SSL Certifikat: Sikkerhedscertifikatet til din hjemmeside

RESUMÉ

Langt de fleste virksomheder, der har sin egen hjemmeside, vil få gavn af at blive SSL-certificeret. Det mindsker risikoen for kunderne, når de besøger din side gennem kryptering af deres informationer, og det øger troværdigheden af dit domæne, fordi din identitet er bekræftet. Det er relativt hurtigt og nemt at få tilegnet sig, da man med få trin kan få købt og installeret certifikatet. Vælg EV, OV eller DV SSL alt efter autenticitetsniveauet, du ønsker at udstråle, og vælg den udbyder, der giver dig den bedste aftale ud fra dit behov.

I denne artikel lægger vi ud med at beskrive, hvad et SSL certifikat er, og hvorfor din virksomhed bør investere i det. Herefter udpensler vi i en simpel guide bestående af 4 smertefrie trin, hvordan din hjemmeside bliver SSL-certificeret. For de fleste virksomheder, der har en hjemmeside, giver det mening at få et SSL certifikat, men der findes mange udbydere og flere forskellige slags certifikater med forskellige egenskaber. Du bør derfor overveje, hvad din virksomheds behov for SSL er, alt efter om du har en webshop og bearbejder betalingsoplysninger, eller om du har en hjemmeside, der kun lagre mindre personfølsomme oplysninger, som for eksempel e-mail adresser.

Hvad er et SSL certifikat?

SSL står for "Secure Sockets Layer", og certifikatet forsikrer den besøgende om, at din hjemmeside er et sikkert sted at befærde sig på. Overordnet set løser SSL-certifikatet to tekniske opgaver:

› **Kryptering af information:** Du undgår, at uvedkommende kan opfange de informationer, som en besøgende udleverer til din side, og bruger til andre formål, end det tiltænkte. Krypteringen gør, at et forsøg herpå blot vil afgive uforståelige tal og bogstaver, og ikke dine kunders personlige oplysninger, som kun er forbeholdt afsender og modtager.

› **Bekræftelse af din virksomheds identitet:** Da SSL-certifikatet også inkluderer informationer om hjemmesiden, der besøges, kan kunden derved verificere, at de har besøgt netop din hjemmeside, og ikke en falsk hjemmeside lavet af nogen, der giver sig ud for at være din virksomhed.

Hvis ikke du har et SSL certifikat, svarer det til, at man som kunde skriver sine oplysninger ude på konvolutten, og sender den afsted uden at være 100 % sikker på, at du er legitim, og uden at være sikker på, at andre ikke læser dem på vejen til dig. Med SSL er oplysningerne skrevet inde i konvolutten med en hængelås på, og der er ikke tvivl om, at den bliver sendt til den tiltænkte modtager[1].

Det er derfor relevant for langt de fleste virksomheder med en hjemmeside, og det er definitivt et 'must' for virksomheder, der ejer en webshop. Få i øvrigt altid din hjemmeside e-mærket, hvis du ejer en webshop.

Følg fire enkle trin, og bliv SSL-certificeret!

Heldigvis er det ikke særlig svært at få din virksomheds hjemmeside SSL-certificeret. Ved at følge nedenstående fire trin, kan du få certifikatet allerede i dag.

Trin 1: Få styr på IP-adressen
Før du køber dit SSL-certifikat, skal du undersøge, om din IP-adresse understøtter muligheden for at implementere sikkerhedscertifikatet. Hvis du bruger en mindre web host

udbyder, vil du med basispakken i mange tilfælde få tildelt en såkaldt "delt" IP adresse, hvilket betyder, at dit domæne er forbundet til en overordnet adresse, der er delt mellem adskillige domæner. Hvis ikke din IP adresse er delt, så er den dedikeret, hvilket vil sige, at dit domæne har en hel adresse for sig selv. Men hvad betyder det i praksis for muligheden for SSL, og hvad behøver du at gøre?

Dedikeret IP-adresse vs. delt IP-adresse

Før i tiden var det et krav, at du havde en dedikeret IP-adresse, hvis du gerne ville blive SSL-certificeret. Sidenhen er SNI, Server Name Identification (Server navn identificering på dansk), blevet udviklet, og det har for langt de fleste løst det problem. Basalt set sikrer SNI, at du kan få flere SSL-certifikater på en enkel IP-adresse, og derved kan du selv med en delt adresse få "HTTPS" bag dit domænenavn. Undtagelsen er her, hvis du med din web host bruger Internet Explorer på Windows XP eller en Android browser på Android 1.x eller 2.x. Det er der dog kun under 2 % af markedet, der gør[2]. Derfor vil du med al sandsynlighed have styr på dette trin, uden du behøver at foretage dig noget som helst. Hvis du alligevel er en af de få, der har behov for en dedikeret IP adresse for at få SSL-certifikatet, kan du med din nuværende web host købe en opgradering, som enten vil koste et engangsbeløb eller et mindre månedligt gebyr.

Trin 2: Køb certifikatet

Når du skal købe dit SSL certifikat, findes der mange forskellige udbydere, du kan vælge imellem. Her bør du vælge ud fra pris og ud fra hvilken type certifikat, du har behov for. Overordnet set findes der tre forskellige SSL-certifikater, du kan vælge imellem: EV SSL, OV SSL og DV SSL.

