



RAPPORT

DE SENASTE FRAMSTEGEN INOM SSL-BASERADE SÄKERHETSLÖSNINGAR

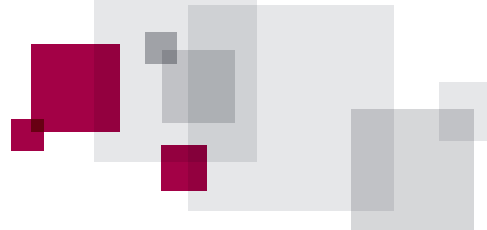


RAPPORT

INNEHÅLL

- 1 INLEDNING
- 1 ÖVERSIKT
- 1 EXTENDED VALIDATION (EV) SSL: HÖGSTA STANDARDEN FÖR AUTENTISERING
- 3 FÖRTROENDEMÄRKEN: INGE KUNDERNA FÖRTROENDE
- 3 VÄLKÄNDA FÖRTROENDEMÄRKEN INGER TILLIT OCH FÖRTROENDE
- 3 FÖRTROENDEMÄRKEN NÅR NYA HÖJDER: VERISIGN® SEAL-IN-SEARCH™
- 3 SGC (SERVER GATED CRYPTOGRAPHY): ENHETLIG OCH KRAFTFULL KRYPTERING
- 4 SAMMANFATTNING
- 4 OM VERISIGN





DE SENASTE FRAMSTEGEN INOM SSL-BASERADE SÄKERHETSLÖSNINGAR

INLEDNING

SSL-tekniken (Secure Sockets Layer) är den faktiska standarden för e-handelssäkerhet. Den är inriktad på de problem som kan tänkas förekomma i form av obehörig insyn i konfidentiell information, manipulering av data, kapning av data, nätfiske (phishing) och andra lömska onlinebedrägerier. Den fungerar genom att kryptera känsliga data så att bara behöriga mottagare får tillgång till dem. Dessutom bidrar SSL:s autentiseringsfunktioner till att göra besökarna på din webbplats trygga i förvisningen om att de har kommit till en äkta webbplats. Alla större operativsystem, webbprogram, webbläsare och servermaskinvaror har inbyggt stöd för SSL. Det innebär att SSL:s kraftfulla krypteringsteknik och autentiseringsfunktioner bidrar till att ge ditt företag ett övergripande skydd som ger konsumenterna oavbruten tillit, ökar andelen slutförda transaktioner och förbättrar vinsten för företaget.

Tack vare de senaste framstegen inom SSL-tekniken och närliggande tekniker finns ett spektrum av funktioner i de olika SSL-erbjudandena på marknaden. I den här rapporten diskuterar vi några av de framstegen i syfte att hjälpa dig att avgöra vilka lösningar som bäst passar din organisation.

ÖVERSIKT

SSL, som lanserades kommersiellt av VeriSign i mitten av 1990-talet, skyddar meddelanden som skickas via nätet mot obehörig åtkomst. En datafil, dvs. ett SSL-certifikat, skapas för en viss domän, på en viss server och för ett visst företag. SSL-certifikatet, som kan liknas vid pass eller körkort, utfärdas av betrodda instanser, certifikatutfärdare (CU). Varje organisation som vill ha ett SSL-certifikat måste genomgå någon form av autentisering, genomförd av certifikatutfärdaren, där den sökandes identitet och legitimitet bekräftas. I och med den enorma ökningen av nätfiske och andra bedrägerier med syfte att stjäla personlig information är verifiering av identiteten viktigare än någonsin.

