



RAPPORT

SIKKERHED OG TILLID – GRUNDLAGET FOR AL E-HANDEL



RAPPORT

INDHOLD

- 3 INDLEDNING
- 3 KRYPTERINGSTEKNOLOGI OG SSL-CERTIFIKATER
- 6 VERISIGN® SEAL-IN-SEARCH™ SIGNALERER SIKKERHED FRA STARTEN
- 6 SSL MED EXTENDED VALIDATION (EV) GIVER KUNDETILLID
- 7 VERISIGN - MARKEDETS FØRENDE LEVERANDØR AF NETSIKKERHED OG TILLID
- 8 KONKLUSION
- 8 FÅ MERE AT VIDE
- 8 OM VERISIGN



SIKKERHED OG TILLID – GRUNDLAGET FOR AL E-HANDEL

INDLEDNING

At vinde kundernes tillid på internettet er afgørende for ethvert firma, som har brug for at sende og modtage følsomme data på internettet. Forbrugere på nettet er meget bekymret for bl.a. identitetstyper og er forståeligt nok tilbageholdende med at udlevere personlige oplysninger på websteder, de ikke har tillid til. Oplysningerne er typisk kreditkortoplysninger, cpr-nummer, adgangskoder, helbredsoplysninger og andre fortrolige data. Bekymringen går på, om sådanne følsomme oplysninger bliver opsnappet undervejs, eller om der står svindlere bag det pågældende websted.

Konsekvensen er, at mange vælger ikke at gennemføre handler, de ellers er i gang med, og det er gift for al e-handel. Et studie¹ i Danmark og Sverige viser at forbrugernes bekymringer vedrørende onlinesikkerheden afholder potentielle kunder fra at handle på nettet.

Og frygten er velbegrunderet. Millioner af phishing-URL'er blev indberettet i 2008. Og antallet af globale phishing-angreb steg med utrolige 66 procent sammenlignet med 2007, i tal omregnet til 135.426 enkeltstående hændelser ifølge en undersøgelse fra RSA Security.²

Netbutikker har rigtig meget at vinde ved at tage skridt til at få kundernes frygt bilagt. Bekymringen for svindel på internettet er en stor hindring for e-handel. Ifølge et studie er 65 procent af europæiske forbrugere bekymrede for at miste private data online.³ Fordi frygten for svindel på nettet ikke blot begrænser antallet, men også beløbsstørrelsen af transaktioner, kan der opnås et betydeligt potentielt mersalg ved at arbejde med kundetillid. Der er også fordele at hente for forbrugerne. Som forbruger er der ikke noget så praktisk og billigt som at handle på nettet. Forbrugere tjekker ofte flere websteder for en bestemt vare – både dem, de har tillid til og dem, de ikke har tillid til. Muligheden for at shoppe rundt på en lang række websteder, som forbrugerne kan have tillid til, giver dem ikke bare mulighed for at finde den ønskede vare, men også for at de trygt kan udlevere deres personlige oplysninger.

Heldigvis er der teknologi til rådighed til at hjælpe netbutikker med at beskytte følsomme kundedata og med at sikkerhedsgodkende deres websteder og opnå kundernes tillid. Teknologi, der hjælper kunderne med at kende forskel på sikre websteder og på falske, hvor der står svindlere bag.

I denne rapport redegør vi for den nuværende situation for netsikkerheden på websteder, og hvordan VeriSign hjælper firmaer med at beskytte fortrolige oplysninger og skabe kundetillid. For det første er der SSL-kryptering (Secure Sockets Layer), som tager sig af det mest oplagte og længst eksisterende problem inden for e-handel, nemlig risikoen for at internetkriminelle opsnapper forbrugernes følsomme data. Her i rapporten ser vi på behovet for den datakryptering, som opnås med SSL – og behovet for yderligere foranstaltninger, som f.eks. autentificering af et websteds identitet og opbygning af tillid hos et firmas kunder.

KRYPTERINGSTEKNOLOGI OG SSL-CERTIFIKATER

Kunderne ved, at det er risikabelt at udlevere personlige oplysninger på websteder, som ikke har ordentlig netsikkerhed. For at overleve på markedet er netbutikker nødt til at anskaffe SSL-certifikater til at kryptere og beskytte følsomme kundeoplysninger.

