



Industrieweg 99C
3044 AS Rotterdam
Telefoon: 010 - 714 61 38
Fax: 010 - 462 60 77

De beveiliging van de SSL certificaten van Lancom

Wat zijn SSL certificaten?

Voor het beveiligen van websites en transacties op internet als webmail of VPN is het Secure Sockets Layer protocol de standaard. Dit SSL protocol maakt gebruik van certificaten om de verstuurd data te beveiligen en de identiteit van de eigenaar van het certificaat te garanderen. Door het gebruik van een SSL Certificaat op een website kan een bezoeker er zeker van zijn dat zijn gegevens veilig via https worden verzonden en kan hij eenvoudig de eigenaar van de website controleren.

Veelgestelde vragen naar aanleiding van DigiNotar incident

Naar aanleiding van het DigiNotar incident, waarbij een hacker geslaagd is in het uitgeven van een aantal valse certificaten, zijn de SSL certificaten momenteel volop in het nieuws. Wij krijgen hierover veel vragen waarvan we in dit bericht de meest gestelde vragen willen beantwoorden.

Mocht u verder nog vragen hebben dan horen we deze graag. Wij beantwoorden uw vragen graag.

Vraag 1

Volgens recente nieuwsberichten bleek DigiNotar sleutels (private keys) van klanten te bewaren. Lancom schaft haar certificaten bij een andere organisatie aan dan Diginotar. Bewaart Lancom deze sleutels ook?

Nee, een certificaat maken wij altijd aan op basis van de CSR (Certificate Signing Request). Wij ontvangen nooit de private keys voor klanten en zullen deze voor klanten ook nooit zelf genereren. De private key is strict voor de klant bedoeld en hoort de servers of het netwerk van de klant nooit te verlaten. Een SSL certificaat welke wordt aangemaakt is de zogenaamde publieke sleutel. Deze certificaten of publieke sleutels bewaren wij wel, maar dit vormt geen enkel risico. Publieke sleutels zijn door iedere bezoeker van een website in te zien en is er voor gemaakt om publiek beschikbaar te zijn.

Private Key - Sleutel welke nooit uw eigen netwerk dient te verlaten.

Public Key - Het SSL Certificaat zelf welke door iedereen wordt opgevraagd.

Certificate Signing Request (CSR) - De ongetekende Public Key, bestand waarmee een Certificaat wordt aangevraagd.

Indien de private keys van uw organisatie ooit in handen zijn gekomen van derden, dan raden wij u aan om per direct nieuwe private keys te genereren en hiervoor nieuwe certificaten aan te vragen. Het veilig zijn van de private keys is essentieel voor een beveiligde website; u dient van een CA nooit de private keys te krijgen of de CA deze private keys te sturen.



Industrieweg 99C
3044 AS Rotterdam
Telefoon: 010 - 714 61 38
Fax: 010 - 462 60 77

Vraag 2

Er bleken grote hiaten te zijn in de beveiliging van DigiNotar. Heeft Lancom haar beveiliging op orde?

Lancom neemt haar beveiliging zeer serieus, en doet er al jaren alles aan om haar systemen optimaal te beveiligen. De certificaten worden echter nooit door ons uitgegeven, Lancom is zelf geen CA (degene die certificaten uitgeeft), maar intermediair. Lancom maakt gebruik van externe leveranciers / CA's om de certificaten te genereren.

Beweren dat ons systeem veilig is, is natuurlijk makkelijk en we beseffen dat het voor u als klant lastig is om deze beveiliging te controleren. Om een antwoord te geven op specifieke vragen die we gesteld krijgen, en een indicatie te geven van beveiligingsmaatregelen die wij al jaren hanteren, een kort overzicht van een deel van onze maatregelen:

- Alle servers van Lancom en onze partners zijn volledig up-to-date en voorzien van de benodigde updates en patches en worden dagelijks nagelopen op onregelmatigheden.
- Alle servers zijn geplaatst in een streng beveiligd en professioneel datacenter.
- Alle servers en werkstations zijn voorzien van een up-to-date virusscanner.
- De gehele website van onze partner, inclusief Control Panel is beveiligd met een EV SSL Certificaat.
- Alle logging wordt verstuurd en opgeslagen op een volledig afgeschermd extern geplaatste server.
- Wachtwoorden van klanten worden versleuteld opgeslagen als een zogenaamde salted SHA-256 hash, een manier van bewaren van wachtwoorden waarbij het originele wachtwoord niet meer te achterhalen is.
- Vertrouwelijke gegevens als private keys, logingegevens en kopieën van identiteitsbewijzen worden door ons niet opgeslagen maar onmiddellijk verwijderd.

Lancom is ingeschreven bij de KvK te Rotterdam onder nummer 29044388, op al onze leveringen zijn onze algemene contract en leveringsvoorwaarden van toepassing.