Med hjälp av ett system med en privat och en publik nyckel krypterar SSL anslutningen mellan två parter, t.ex. en konsument och en webbplats försedd med ett SSL-certifikat. När konsumentens webbläsare öppnar en webbplats där SSL-skyddet används, autentiseras båda parter med ett "handslag". För varje session används en unik krypteringsnyckel (ju längre nyckelns bitlängd är, desto starkare är krypteringen). När anslutningen har etablerats, kan parterna inleda en säker session där sekretess och förfalskningskydd garanteras. Skyddet är särskilt viktigt när personer utbyter känslig och konfidentiell information via Internet, ett extranät eller ett intranät. När det gäller e-handel är en säker SSL-anslutning av avgörande betydelse för affärsverksamheten, eftersom de flesta Internetanvändare drar sig för att skicka känsliga uppgifter till en webbplats som inte erbjuder SSL-skydd.

Ett litet inköp här, ett ännu mindre inköp där, och tvekan inför att ändra ingrodda köpvanor eller avslöja konfidentiell information – detta är exempel på beteenden som hämmar e-handeln. För att undanröja sådana farhågor måste nätföretagen anstränga sig för att skapa tillit hos befintliga och tänkbara kunder. Nedan beskrivs ett antal funktioner som du bör beakta när du väljer SSL-lösning för ditt företag.

EXTENDED VALIDATION (EV) SSL:

Högsta standarden för autentisering

Även om allt fler känner sig hemma på Internet, är det fortfarande ett stort avstånd mellan antalet nätsurfare och antalet personer som är benägna att göra affärer på nätet. Detta beror på rädslan för att konfidentiella uppgifter ska röjas. I en undersökning som TNS genomförde i mars 2010 på begäran av VeriSign kunde fyra av tio inte tänka sig att betala sina räkningar eller sköta sina bankärenden på nätet på grund av oro för bristande säkerhet. Omkring en tredjedel kunde inte tänka sig att hantera sina investeringar eller köpa något via nätet på grund av säkerhetsproblem.¹

1. VeriSign Trust Index Report, mars 2010. Rapporten finns på adressen https://www.trustthecheck.com/assets/VeriSign_Internet_Trust_Index_March_201





Uppenbarligen är alltför många potentiella e-handelskunder fortfarande rädda för att avslöja privat eller ekonomisk information för ett företag som man varken har sett eller känner personligen. De behöver bli förvissade om att deras konfidentiella information är i säkert förvar, och i allt högre grad kräver de bevis på att tillräckliga säkerhetsåtgärder har vidtagits innan de överför konfidentiella uppgifter eller genomför en ekonomisk transaktion via nätet – 53 procent av Internetanvändarna i Sverige oroar sig för betalningssäkerheten.²

Den här typen av oro ledde till att en grupp certifikatsutfärdare, webbläsarföretag och WebTrust-granskare inrättade sammanslutningen CA/Browser Forum i syfte att utveckla en ny SSL-standard – en standard som världens nätkonsumenter lätt skulle kunna förstå och ta till sig. Detta konsortium, med representanter för såväl Microsoft och VeriSign som andra organisationer, har skapat Extended Validation-autentisering (EV). Det är en branschstandard med syfte att bekämpa tillväxten av Internethot såsom nätfiske.

För att erhålla ett EV SSL-certifikat måste den sökande genomgå en gedigen autentiseringsprocess, genomförd av en certifikatsutfärdare som omfattar både verksamheten och webbplatsen. I den bemärkelsen anses EV SSL vara ”den gyllene standarden” inom e-handeln när det gäller autentisering av en webbplats äkthet. För att få rätt att utfärda EV SSL-certifikat måste en certifikatsutfärdare genomgå en omfattande granskning av WebTrust och VeriSign leder alltjämt utvecklingen och tillämpningen av EV SSL-standarderna.

Ett EV SSL-certifikat ger onlineföretaget och kunden ett skydd mot de alltmer sofistikerade förfalskningsbedrägerierna på Internet och är ett rekommenderat skydd som är erkänt i vida kretsar. EV SSL innehåller ett antal visuella förbättringar som kännetecknar en autentiserad webbplats på ett mer uppenbart sätt för slutanvändarna. Nyare webbläsare visar EV SSL-certifikat på ett annat sätt än traditionella SSL-certifikat. När kunderna besöker en webbsida som skyddas med ett EV SSL-certifikat blir adressfältet grönt och i ett särskilt fält visas namnet på den legitima innehavaren av webbplatsen jämte namnet på det säkerhetsföretag (certifikatsutfärdaren) som har utfärdat certifikatet.