Ved kryptering omdannes data, så de er uforståelige for alle undtagen den modtager, som de er tiltænkt. Det er grundlaget for at opretholde den dataintegritet og fortrolighed, som er nødvendig for al e-handel. Kunder og forretningspartnere vil kun sende følsomme oplysninger og foretage transaktioner på websteder, når de har tillid til, at det kan ske sikkert. Løsningen for seriøse e-handelsfirmaer er at implementere en netsikker infrastruktur baseret på krypteringsteknologi.

SSL (Secure Sockets Layer) er den globale standard for netsikkerhed, som anvendes til at kryptere og beskytte oplysninger, der sendes over internettet, ved hjælp af den allestedsnærværende HTTP-protokol. Ved overførsel beskytter SSL data ved hjælp af kryptering mod opspionage

1. "VeriSign 2009 Brand Research," Synovate/GMI, May 2009

2. RSA Security Report, December 2008. Kan downloades på http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_1208.pdf (På engelsk).

3. "Data Loss is Europe-Wide Problem Says EU Expert," SC Magazine, October 2008. Kan downloades på <http://www.scmagazineuk.com/Data-loss-is-Europe-wide-problem-says-EU-expert/article/119969/> (På engelsk).



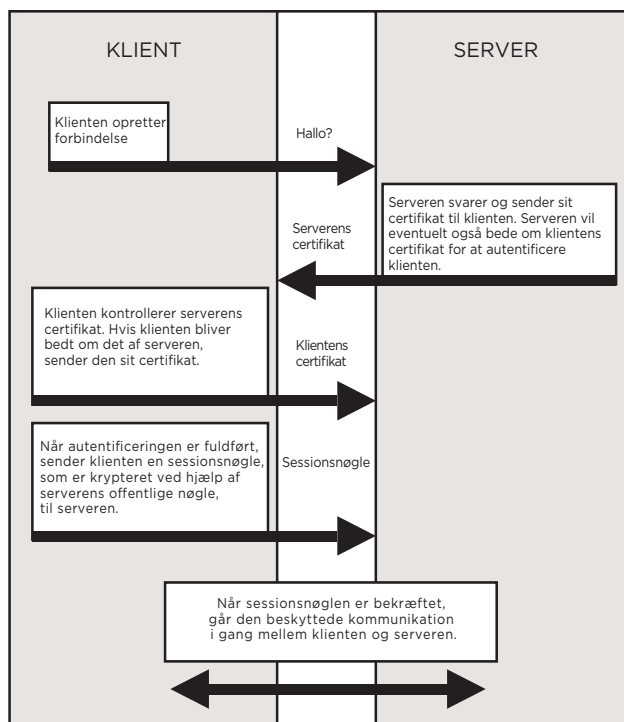


RAPPORT

og manipulation. Alle populære operativsystemer, webbrowsere, internetprogrammer og servere understøtter SSL.

Et SSL-certifikat er en elektronisk fil, som identificerer individuelle personer og websteder, og som krypterer kommunikation. SSL-certifikater svarer til et "digitalt pas" eller legitimationsoplysninger. Udstederen af et SSL-certifikat er typisk et certificeringscenter, som er en tredjepartsleverandør. VeriSign er verdens førende certificeringscenter, som beskytter mere end 1 mio. webservere på verdensplan.⁴

I diagrammet nedenfor ses processen, som garanterer sikker kommunikation mellem en webserver og en klient. Alle SSL-certifikatudvekslinger sker på få sekunder, uden at forbrugeren skal foretage sig noget.



Krypteringsniveauer og SGC

Datakryptering findes på forskellige niveauer afhængig af det antal bit, der anvendes i krypteringsalgoritmen. Den nuværende minimumstandard er 128 bit, hvilket i enhver henseende anses for at være umuligt at hacke ved de nuværende computerhastigheder. Bestemte ældre versioner af nogle operativsystemer og browsere (i bestemte kombinationer) understøtter højst 40- eller 56-bit kryptering. Kryptering på disse lavere niveauer er nem at hacke, hvilket gør brugere af disse operativsystem- og browserkombinationer sårbare over for angreb.

SGC-teknologien (Server-Gated Cryptography), som indgår i bestemte VeriSign SSL-certifikater, løser dette problem for 99,9% af webstedsbesøgendes vedkommende. Websteder, som har SGC, "opgraderer" kommunikationen med systemer, der normalt kun kan fungere med 40- eller 56-bit kryptering, til 128-bit kryptering.* Derfor kan firmaer med SGC SSL-certifikater garantere et tilstrækkeligt krypteringsniveau for alle sine kunder. VeriSign Secure Site Pro og Secure Site Pro med EV understøtter SGC 128-bit kryptering. Alle VeriSign SSL-certifikater understøtter op til 256-bit kryptering af alle forbindelser, så både klienten og serveren er i stand til at kryptere på dette niveau.

