

# Slecht SSL beheer maakt uw webdiensten onbereikbaar

Auteur: Kick Willemse > Kick Willemse is eigenaar van het bedrijf Evidos, evidence in online services ([www.evidos.nl](http://www.evidos.nl)). Evidos helpt organisaties bij het opzetten van goed certificaatbeheer. Kick Willemse is bereikbaar via e-mail: [K.willemse@evidos.nl](mailto:K.willemse@evidos.nl).

Het niet beschikbaar zijn van uw online diensten kan leiden tot grote schade. De nieuwe versies van de webbrowsers blokkeren uw website en tonen beveiligingswaarschuwingen als u de beveiliging (SSL) niet juist instelt op de website. Meer dan de helft van de website bezoekers haakt af bij beveiligingswaarschuwingen, het goed organiseren en beheren van uw SSL certificaten is essentieel.

SSL staat voor **Secure Sockets Layer** en is de meest gebruikte manier om elektronische transacties via het internet te beveiligen en om internetfraude tegen te gaan.

In de browser verandert uw adres van <http://www.mijnwebsite.nl> naar <https://www.mijnwebsite.nl> en in de browser balk is een slotje terug te vinden.

Een beveiligde website kunt u activeren door een digitaal identiteitsbewijs te installeren op de webserver. Dit identiteitsbewijs wordt ook wel certificaat genoemd en is gebaseerd op versleutelingstechnieken (PKI). In het identiteitsbewijs staan de volgende identificerende gegevens:

- Webadres van de server

- Uitgifte datum
- Verloop datum
- Uitgevende instantie

Bij het bezoeken van een website is het belangrijk dat een browser de volgende controles automatisch uitvoert om fraude te voorkomen:

1. Komt het adres dat de eindgebruiker intypt overeen met het adres in het identiteitsbewijs
2. Is het identiteitsbewijs verlopen
3. Is het identiteitsbewijs uitgegeven door een betrouwbare instantie
4. Is het identiteitsbewijs niet aangemerkt als geblokkeerd

Tot voor kort hanteerde de webbrowsers geen strikte controle op de juistheid van een SSL server certificaat. De website bezoeker kon zonder problemen op uw website terecht ondanks dat het SSL certificaat niet juist was.

Onder druk van de groeiende internetfraude is een werkgroep opgestart door de browserleveranciers en identiteitverstrekkers. Als resultaat zijn de volgende maatregelen genomen:

- Introductie van een EVSSL certificaat
- Eenduidige gebruikerservaring bij het bezoeken van een beveiligde website
- Striktere controles op de juistheid van het identiteitsbewijs van de website

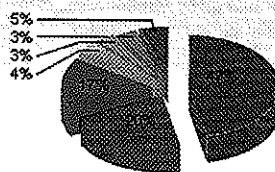
Extended Validation SSL certificaten (EV SSL) zijn de nieuwe internationale standaard op het gebied van SSL beveiliging. EV SSL certificaten worden uitgegeven conform de Extended Validation richtlijn waarin strenge eisen worden gesteld aan de controle van de organisatie die het SSL certificaat aanvraagt en het domein waarvoor het certificaat wordt aangevraagd. De groene adresbalk zorgt er bovendien voor dat bezoekers in één oogopslag zien dat uw website veilig en vertrouwd is.



In het verleden moest de eindgebruiker de aanvullende beveiligingscontroles handmatig aanzetten, in de nieuwste browsers, Internet Explorer 6 en 7, Firefox 3, Opera en Chrome, staan deze strikte controles standaard aan. Deze browsers hebben al een gezamenlijk marktaandeel van 85 procent.

Marktaandeel browsers December 2008  
(Bron: <http://marketshare.hitslink.com/report.aspx?qprid=2>)

Total Market Share

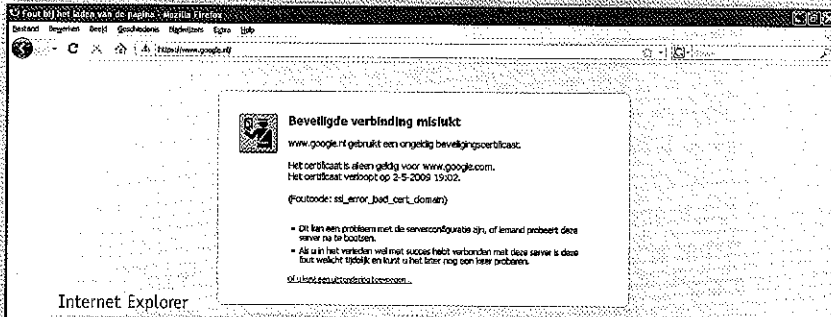


- 46.77% - Microsoft Internet Explorer 7.0
- 20.46% - Microsoft Internet Explorer 6.0
- 17.18% - Firefox 3.0
- 3.77% - Firefox 2.0
- 3.39% - Safari 3.2
- 3.28% - Safari 3.1
- 5.05% - Other

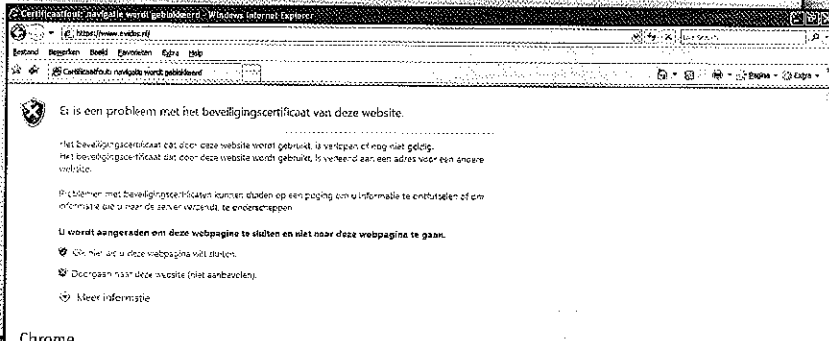
## Wat zien de bezoekers als het SSL certificaat niet juist is?