Alle tre type certifikater tilbyder samme krypteringsniveau, så ud fra sikkerheden af dine kunders oplysninger, er der ingen merværdi at hente ved den ene type fremfor den anden. Det, der adskiller dem, er hvor meget de gør ud af at bekræfte din identitet, hvilket er relevant for din hjemmesides troværdighed[3].

EV SSL: Det står for "Extended validated SSL". Dette er det mest troværdige SSL-certifikat, du kan have, da udstederen verificerer alt fra rettigheder til din virksomheds eksistensgrundlag og meget andet. Hvis du køber et EV SSL, vil det fremgå i URL-adressen ved, at dit domænenavn står i "baren" til venstre for HTTPS, hvor fonten iblandt vil være grøn. Dette anbefales for virksomheder, der ønsker at fremstå med den allerhøjest mulige autenticitet.

Fx:
OPR-Finance ApS [DK] https://opr-virksomhedslån.dk/

OV SSL: Det står for "Organization Validated SSL". Her verificeres rettigheden til domænet samt nogle grundlæggende oplysninger om din organisation, og din virksomhed fremstår derfor også meget troværdigt. I nogle browsere, som Chrome, vil man se en lås til venstre for HTTPS, og fonten vil i nogle tilfælde være grøn. I andre browsere, som Internet Explorer, vil man ikke se nogen lås, men der står stadig "HTTPS" foran dit domænenavn. Virksomheder, der modtager meget personfølsomme oplysninger, som f.eks. CPR-nummer og betalingsoplysninger, herunder webshops, bør som minimum overveje et OV SSL.

DV SSL: Det står for "Domain Validated SSL". Her tjekkes der udelukkende for, om du har rettighederne til at bruge domænenavnet, og intet andet om din virksomhed. I URL-linjen fremstår certifikatet på samme måde som et OV SSL, og fordelen her er, at det både er billigere og hurtigere at få end to andre, da du ikke skal indsende dokumenter om din virksomhed. Dette vil sandsynligvis egne sig til virksomheder, som kun bearbejder mindre sensitive personlige oplysninger som f.eks. e-mails, navne e.l.

Brug lidt tid på at overveje, hvilken form for SSL-certifikat, der er bedst for din virksomhed, og kig nogle forskellige udbydere igennem for at finde det bedste tilbud for dig.

Liste over nogle kendte udbydere:

› https://chosting.dk/da/ssl/
› https://www.rapidssl.com/europe/index.html
› https://www.namecheap.com/security/
› https://billigssl.dk/
› https://www.gogetssl.com/ssl-certificates/
› https://www.geotrust.com/ssl/
› https://www.websecurity.symantec.com/ssl-certificate
› https://www.alphassl.com/
› https://www.globalsign.com/en/ssl/
› https://www.fairssl.dk/da/

Trin 3: Aktiver certifikatet

Efter at du har købt dit SSL-certifikat, skal det aktiveres. I nogle tilfælde gør din web host det helt automatisk, så før du gør noget, bør du kontakte dem og høre dem ad. Hvis du selv skal stå for aktiveringen, skal du generere et SSL CSR: "SSL Certificate and Signing Request". Det gør du ved at gå ind i kontrolpanelet på din web host, hvorefter du skal klikke på et SSL/TLS admin area. Herinde vælger du "generer et SSL CSR", hvorefter du udfylder de påkrævede informationer.

Hvis der opstår tvivl undervejs i dette trin, anbefaler vi, at du kontakter din web host for yderligere hjælp.

Trin 4: Installer certifikatet.

Efter aktiveringen skal du installere certifikatet. Dette trin kan ligesom trin 3 i nogle tilfælde blive gjort helt automatisk af din web host. Hvis du selv skal gøre det manuelt, er det meget lige til, da der i kontrolpanelet (typisk lige nedenunder "genererer SSL CSR") vil være en "installer certifikatet" knap. Når du klikker på den knap, skal du blot indsætte dit certifikat, og derefter er du certificeret!

Gør dig selv og dine kunder en tjeneste

Med tanke på de mange fordele, der hører til en SSL-certificering, mener vi, at alle virksomheder burde købe certifikatet. Internettet bliver en stadigt større markedsplads, og uden den rette sikkerhed for din hjemmeside, kan du, udover at bringe dine kunders privatliv i fare, miste en masse potentielle kunder, der ikke har tiltro til din online tilstedeværelse, hvilket kan gøre ondt på bundlinjen.

Få yderligere inspiration om hjemmesider i:

› Design din hjemmeside: Vigtigheden af en god hjemmeside
› Lav din egen hjemmeside: det er nemmere end du tror

Eller bliv klogere på hvordan du analyserer og laver SEO til din hjemmeside ved at læse:

› SEO Guide: Lær SEO og få mere hjemmesidetrafik
› Analyse af hjemmeside: Google Analytics hjælper dig med at forstå dit firma

Overvejer du at starte en webshop, så læs med her:

› E-handel: Kan mindre webshops etablere sig i det danske marked?
› Lav din egen webshop: Find den rigtige udbyder (del 1)

Kilder:

1) https://www.fairssl.dk/da/ssl-information/what-is-an-ssl-certificate/
2) https://kinsta.com/blog/dedicated-ip-address/#
3) https://www.globalsign.com/en/ssl-information-center/types-of-ssl-certificate/
4) https://www.computerworld.dk/art/231741/guide-saadan-goer-du-din-hjemmeside-sikker-med-https