* Brugere med nedenstående browserversioner og operativsystemer er automatisk omfattet af 128-bit SSL-kryptering, når de besøger et websted, som har et SSL-certifikat med SGC: Versioner af Internet Explorer-"eksportbrowsere" fra og med 3.02 men før 5.5. Versioner af Netscape-"eksportbrowsere" efter 4.02 til og med 4.72. Windows 2000-operativsystemer leveret før marts 2001, som ikke har installeret Microsofts High Encryption Pack eller Service Pack 2, og som anvender Internet Explorer. Internet Explorer-browserversioner før 3.02 og Netscape-browserversioner før 4.02 er ikke kompatible med 128-bit kryptering baseret på SSL-certifikater.

4. Inkl. VeriSigns datterselskaber, partnere og forhandlere.



Autentificeringsniveauer og tillid

Et af hovedformålene med SSL-certifikater er at forsikre forbrugerne om, at de faktisk handler på det websted, som de regner med. Det vil sige, at webstedets identitet er godkendt af en anerkendt tredjepartsudbyder af netsikkerhed. Der anvendes generelt 3 kategorier af SSL-autentificering:

- Domæne
- Firma
- Extended Validation (EV)

Forskellene i sikkerhed på disse niveauer, og den tilsvarende kundetillid, som de giver, er et afgørende aspekt. Selv på det samme niveau varierer de specifikke autentificeringsprocesser fra certificeringscenter til certificeringscenter, og det er hovedårsagen til, at netbutikker bør vælge et kendt og anerkendt certificeringscenter. Det kendteste og mest velanskrevne certificeringscenter på markedet er VeriSign.

Autentificering på domæneniveau

Domæneautentificerede certifikater er den mest begrænsede form for autentificering. På dette godkendelsesniveau anvender certificeringscentrene en proces til at kontrollere, om et firma, som ansøger om et domæneautentificeret SSL-certifikat, reelt enten ejer det pågældende domæne eller har ret til at anvende domænenavnet. Desuden kontrollerer certificeringscentret eventuelt, om e-mail-adressen for den kontaktperson, som ansøger om certifikatet, findes i Whois-databaser, eller om den overholder certificeringscentrets krav til e-mail-aliaser. Alle websteder, som beskyttes af certifikater med VeriSign® varemærket, er autentificeret på et højere sikkerhedsniveau end domæneautentificering.

Autentificering på firmaniveau

Autentificering på dette niveau er den godkendelsesproces, som VeriSign og andre certificeringscentre anvender ved udstedelse af almindelige SSL-certifikater (dvs. uden EV). Certificeringscentret starter med at kontrollere firmaets faktiske eksistens via de offentlige erhvervsregistre, typisk ved at søge i offentlige og private databaser. Om nødvendigt vil certificeringscentret bede ansøgeren om at forevise f.eks. firmaets vedtægter, selskabsregistrering og dokumentation for, om firmaet driver forretning under et andet navn. Før certificeringscentret udsteder et SSL-certifikat efter autentificering på firmaniveau, kontrollerer det firmaets identitet, og at det eksisterer i juridisk henseende. Desuden kontrollerer certificeringscentret, at firmaet har tilladelse til at bruge det domænenavn, som er angivet i certifikatet, og at den person, som ansøger om SSL-certifikatet på vegne af firmaet, er bemyndiget hertil.

Autentificering med Extended Validation (EV)

Dette er den stærkeste form for autentificering i forbindelse med udstedelse af SSL-certifikater. Autentificering med EV er en godkendelsesproces med specifikke rammer og kontrolforanstaltninger. Den omfatter en dybtgående kontrol af et firmas identitet og starter med en underskrevet bekræftelse fra firmaets kontaktperson. Desuden kan der stilles krav om dokumentation for firmaets officielle registrering, hvis certificeringscentret ikke kan få bekræftet firmaoplysningerne via databaser hos offentlige myndigheder. Og der kan stilles krav om et juridisk responsum for at få bekræftet nedenstående oplysninger om firmaet:

- Adressen for firmaets fysiske forretningssted
- Telefonnummer
- Bekræftelse på firmaets eneret til at bruge domænet
- Yderligere bekræftelse af firmaets eksistens (hvis det har eksisteret i mindre end 3 år)
- Kontrol af firmakontaktpersonens ansættelse

Processen er minimalt besværlig for legitime firmaer, men en stopklods for svindlere.