Voorbeelden:

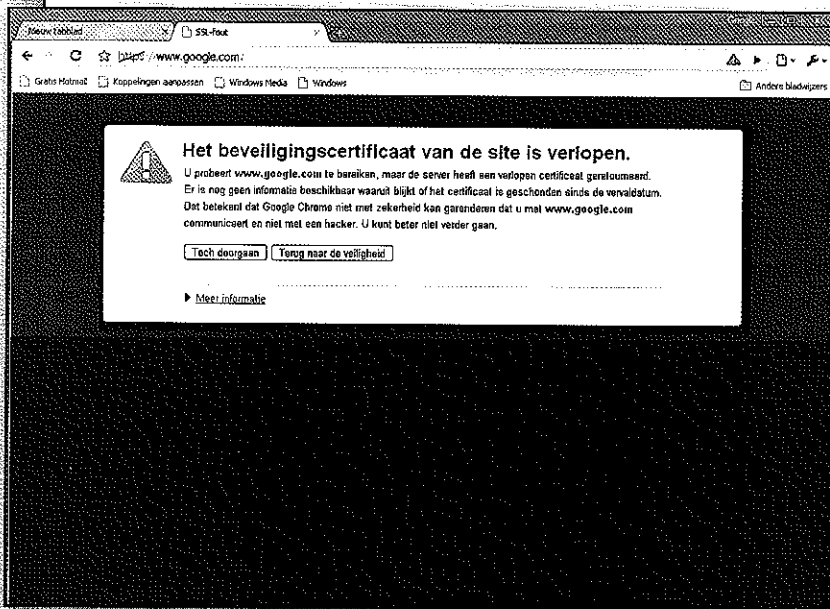
Firefox



Internet Explorer



Chrome



Het is eenvoudig om zelf een test uit te voeren en de problematiek te ervaren. Pas de datum/tijd van uw PC aan door het jaar op 2015 te zetten. Bezoek vervolgens de beveiligde website van uw organisatie of ga naar <https://www.google.com>. Op dit moment zijn er ongeveer 800.000 publiekelijk bekende SSL certificaten in omloop. Verschillende steekproeven wijzen erop dat ongeveer twintig procent van alle beveiligingscertificaten een probleem geeft. Vijftig procent van de website bezoekers haakt af bij beveiligingswaarschuwingen.

## Wat moet ik doen als organisatie?

Na het lezen van dit artikel kunt u direct op zoek naar de SSL certificaten van uw organisatie en controleren of er problemen zijn, vaak ontbreekt het echter aan een duidelijk overzicht. Grotere organisaties beheren vaak wel tientallen certificaten. Bij veel bedrijven is er geen eenduidig certificaatbeleid en vaak is onduidelijk bij wie deze verantwoordelijkheid ligt. Het gebruik van certificaten gaat verder dan alleen SSL certificaten en zal in de toekomst toenemen door toepassingen

als: Webservices security, documenten waarmerken, werkplek toegang en meer websites waar SSL verplicht zal zijn vanuit regelgeving.

Het is belangrijk om de rol voor certificaatbeheer, PKI Officer, goed te beleggen binnen de organisatie.

De taken van een PKI Officer:

1. Centraal verzamelpunt voor het beheren van de verschillende identiteitverstrekkers
2. Duidelijke kennis over welk type certificaat in een bepaald project noodzakelijk is:
  - a. SSL, Handtekening, CodeSigning, Windows login
  - b. Interne CA of Externe CA
  - c. Persoonlijk certificaat of services certificaat
  - d. Gewenste vertrouwensniveau (PKIO, QC)
3. Goed bewaken van de certificaatlevensloop
  - a. Verlooptdatum van het certificaat
  - b. Sleutel lengte
  - c. Geblokkeerde certificaten
  - d. Back-up procedure in geval van calamiteiten
4. Faciliteren van het aanvraagproces
  - a. Aanvragen dient te gebeuren door een bevoegde aanvrager
  - b. Sleutel ceremonie
5. Aanspreekpunt in het geval van security calamiteiten rondom certificaten
  - a. Voorbeelden van dergelijke incidenten in de afgelopen tijd zijn het "MD5 hash collision" en het "Debian bug ssl" Informatie over deze twee incidenten is te vinden via google en bovenstaande termen.
6. Inkoop, duidelijk overzicht van de verschillende leveranciers, mogelijkheden voor raamcontract om zo kosten te besparen.

In veel organisaties zijn de bovenstaande taken versnipperd belegd. De rol PKI Officer zou een goede plek hebben binnen de audit/ quality afdeling. Vaak zie je dat er ook een link is naar de centrale IT afdeling, netwerk services, inkoop of personeelszaken. De manier van inrichten verschilt per organisatie.

Om de continuïteit van uw online dienstverlening te garanderen is het van belang om uw (SSL)certificaatbeheer goed te organiseren.