De riktlinjer för EV som reglerar utfärdandet av EV SSL-certifikat ger även konsumenterna och webbplatsinnehavarna ett extra skydd. De kräver att utfärdaren följer en strikt process för utfärdande och hantering, definierad av CA/Browser Forum. Denna standardiserade enhetlighet i processen minskar risken för fel vid utfärdandet vilka skulle kunna medföra sänkt säkerhetsnivå.

Dussintals test som har genomförts fram till april 2010 av företag runtom i världen visar att användningen av VeriSign® EV SSL har ökat antalet transaktioner med i genomsnitt 17,8 procent (i mer än 30 test).³ Bland exemplen på kundframgångar med VeriSign EV SSL finns följande:

Faktiska resultat med VeriSign EV SSL

Scandinavian Design Online: 8% ökning av onlineförsäljningen

CRSHotels.com: 30% fler omvandlingar

Misco: 5,27% minskning av avbrutna köp

Worldticketshop: 20% ökning av onlineförsäljningen

Alla detaljer finns på www.verisign.se/ssl/ssl-information-center/ssl-case-studies/index.html

Precis som traditionella SSL-certifikat underlättar ett EV SSL-certifikat säker, krypterad kommunikation mellan en webbplats och kundens webbläsare. Det autentiserar dessutom äktheten hos webbplatsen, så att alla besökare vet att de verkligen har kommit dit de vill och inte till en bedragare.

2. E-barometern Q1 2010 www.hui.se/web/e-barometern

3. Alla detaljer finns på www.verisign.se/ssl/ssl-information-center/ssl-case-studies/index.html





VeriSign är världens ledande leverantör av SSL-certifikat. Hittills har fler än 24 000 webbplatser börjat använda Extended Validation (EV) SSL-certifikat, och VeriSign är förstahandsvalet för fler än 17 000.⁴

FÖRTROENDEMÄRKEN: INGE KUNDERNA FÖRTROENDE

Praktiskt taget alla kunder säger sig vara oroade av risken för identitetsstöld, kreditkortsbedrägeri och andra Internet-bedrägerier. De har goda skäl till det. Nätfiske är fortfarande ett högst reellt och växande hot. Under fjärde kvartalet 2009 ökade antalet kapade varumärken i oktober till rekordnivån 356. Det är en ökning med nästan 4,4 procent jämfört med det tidigare rekordet 341 (augusti 2009).

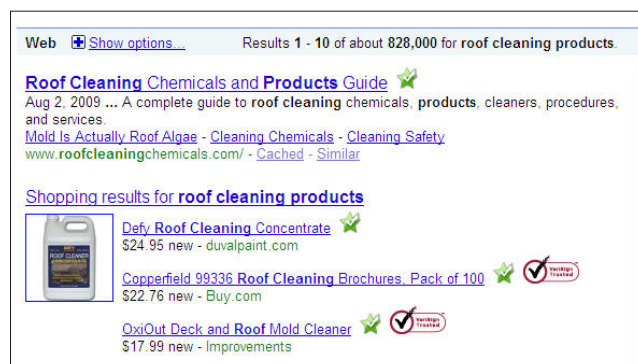
Konsumenternas medvetenhet om säkerhetslösningar kommer sannolikt att öka allt eftersom både säkerhetsbranschen och myndigheter informerar om behovet av säkerhet. Och nätkunderna blir också alltmer på det klara med de här frågorna. Många väntar sig att få se ett välbekant förtroendemärke från en tredje part som visar att en nätförsäljares webbplats är säker och välfungerande. Att ha ett sådant lätt igenkännbart förtroendemärke på webbplatsen är numera nödvändigt för att leda konsumenterna från att jämföra pris och produkter till att genomföra ett köp.