Tillidsmærker

For at skabe kundetillid og maksimere omsætningen på e-handel er netbutikker nødt til ikke blot at beskytte deres kunders transaktioner på nettet, men også klart og tydeligt gøre opmærksom på, at de tager de nødvendige forholdsregler for at beskytte kunderne i denne henseende. Til det formål, og for at vinde kundernes tillid, anvender certificeringscentrene segl med deres eget tillidsmærke, som typisk placeres på fremtrædende steder på en netbutiks websider.

VeriSign-seglet er verdens kendteste og mest anvendte sikkerhedsmærke. Når en kunde klikker på seglet, bliver der åbnet et vindue med navnet på certifikatets ejer, gyldighedsperioden, oplysninger om leverede sikkerhedstjenester samt oplysninger om den proces for godkendelse af ejeren, som VeriSign har udført før udstedelsen af certifikatet. 74% af onlineforbrugere i Danmark og Sverige føler sig mere trygge ved at indtaste personlige data på websteder, der bruger sikkerhedsindikatorer som f.eks. VeriSign Secured Seal.⁵

5. "VeriSign 2009 Brand Research," Synovate/GMI, May 2009.

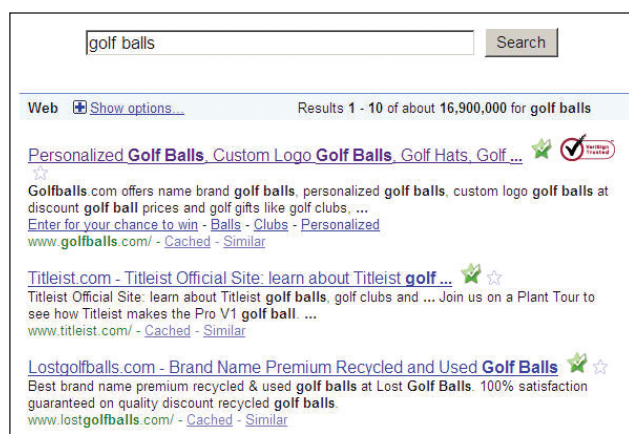




RAPPORT

VERISIGN® SEAL-IN-SEARCH™ SIGNALERER SIKKERHED FRA STARTEN

SSL giver kunderne sikkerhed for, at deres transaktioner på nettet er beskyttet, og at webstedet, de handler på, er den ægte vare. Men der kræves avancerede løsninger til at informere kunderne om, at sikkerheden er i orden, og at gøre det alle de steder på internettet, som de typisk går ind på. For jo tidligere de får budskabet om, at et websted har netsikkerheden i orden, jo bedre. For at skabe tillid på alle de trin, som en kunde gennemgår i løbet af en købeproces på nettet, kombinerer VeriSign SSL med yderligere tillidsskabende funktioner, som f.eks. scanning af websteder for malware og (afhængig af resultatet af scanningen) placering af et tillidsmærke ved siden af søgeresultaterne i søgemaskiner.



Med denne funktion, som hedder VeriSign® Seal-in-Search™, kan netbutikker signalere, at deres netsikkerhed er i orden, allerede før kunderne klikker sig frem til deres websted. Med denne mulighed for at nå ud til potentielle besøgende med et positivt tillidsbudskab så tidligt i processen, kan netbutikker skille sig ud fra de konkurrenter, som anvender SSL-certifikater fra andre udbydere, der ikke tilbyder scanning af websteder for malware eller muligheden for at få et tillidsmærke ved siden af søgeresultaterne i søgemaskiner.

SSL MED EXTENDED VALIDATION (EV) GIVER KUNDETILLID

Tidligere var indikationer på, at et websted var beskyttet med et SSL-certifikat, som f.eks. "https" i webadressen eller låseikonet af guld, tilstrækkeligt til, at forbrugerne ikke

var bekymret for ondsindede aktiviteter på internettet. Det signalerede, at de følsomme oplysninger, som forbrugerne udleverede på nettet, var beskyttet ved hjælp af kryptering på et tilstrækkeligt sikkerhedsniveau. I dag er selv den stærkeste kryptering ikke længere nok på grund af et helt andet problem, nemlig phishing. Internetsvindlere er blevet dygtige til at maskere falske websteder som den ægte vare. De køber SSL-certifikater – der desværre er alt for nemme at anskaffe fra mindre seriøse certificeringscentre med utilstrækkelige godkendelsesprocedurer – og bruger dem til at narre kunder til at udlevere følsomme oplysninger. Kryptering er en nødvendighed, men ikke længere tilstrækkeligt, for det nytter ikke, hvis modtageren af krypterede data er et falsk websted og bruger fortrolige oplysninger til identitetstyveri eller andre ulovligheder. Det at signalere over for brugerne, at netsikkerheden er i orden, er en stor udfordring. Selvom et websted ser ud til at være en kendt netbutik, som har sikkerheden i orden, kan netbrugere jo ikke vide, om det er en klon oprettet af en smart svindler!

