

VIRKSOMHEDSKONTINUITET OG BESKYTTELSE  
MOD BRUD PÅ DATASIKKERHEDEN: HVORFOR  
ADMINISTRATION AF SSL-CERTIFIKATER ER  
VIGTIG FOR DAGENS VIRKSOMHEDER

## Hvidbog

Virksomhedskontinuitet og beskyttelse mod brud på datasikkerheden: Hvorfor administration af SSL-certifikater er vigtig for dagens virksomheder

## Virksomhedskontinuitet og beskyttelse mod brud på datasikkerheden: Hvorfor administration af SSL-certifikater er vigtig for dagens virksomheder

### Indhold

<b>Indledning</b> . . . . .	<b>3</b>
<b>Udfordringer ved administration af SSL-certifikater</b> . . . . .	<b>3</b>
<b>Farerne ved udløbne og defekte SSL-certifikater</b> . . . . .	<b>4</b>
Tyveri af kundedata . . . . .	4
Mister kunder til konkurrenter . . . . .	6
Flere henvendelser til kundesupport. . . . .	6
Øget belastning af it-afdelinger. . . . .	6
<b>Best Practices ved administration af SSL-certifikater</b> . . . . .	<b>7</b>
<b>Konklusion</b> . . . . .	<b>8</b>
<b>Symantec® Certificate Intelligence Center: Robust opdagelse og administration af SSL</b> . . . . .	<b>8</b>

## Indledning

SSL-certifikater har været anvendt i næsten 15 år, og de spiller fortsat en afgørende rolle ved beskyttelse af data, når de overføres på tværs af internettet og andre netværk. Fra online finansielle transaktioner til e-handle og produktudvikling gør SSL-certifikater det muligt for brugere verden over trygt at overføre følsomme oplysninger, som er beskyttet mod ondsindede hackere.

De sidste 30 år har internettet udviklet sig på utallige måder. Hvorfor giver SSL-certifikater stadig tryghed? Den enkle forklaring er, at SSL-certifikater er uhyre effektive til at beskytte data under overførsel. Faktisk viser nogle beregninger, at det vil tage ca. seks tusinde milliarder år - eller ca. en million gange længere end jorden har eksisteret - at bryde den 128-bit kryptering i SSL-certifikater ved hjælp af rå vold.<sup>1</sup> Selv i den situation sker der en fortsat udvikling i sikkerhedsbranchen, og mange certifikatudstedende myndigheder er begyndt at indføre 2048-bit kryptering i deres SSL-certifikater, hvilket yderligere styrker beskyttelsen af online datakommunikation.

Alligevel står kunders overførsel af data på websteder og systemer, der er beskyttet med SSL, stadig over for alvorlige trusler. En af hovedårsagerne til denne fare er dårlig administration af SSL-certifikater. Virksomheder med hundreder af SSL-certifikater fra forskellige leverandører kan miste overblikket over certifikaterne i deres miljø. Når det sker, kan certifikater udløbe, og der kan gå flere måneder, før det opdages, hvilket gør besøgende på webstedet sårbare over for hackere.

Somme tider er det første tegn på, at der er "mistet" et SSL-certifikat, at en kunde, der har bemærket et udløbet certifikat, spørger, om der nu også er sikkert at handle på webstedet. Andre gange kan det være alvorligere, som eksempelvis en phishinghændelse, hvor cyberkriminelle har fået mulighed for at stjæle følsomme kundedata. Eller et brud på datasikkerheden hos en certifikatudstedende myndighed kan give problemer for en virksomhed, fordi den ikke kan reagere hurtigt på grund af manglende indblik i sine SSL-certifikater.

Uanset årsagen kan et manglende overblik over SSL-certifikater medføre betydelige økonomiske tab og skader på omdømmet. Heldigvis behøver administration af SSL-certifikater i en virksomhed ikke at være kompliceret eller langsommelig.

Denne hvidbog fortæller om faldgruberne i forbindelse med dårlig administration af SSL-certifikater, hvorfor det er potentielt farligt for virksomheden, og hvordan store virksomheder effektivt kan fastholde overblikket over SSL-certifikater.

## Udfordringer ved administration af SSL-certifikater

Store virksomheder har i dag komplicerede miljøer, der ofte indeholder flere interne netværk og websteder, der er rettet mod offentligheden. Derfor kan en virksomhed på et givet tidspunkt benytte snesevis, eller måske endda flere hundrede forskellige SSL-certifikater.

1. <http://www.inet2000.com/public/encryption.htm>

Ud over mange SSL-certifikater benytter mange store virksomheder en blanding af forskellige certifikater fra forskellige certifikatudstedere. En stor virksomhed kan f.eks. installere SSL-certifikater fra en velkendt og pålidelig leverandør på de websteder, der er rettet mod offentligheden, og specielle certifikater på sit intranet, som virksomheden eventuelt selv har udviklet.

