دقیقی در مورد آن‌ها داشته باشید. نام میزبان و وضعیت دامنه پس از پیاده‌سازی نقش مرجع صدور (CA) قابل تغییر نیستند. اطمینان حاصل کنید که نام میزبان نهایی خود را به درستی تنظیم کرده‌اید و قبل از نصب نقش AD CS ، این سرور را به دامنه (در صورت وجود) متصل کرده‌اید. پس از پیاده‌سازی زیرساخت کلید عمومی قادر به انجام این‌کار نیستید.

در شماره آینده آموزش رایگان **ویندوز سرور 2019** مبحث فوق را ادامه خواهیم رفت.

برای مطالعه تمام بخش‌های **آموزش ویندوز سرور 2019** روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:

04 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15964/%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D8%A7%D9%86%D9%88%D8%A7%D8%B9-%D9%88-%D9%86%D8%AD%D9%88%D9%87-%DA%A9%D8%A7%D8%B1-%DA%AF%D9%88%D8%A7%D9%87%DB%8C%E2%80%8C%D9%86%D8%A7%D9%85%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-ssl-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019