For at få kundernes tillid skal man på en nem og pålidelig måde kunne vise dem, at deres transaktioner på nettet ikke blot er sikre, men også at webstedet, som forbrugeren foretager transaktionen på, er den ægte vare, og at det ejes af et firma, som er behørigt kontrolleret og godkendt. Det var med det formål, at udbydere af netsikkerhed og udviklere af webbrowsere slog sig sammen og etablerede standarden Extended Validation (EV), som er den første grundlæggende ændring inden for sikker e-handel på globalt plan i mere end 10 år. VeriSigns SSL-certifikater med Extended Validation opfylder denne standard.

Når en kunde via en netsikker browser går ind på et websted, som er sikret med et EV SSL-certifikat, skifter adresselinjen til grøn, og der ses et ekstra felt ved siden af navnet på den retmæssige ejer af webstedet sammen med navnet på den netsikkerhedsudbyder, som har udstedt EV SSL-certifikatet. Browseren og netsikkerhedsudbyderen sørger for, at dette sker for at afholde phishere og svindlere fra at anvende webstedets brand og kundeoplysninger ulovligt. Netsvindlere er blevet dygtige til at efterligne stort set alt på et websted. Men uden det retmæssige firmas EV SSL-certifikat har de ingen mulighed for at vise firmaets navn på adresselinjen, fordi de viste oplysninger er uden for deres kontrol. Der er ingen risiko for, at andre end den retmæssige webstedsejer kan få fat i firmaets EV SSL-



certifikater på grund af den strenge godkendelsesproces, som certificeringscentret anvender.

EV SSL skaber forbrugertillid

- Kunder på internettet kan se navnet på certifikatets ejer på adresselinjen, så de ved med sikkerhed, at webstedet er oprettet af det rigtige firma og ikke af en svindler.
- Certificeringscentre foretager yderligere kontrol af et firmas identitet og faktiske eksistens, før de udsteder EV SSL-certifikater til firmaet, for at forhindre svindlere i at udgive sig for legitime internetfirmaer.
- For at være berettiget til at udstede EV SSL-certifikater skal certificeringscentre opfylde en række strenge krav. Certificeringscentre skal opfylde betingelserne ved regelmæssige, tredjepartsudførte Webtrust-kontroller, som er baseret på de standarder, der er fastlagt af sammenslutningen af certificeringscentre og udbydere af webbrowsere, CA/Browser Forum. Dette eliminerer de utilstrækkelige baggrundstjek, som useriøse certificeringscentre anvender, og som gør det muligt for netsvindlere at operere uhindret. Med EV SSL kan kunderne have tillid til, at firmaet er korrekt godkendt som webstedets retmæssige ejer.
- Farveskiftet til grøn ser ud til at give forbrugerne positive associationer. Selv kunder, der ikke kender de "faktiske" årsager til, at de er beskyttet på nettet af EV, er mere tilbøjelige til at købe – og til at købe mere pr. handel – når de ser den grønne linje.

Der er overvældende dokumentation for, at EV SSL fungerer. Siden april 2010 har en stribe tests udført af virksomheder verden over vist, at med VeriSign® EV SSL opnås i gennemsnit 17,8% flere transaktioner (som påvist i mere end 30 tests).⁷

Kundeundersøgelser af denne type dokumenterer værdien og vigtigheden af EV SSL og VeriSign-brandet med hensyn til, hvad kunder genkender, har tillid til og foretrækker.

Desuden gør VeriSign-seglet, som medfølger til alle VeriSign SSL-certifikater, det muligt for firmaer at skilte med internettets mest anerkendte tillidsmærke. Ifølge en Synovate/GMI-undersøgelse genkender næsten 2 ud af 3 onlineforbrugere i Danmark og Sverige VeriSign-seglet, hvilket er betydeligt mere end noget andet tillidsmærke.⁸ Med VeriSign-seglet kan besøgende desuden til enhver tid kontrollere oplysningerne og status for SSL-certifikatet, hvilket øger kundernes tillid, når de handler på nettet.

