18 – [illegible]

[illegible] 2019 [illegible]



[illegible] MSC [illegible] MMC [illegible] 2019 [illegible]

[illegible] MSC:

- DSA.MSC: Active Directory Users and Computers
- WF.MSC: Windows Defender Firewall with Advanced Security
- DSSITE.MSC: Active Directory Sites and Services
- DNSMGMT.MSC: DNS Manager
- GPEDIT.MSC: Local Group Policy Editor
- GPMC.MSC: Group Policy Management Console
- CERTSRV.MSC: Certification Authority Management
- CERTTMPL.MSC: Certificate Template Management

- CERTLM.MSC: Local Computer Certificates Store
- CERTMGR.MSC: Current User Certificates Store
- COMPMGMT.MSC: Computer Management
- DEVMGMT.MSC: Device Manager
- DHCPMGMT.MSC: DHCP Manager
- DISKMGMT.MSC: Disk Management
- EVENTVWR.MSC: Event Viewer
- PERFMON.MSC: Performance Monitor
- SECPOL.MSC: Local Security Policy Console
- FSMGMT.MSC: Shared Folders

[illegible] 2019

[illegible]

[illegible] (PKI) [illegible] **Public Key Infrastructure** [illegible] PKI.

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] TPM [illegible]

[illegible] PKI [illegible]

[illegible]

[illegible] SCCM [illegible] IPsec [illegible] DirectAccess [illegible]

SSL [illegible]

[illegible] CA [illegible] SSL [illegible] HTTPS [illegible] SSL [illegible]

[illegible] mail.contoso.com [illegible] Outlook Web Access [illegible] DNS [illegible] HTTPS [illegible] SSL [illegible]

میشود از وجود این گواهی اطلاعی پیدا نخواهد کرد . از طرف دیگر، اگر ترافیک میان کاربر و سایت در حال رهگیری و هدایت مجدد به وبسایت جعلی باشد، وضعیت بررسی گواهینامه SSL خراب گزارش داده شده (زیرا مهاجمان گواهی SSL معتبری برای نام وبسایت شرکت شما ندارند) و رهگیری کاربر متوقف میشود . در این حالت صفحه هشداری در ارتباط با گواهینامه به کاربر نشان داده میشود .

در این مرحله، کاربر باید کار را متوقف و بررسی کند که اشتباهی رخ نداده و با کارمندان IT سازمان تماس گرفته تا موضوع را بررسی کنند . گواهینامههای SSL که توسط وبسایتها در اینترنت استفاده میشوند، متفاوت از گواهینامههایی هستند که سرور CA داخلی یک سازمان از آن استفاده میکند . شاید در مورد شرکتهایی همچون DigiCert ، Entrust ، Verisign و GoDaddy مطالبی دیده باشید . بیشتر سازمانها از این شرکتهای مطرح گواهینامههای SSL را خریداری میکنند، زیرا گواهینامههای SSL معتبر و قابل اعتمادی را ارائه میکنند . هنگامی که به وبسایتی که گواهینامه SSL آن توسط یکی از فروشندگان عمومی ارائه شده مراجعه میکنید، کامپیوتر شما به آن گواهینامه اعتماد میکند . مراجع صدور گواهینامههای عمومی نهادهای شناخته شده هستند که به خاطر تواناییشان در صدور ایمن گواهینامههای SSL معروف هستند.

نویسنده :
حمیدرضا تائبی
دسته بندی:
فناوری شبکه
تاریخ انتشار :
14:45 - 02/06/1398
برچسب:
Public Key Infrastructure - ویندوز سرور 2019 - آموزش ویندوز سرور 2019 - Windows Server 2019 - آموزش جامع ویندوز سرور 2019 - آموزش رایگان ویندوز سرور 2019 - آموزش رایگان Windows Server 2019 - MSC - MMC - گواهینامههای SSL - گواهیهای کامپیوتر

نشانی
https://www.shabakeh-mag.com/networking-technology/15948/%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-%DA%86%D9%87-%D9%86%D9%82%D8%B4%DB%8C-%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-%D8%AF%D8%A7%D8%B1%D9%86%D8%AF%D8%9F