SSL Certificates

Duur: 1 dag **Prijs: € 699**

Open Rooster

Doelgroep Cursus SSL Certificates

De cursus SSL Certificates is bedoeld voor systeem beheerders, security professionals, developers en andere geïnteresseerden die SSL certificates moeten installeren en beheren.

Voorkennis Cursus SSL Certificates

Om aan deze cursus te kunnen deelnemen is algemene kennis van automatisering vereist. Ervaring met security concepten en web applicaties is bevorderlijk voor de begripsvorming maar niet vereist.

Uitvoering Training SSL Certificates

De cursus SSL Certificates heeft een hands-on karakter. De theorie wordt behandeld aan de hand van presentatie slides en wordt afgewisseld met praktische oefeningen. Het cursusmateriaal is Engelstalig. De cursustijden zijn van 9.30 tot 16.30.

Certificering cursus SSL Certificates

De deelnemers krijgen na het goed doorlopen van de training een officieel certificaat SSL Certificates.

Inhoud Cursus SSL Certificates

De cursus SSL Certificates behandelt de theorie en praktijk van SSL certificates die essentieel zijn bij het opzetten van veilige en versleutelde Internet verbindingen. De oorspronkelijke SSL 2 en SSL 3 protocollen zijn inmiddels vervangen door het TLS protocol maar de naam SSL wordt nog steeds gebruikt. Bij SSL heeft de ene kant van de connectie een private key, terwijl een public key beschikbaar wordt gesteld aan anderen die een verbinding willen maken.

SSL Intro

De cursus gaat van start met een bespreking van hoe een SSL verbinding tot stand komt. Aan de orde komt hoe de SSL verbinding start met een handshake tussen client en server. In de eerste stap in de connectie gebruikt de client de public key van de server om een bericht te versleutelen. De server heeft de corresponderende private key en kan het bericht daarmee lezen. Vervolgens wordt een geheime sleutel gegenereerd. Die sleutel is alleen bekend bij zowel de client en als de server en wordt gebruikt bij het onderlinge berichten verkeer.

Encryption Algoritmes

Vervolgens wordt aandacht besteed aan de diverse vormen van encryptie die bij SSL een rol spelen. Bij asymmetrische encryptie hebben weerszijden van de connectie verschillende keys die op elkaar passen en die elkaars berichten kunnen ontcijferen. Bij symmetrische encryptie hebben beide kanten dezelfde key die dan verborgen moet zijn voor de buitenwereld. En bij hash encryptie is er sprake van one way encryptie. Een bericht kan dan niet worden ontcijferd, maar er kan wel gecontroleerd worden of het bericht is veranderd.

SSL Certificates

Ook wordt besproken wat SSL certificates zijn en hoe ze gebruikt worden om een server of een client te identificeren. Uitgelegd wordt welke vormen van certificates er zijn. Hierbij wordt ingegaan op client, server en self-signed certificates en komen ook root certificates en wild card certificates aan de orde. Tevens wordt behandeld hoe je certificates kunt aanmaken of aanvragen en hoe je ze in bekende servers kunt installeren.

Public Key Infrastructure

Erkende certificaten worden verstrekt door certificate authorities als Thawte, Verisign, Let's Encrypt en andere organisaties. Zij gaan na of de aanvrager van een certificaat wel echt is wie hij zegt te zijn en gebruiken daarvoor diverse verificatie methoden. De certificate authorities maken onderdeel uit van de Public Key Infrastructure. Protocollen zoals DANE en DNSSEC komen daarbij ook aan de orde.

Modules Cursus SSL Certificates

Module 1 : SSL Intro	Module 2 : SSL Encryption	Module 3 : Certificates
SSL Overview Secure Sockets Layer (SSL) SSL en TLS SSL Characteristics SSL Handshakes SSL Connectors Configuring SSL Server Name Indication SNI Protocol Key Files Private and Public Key OpenSSL Library	Encryption Algorithms RSA algoritme ECC algoritme SSL Encryption Types Asymmetric Encryption Symmetric Encryption Hash Encryption HTTPS Connections HTTP Strict Transport Security Secure Mime Digital Signing Salt Function	SSL Certificates Creating Certificates CSR's Server Certificates Client Certificates Common Name Root Certificates Wild Card Certificates Subdomains Certificate Revocation List Black and White Listing OCSP and Stapling

Module 4 : PKI Infrastructure
Chain of Trust Certificate Authorities Domain Validation Organization Validation Cipher Suites Handshake CAA Record Configuring CAA DANE Protocol Trust Anchor File Approver DNSSEC Protocol