Reelle resultater med VeriSign EV SSL

Papercheck.com: 87% flere kunderegistreringer på webstedet.

CRSHotels.com: 30% flere besøgende, der vælger at købe.

CarInsurance.com: 18% flere kundetilmeldinger på nettet.

Flagstarbank.com: 10% flere kundetilmeldinger på nettet.

CreditKarma.com: 26% flere besøgende, der vælger at handle på webstedet.

Se detaljerede oplysninger på <http://www.verisign.dk/ssl/ssl-information-center/ssl-case-studies/index.html>.

VERISIGN-MARKEDETS FØRENDE LEVERANDØR AF NETSIKKERHED OG TILLID

VeriSign er verdens førende udbyder af SSL-certifikater, og har en markedsandel for EV SSL-certifikater på over 70%.¹⁰ På listen over kunder med VeriSign EV SSL findes de største firmanavne inden for e-handel og bankvirksomhed.⁹ 97 af verdens 100 største banker og 93% af Fortune 500, som alle bruger SSL, har SSL-certifikater fra VeriSign.¹⁰ VeriSign-seglet findes på mere end 90.000 domæner i 160 lande og er det kendteste tillidsmærke på internettet. Netbrugerne har vænnet sig til se efter, om netbutikker har VeriSign-seglet, der er placeret klart og tydeligt, så besøgende kan se, at en netbutik er den ægte vare, og at den håndterer kundernes fortrolige oplysninger sikkert med SSL-kryptering.

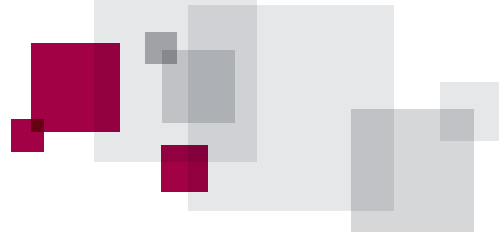
7. Se detaljerede oplysninger på <http://www.verisign.dk/ssl/ssl-information-center/ssl-case-studies/index.html>.

8. "VeriSign 2009 Brand Research," Synovate/GMI, May 2009

9. Netcraft-rapport, april 2010

10. Inkl. VeriSigns datterselskaber, partnere og forhandlere.





KONKLUSION

Med den voldsomme stigning i netsvindler er beskyttelse af transaktioner med personlige data så afgørende som aldrig før inden for e-handel. Udbredelsen af, og konsekvenserne ved, identitetstyveri er yderst velkendt og veldokumenteret. Med det stigende antal tyverier af internetdata er potentielle kunder blevet mere forsigtige, opmærksomme, skeptiske, og rent ud sagt, mere bange. De forventer at blive beskyttet, 64 procent angiver, at de er mindre tilbøjelige til at handle med onlinehandlende, som ikke har et garantimærke.¹¹

At skabe kundetilid på nettet gør hele forskellen. Investeringen i teknologi til at beskytte kunderne og vinde deres tillid er en bagatel i forhold til de totale omkostninger til at drive en virksomhed. Fordi omkostningen fuldstændig overskygges af de potentielle fordele, er det klart, at en forbedring af sikkerheden i en netbutik (med teknologi som f.eks. SSL) er det oplagte valg for netbutikker, som ønsker resultater.

For at sikre, at nuværende og kommende kunder bliver gjort klart og tydeligt opmærksom på en netbutiks investeringer i sikkerhed, er det afgørende at vælge den kendteste og mest anerkendte netsikkerhedsudbyder. VeriSign har gjort sig fortjent til anerkendelsen som branchens førende brand, og den dertilhørende kundetilid, ved at tilbyde markedets mest avancerede netsikkerhedsløsninger.

FÅ MERE AT VIDE

Du kan få mere at vide om VeriSign SSL-certifikater ved at ringe til 80 88 29 78 eller +45 88 61 01 10 eller ved at sende en e-mail til: salg@verisign.dk

OM VERISIGN

VeriSign er den digitale verdens anerkendte leverandør af infrastrukturtenester til internettet. Flere milliarder gange hver eneste dag benytter firmaer og forbrugere vores internetinfrastruktur til at kommunikere og handle trygt på nettet.

Få mere at vide på www.Verisign.dk.

11. "VeriSign 2009 Brand Research," Synovate/GMI, May 2009