Selv om mange certifikatudstedere tilbyder onlineværktøjer til administration af deres certifikater, kan disse værktøjer ofte ikke give indblik i alle certifikater fra forskellige udbydere på tværs af et miljø. I stedet for at lette administrationen gør flere administrationsportaler det vanskeligere at holde overblik over utallige SSL-certifikater i et miljø med forskellige certifikatudstedere. Administratorer skal hele tiden overvåge deres SSL-certifikater via forskellige systemer og lave deres egne rapporter for at få en samlet overblik over alle deres SSL-certifikater.

For at komplicere tingene kan virksomheder med distribuerede netværk have sikkerhedspolitikker, der varierer fra gruppe til gruppe. Det betyder, at gruppe A kan have Extended Validation SSL-certifikater til at beskytte de data, den administrerer, mens gruppe B bruger en anden type SSL-certifikater fra en anden udsteder. Eller det kan blive mere udbredt, at gruppe A har behov for 2048-bit SSL-certifikater, mens gruppe B anvender 1024-bit certifikater. Med forskellige politikker og ingen enkel måde aft opnå et samlet overblik over SSL-certifikater på tværs af en stor virksomhed, kan disse manglende sammenhænge medføre sikkerhedsfarer og manglende compliance med virksomhedens og myndigheders krav til politikker.

Overvej også, hvad der vil ske, hvis den person, der er ansvarlig for administrationen af SSL-sikkerheden, skifter rolle eller forlader virksomheden. Hvis de ikke omhyggeligt dokumenterer, hvilke certifikater de administrerer - og videregiver disse oplysninger til andre i teamet - kan disse SSL-certifikater blive glemt, når en ny medarbejder overtager opgaven. Da store virksomheders it-team har travlt og ofte har for få ressourcer, vil manuel sporing af SSL-certifikater ikke blot være en byrde, men kan også let være behæftet med menneskelige fejl.

Alle disse faktorer bidrager til et miljø, hvor SSL-certifikater kan blive væk eller overset. I en stor virksomhed vil et sådant miljø kunne medføre nedbrud og skabe sikkerhedsrisici for kunderne.

### **Farerne ved udløbne og defekte SSL-certifikater**

Et udløbet eller defekt SSL-certifikat i et netværksmiljø kan få alvorlige konsekvenser. Det kræver kun ét forældet eller defekt certifikat for at eksponere virksomheden - og måske endnu vigtigere dens kunder - for skadelig cyberkriminalitet. Det følgende er blot nogle af de mulige konsekvenser af et udløbet eller defekt SSL-certifikat.

#### **Tyveri af kundedata**

Takket være mange års avisoverskrifter om brud på datasikkerheden og påvisning fra forbrugertalsmænd og virksomheder, er offentligheden blevet stadig mere bekymret for identitetstyveri. En nyere undersøgelse viste, at 64 % af amerikanere

er meget eller virkelig meget bekymret for, at nogen stjæler deres identitet, mens 31 % beskriver sig som ekstremt bekymret.<sup>2</sup>

I denne sammenhæng er faren for phishing en stor bekymring. Ved et phishingangreb vil en hacker forklæde sig som en legitim virksomhed - og udnytte virksomheders manglende sikring af ægthed med ikke-eksisterende eller udløbne SSL-certifikater - og oprette et falsk websted, der ligner eller er helt identisk med det ægte websted. Godtroende kunder vil derefter indtaste fortrolige oplysninger, som for eksempel kreditkortoplysninger eller CPR-nummer på websiden. Phishingsiden overfører dataene direkte til hackeren, som derefter kan sælge dem videre til andre kriminelle.

Selv hvis en phishinghændelse eller et brud på datasikkerheden er relativt lille, kan det skærpe frygten og alvorligt true virksomheden.

Ud over disse umiddelbare tab kan phishing og brud på datasikkerheden også påvirke en stor virksomheds omdømme og medføre, at både nuværende og potentielle kunder stiller spørgsmål ved, om den pågældende virksomhed er troværdig. Ekspert i branchen siger, at det tager ca. 6 måneder at stabilisere salg og tillid til en virksomheds netværk efter et brud på datasikkerheden<sup>3</sup> - og selv da kan en virksomheds omdømme meget vel endnu ikke været helt gendannet.

### De voksende omkostninger ved brud på datasikkerheden

Selvom det kan være svært at måle skaderne på en virksomheds omdømme, er det let at se de økonomiske konsekvenser ved et brud på datasikkerheden. En nyere amerikansk undersøgelse viser, at den gennemsnitlige omkostning ved et brud på datasikkerheden er \$ 7,2 millioner pr. hændelse eller ca. \$ 214 pr. kompromitteret post,<sup>4</sup> og det er tal, der forventes fortsat at ville stige.