Välkända förtroendemärken inger tillit och förtroende

Forskning har visat att de allra flesta nätkonsumenterna känner igen VeriSign-sigillet, och de har angett att de skulle kunna göra ett nätköp just på grund av att sigillet finns på en webbplats. Detta sigill, som ses mer än 250 miljoner gånger varje dag, är det mest kända förtroendemärket i hela världen.⁵ När du köper ett VeriSign SSL-certifikat får du rätten att visa VeriSign Trust™-sigillet på en framträdande plats på din webbplats och i sökresultat. Om du visar upp VeriSign-sigillet höjs kundernas förtroende för din webbplats, vilket kan leda till fler genomförda transaktioner.

FÖRTROENDEMÄRKEN NÅR NYA HÖJDER: VERISIGN® SEAL-IN-SEARCH™

Det blir allt viktigare att nå kunderna så tidigt som möjligt för att inge förtroende för webbplatsen. Din webbplats utmärker sig på ett naturligt sätt om du kan visa upp ett förtroendemärke bredvid din länk i sökresultaten. Med denna teknik, som kallas VeriSign® Seal-in-Search™ (sigill i sökresultat), kan nätföretaget inge kunderna förtroende redan innan de besöker webbplatsen. Kunderna går ofta vidare till länkar med förtroendemärken när de söker och jämför priser. Genom att tidigt inge kunderna förtroende har din webbplats bättre förutsättningar att öka trafiken och intäkterna.



Förtroendemärken kan hjälpa företagen att redan i sökresultaten visa att de är tillförlitliga och att uppmuntra till besök på webbplatsen.

SGC (Server Gated Cryptography): Enhetlig och kraftfull kryptering

SGC (Server Gated Cryptography) – ytterligare en förbättring – är ett SSL-tillägg som skapades för att möjliggöra den lägsta rekommenderade krypteringsnivån (128 bitar) oavsett vilken krypteringsstyrka som är tillgänglig i kundens webbläsare. Med SGC styrs krypteringsnivåerna bara av servern och är oberoende av kundsystemets webbläsare. Utan SGC blir krypteringsnivån den lägsta som server och webbläsare kan hantera. Eftersom branschexperter rekommenderar minst 128 bitars kryptering för alla säkra sessioner, kan detta vara en viktig funktion i en miljö där äldre webbläsare används.

4. www.antiphishing.org

5. VeriSign Brand Tracker-undersökning, 2009





RAPPORT

VeriSign erbjuder marknadsledande SSL-certifikat med SGC-kapacitet, vilket betyder att så gott som alla som besöker din webbplats får ett skydd på den rekommenderade miniminivån 128 bitar.

SAMMANFATTNING

Trovärdighet betyder mycket när det gäller Internetsäkerhet. VeriSign är i dag det mest kända av världens alla varumärken för säkerhet online. Det anseendet har odlats under många år och har utvecklats tillsammans med kunder och onlineföretag. VeriSigns branschledande ställning och tillämpningen av den senaste tekniken har gjort dess SSL-lösningar ledande på marknaden. EV SSL och Seal-in-Search är bara två exempel på VeriSigns avancerade metodik för att gripa sig an problem, en metodik som hela tiden vidareutvecklas för att ge skydd i den ständigt föränderliga hotmiljön på Internet. Om du vill vara säker på att konsumenterna ska våga handla på din e-handelsplatser är VeriSigns SSL-certifikat rätt val.

OM VERISIGN

VeriSign är en betrodd leverantör av infrastrukturtjänster på Internet för den digitala världen. Företag och konsumenter förlitar sig på vår Internetinfrastruktur miljarder gånger per dag för att kommunicera och sköta sina affärer på ett säkert sätt.

Besök oss på www.Verisign.se så hittar du mer information.