Konsekvenser ved uventet SSL-udløb og browseradvarsler

2. "Identity theft fears weigh on Americans," af Tim Greene, Network World, 4/12/2010

3. "Sony Data Breach Exposes Users to Years of Identity-Theft Risk," af Cliff Edwards og Michael Riley, BusinessWeek.com, 5/3/11

4. "Cost of a data breach climbs higher," Ponemon Institute, ponemon.org, 3/8/11

### Mister kunder til konkurrenter

Udløbne SSL-certifikater er en anden ting, der bekymrer virksomheder. Et udløbet SSL-certifikat kan på andre måder medføre mistet salg. Hovedårsagen hertil er, at kunderne ser advarsler om udløb af SSL-certifikaert, hvorefter de går ud af dit websted og i stedet køber produkter og tjenester på websteder, der er beskyttet med SSL-certifikater.

Kunderne er måske ikke klar over, hvordan kryptering med offentlig nøgle fungerer, men synlige tegn på SSL-sikkerhed - som et SSL trust-segl eller den grønne Extended Validation-bjælke - øger sandsynligheden for, at de køber noget på et bestemt websted.<sup>5</sup> Hvis SSL-certifikater på e-handels- eller andre typer websteder, der er rettet mod offentligheden, udløber, vil de miste kundernes tillid og miste salg.

### Flere henvendelser til kundesupport

I dag tilbyder mange virksomheder webværktøjer, automatiske telefonmenuer og andre selvbetjeningsmuligheder for at gøre det lettere for kunder, der har spørgsmål til, hvordan de finder de oplysninger, de har brug for. Men hvis kunder besøger et websted og er i tvivl om, hvorvidt deres personlige data er sikret, vil de enten opgive deres køb (som omtalt ovenfor) eller også ringer de til kundesupport.

Gennemsnitsprisen pr. supportopkald variere mellem brancher, men en ting er sikker: Omkostningerne ved utallige supportopkald løber op. Ikke alene går de ekstra supportopkald ud over virksomhedens økonomi, de giver en ekstra belastning af kontaktcenteret og forhindrer supportmedarbejdere i at behandle andre vigtigt kundefølgende henvendelser.

De ekstra omkostninger og besværet i forbindelse med kundefølgende henvendelser kan nemt undgås ved at vedligeholde en opdateret sikkerhed, herunder gyldige SSL-certifikater.

### Øget belastning af it-afdelinger

På samme måde som kunder, der ringer til kundesupport, når de ikke er sikre på et websteds sikkerhed, vil ansatte, som ser advarsler, der stammer fra udløbne SSL-certifikater på intranettet eller andre interne websteder, ofte kontakte en it-medarbejder for at få løst problemet. Det kan give en betydelig belastning af it-afdelinger, der allerede er overbelastet.

I andre tilfælde kan ansatte helt ignorere disse advarsler om udløb, hvilket gør, at den pågældende ressource fortsat er sårbar over for angreb. Det har samtidig en negativ indflydelse på overholdelsen af sikkerhedsregler, fordi det giver indtryk af, at medarbejderne forsømmer interne sikkerhedsforanstaltninger.

Begge disse situationer kan undgås med opdaterede SSL-certifikater på tværs af hele virksomheden.

---

5. <http://www.verisign.dk/ssl/ssl-information-center/ecommerce-trust-ssl/>

## Best Practices ved administration af SSL-certifikater

Heldigvis findes der tjenester, der gør det nemt at opdage og administrere SSL-certifikater på tværs af virksomheden. Nogle løsninger påstår, at de letter besværet ved administration af SSL, selv om de ikke giver dig mulighed for at opdage certifikater fra forskellige udstedere. Andre løsninger kan tilbyde scanning efter forskellige certifikatudbydere, men mangler en intuitiv og brugervenlig brugergrænseflade.

For at hjælpe med at sikre, at du finder den løsning, der passer bedst til dine behov, er der her nogle hovedfunktioner, du skal kigge efter, når du overvejer en løsning:

- **Mulighed for at scanne dit miljø automatisk:** Selv om det er muligt at kontrollere netværk manuelt, tager det for lang tid og kræver for mange medarbejderressourcer til at kunne lade sig gøre i store, komplekse virksomhedsmiljøer. Sørg for at vælge en tjeneste, der giver dit team mulighed for automatiske scanninger, der vil opdage SSL-certifikater fra alle leverandører.
- **Brugervenlig grænseflade:** Svært tilgængelige eller forståelige data duer ikke, så se efter et værktøj med et betjeningspanel, som er nemt at navigere rundt i, og som præsenterer data på en let forståelig og overskuelig måde.
- **Funktioner til uddelegering:** I store virksomheders miljøer er der flere medarbejdere, der administrerer sikkerheden. Derfor er det vigtigt at finde en løsning til at opdage certifikater, hvor administratorer kan give forskellige grader af adgang og kan delegerer opgaver til forskellige medarbejdere på tværs af netværket.
- **Alarmer og rapportering:** Et udløbet SSL-certifikat bringer data i fare, hvorfor det er vigtigt at finde en tjeneste, der alarmerer, før et certifikat skal fornyes. Desuden er det vigtigt med en løsning, hvor det er let at læse og forstå rapporter. Avancerede rapporteringsfunktioner vil ikke alene give en grundig og omfattende oversigt over netværkets certifikater, men vil også give dit team mulighed for effektivt at sende vigtige oplysninger til andre medarbejdere, herunder ledere.
- **Fleksibilitet og skalerbarhed:** Store virksomheders netværk er dynamiske og ændrer sig hele tiden, hvilket medfører, at tjenester til opdagelse af certifikater skal have indstillinger for scanningsvarighed, hvilke IP-adresser der skal scannes osv. Desuden skal tjenesten være skalerbar for at tage højde for fremtidig vækst.
- **Hurtighed:** For at være effektive skal netværksscanninger kunne gennemføres hurtigt. Hvis det tager for lang tid at scanne et helt netværk, kan status for nogle af SSL-certifikaterne have ændret sig, før hele scanningen er gennemført. Det vil medføre et upræcist overblik over SSL-certifikaterne.

## Konklusion

SSL-certifikater er vigtige for beskyttelsen af data under overførsel. På trods af sin styrke og pålidelighed kan SSL-sikkerhed stadig være sårbar over for angreb af en enkel årsag: Dårlig administration af SSL-certifikater.

I et miljø med flere certifikater fra forskellige udstedere er det afgørende at have et samlet overblik over SSL-sikkerheden. At kende status for alle certifikater på tværs af websteder og netværk kan ikke alene hjælpe med at kontrollere omkostninger til kundeservice, men også lette belastningen ved administration af SSL og give travle it-team mere tid til at koncentrere sig om projekter, der er vigtige for virksomheden.

Omhyggelig administration af SSL kan også forhindre langt alvorligere ting, som for eksempel større phishinghændelser og andre typer brud på datasikkerheden, der ikke alene kan være dyre at afhjælpe, men også kan medføre langsigtede skader på dit omdømme over for dine kunder.

## Symantec® Certificate Intelligence Center: Robust opdagelse og administration af SSL

Symantec Certificate Intelligence Center hjælper administratorer til en mere effektiv opdagelse og administration af SSL-certifikater. Symantec Certificate Intelligence Center, der giver dybt indblik og administrationsfunktioner, gør det nemt at have et overblik over SSL-certifikater.

Symantec Certificate Intelligence Center har en intuitiv grænseflade, hvor administratorer kan oprette automatiske scanninger, der hurtigt opdager certifikater fra enhver udsteder. Brugere kan også opsætte alarmer, der proaktivt advarer SSL-administratorer, når certifikater er ved at udløbe.



*Symantec Certificate Intelligence Center har et brugervenligt betjeningspanel*

Symantec Certificate Intelligence Center, der er nemt at skalere, tager højde for hurtige ændringer i netværket, når virksomheder ændrer behov og vokser. Avancerede rapporteringsfunktioner giver desuden administratorer et samlet overblik over SSL-sikkerheden, der er nemt at forstå og kan kommunikeres videre i virksomheden.

Hvis du ønsker flere oplysninger om, hvordan Symantec Certificate Intelligence Center kan hjælpe dig med at forenkle opdagelse og administration af SSL-certifikater, skal du besøge:

<http://www.verisign.dk/ssl/symantec-certificate-intelligence-center/index.html>

## Flere oplysninger

Besøg vores websted

<http://www.verisign.dk>

## Hvis du vil tale med en produktspecialist

80 88 29 78

+45 88 61 01 10

## Om Symantec

Symantec er en af verdens førende leverandører af løsninger til sikkerhed, lager og systemadministration, der hjælper forbrugere og virksomheder med at sikre og administrere deres datadrevne verden. Vores software og serviceydelser beskytter mod flere risici på flere steder og på en mere omfattende og effektivt måde for at sikre tryghed overalt, hvor data bruges eller opbevares. Hovedkontoret ligger i Mountain View, Californien, men Symantec har afdelinger i 40 lande. Yderligere oplysninger findes på [www.symantec.com](http://www.symantec.com)

## Symantec Denmark ApS

Lyngbyvej 20,  
2100 København,  
Danmark

