

AFFÄRSKONTINUITET OCH
INTRÅNGSSKYDD: VARFÖR
HANTERING AV SSL-CERTIFIKAT ÄR
VIKTIG FÖR DAGENS FÖRETAG

Whitepaper

Affärskontinuitet och intrångsskydd: Varför hantering av SSL-certifikat är viktig för dagens företag



VeriSign
Authentication Services

Affärskontinuitet och intrångsskydd Varför hantering av SSL-certifikat är viktig för dagens företag

Innehåll

Inledning	3
Utmaningar med att hantera SSL-certifikat.	3
Faror med utgångna och oövervakade SSL-certifikat	4
Stöld av kundinformation	4
Tappa kunder till konkurrenter	6
Fler samtal till kundsupport.	6
Ökad belastning på IT-avdelningen.	6
Bästa metoder för SSL-certifikatshantering	7
Slutsats.	8
Symantec® Certificate Intelligence Center: Stabil SSL-identifiering och -hantering.	8

Inledning

SSL-certifikat har använts i nästan 15 år, och de spelar fortfarande en viktig roll när det gäller att skydda information som överförs över Internet eller andra nätverk. Med SSL-certifikat kan användare världen över överföra känslig information, t ex vid ekonomiska transaktioner över Internet, e-handel eller produktutveckling, i vetskap om att den är skyddad mot hackare.

Internet har utvecklats på oräkneliga sätt de senaste 15 åren, så varför upplevs SSL-certifikat fortfarande som så trygga? Helt enkelt därför att SSL-certifikat är väldigt effektiva på att skydda data som förflyttas. Faktum är att enligt vissa beräkningar skulle det ta ungefär sex tusen biljoner år – ungefär en miljon gånger fler år än vad jorden har funnits – att knäcka en 128-bitars kryptering på SSL-certifikat med ett brute force-angrepp.¹ Trots detta är säkerhetsbranschen på sin vakt och många certifikatutfärdare har börjat fasa in 2 048-bitars kryptering på sina SSL-certifikat för att stärka datakommunikationen på Internet ytterligare.

Trots det finns det fortfarande allvarliga hot för kunder som gör transaktioner på webbplatser och i program som skyddas av SSL-säkerhet. En huvudanledning till den faran är dålig hantering av SSL-certifikaten. Företag med hundratals SSL-certifikat från flera olika leverantörer kan tappa översikten över certifikaten i sin miljö. Om det händer kan certifikaten förfalla utan att någon upptäcker det på flera månader, vilket gör besökarna på webbplatsen sårbara för angrepp från hackare.

Ibland är det första tecknet på att det finns ett ”försvunnet” SSL-certifikat ett samtal från en kund som upptäckt ett utgående certifikat och undrar om det verkligen är säkert att göra inköp på webbplatsen. Andra gånger kan det vara något mer allvarligt, som ett nätfiskeangrepp där Internetbrottslingarna stjälar känslig kundinformation. Eller så påverkar en säkerhetslucka hos en certifikatutfärdare ett företag då man inte snabbt kan agera eftersom man inte har insyn i SSL-certifikatuppsättningen.

Vilket fall det än rör sig om kan det orsaka betydande ekonomiska förluster och ett skadat rykte om man inte har SSL-certifikaten under kontroll. Som tur är behöver det inte vara komplicerat eller tidsödande att hitta och hantera SSL-certifikat inom företaget.

I detta whitepaper presenteras de fallgropar som en dålig SSL-certifikathantering kan innebära, varför de är potentiellt farliga för företaget och hur företaget kan hålla koll på SSL-certifikaten på ett effektivt sätt.

Utmaningar med SSL-certifikathantering

Dagens företag har en komplex miljö som ofta omfattar flera interna nätverk och webbsidor för allmänheten. Därför kan ett företag ha dussintals om inte hundratals olika SSL-certifikat distribuerade vid en given tidpunkt.

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

Många företag använder en blandning av olika certifikat från olika certifikatutfärdare och dessutom har de många SSL-certifikat. Ett exempel är att ett företag kan installera SSL-certifikat från en välkänd, betrodd leverantör på sin kundinriktade webbplats och billigare eller självsignerade certifikat på intranätet.

Även om vissa certifikatutfärdare erbjuder verktyg på Internet som hanterar deras specifika certifikat, ger oftast inte de verktygen synlighet för alla certifikat från olika certifikatutfärdare i en miljö. I stället för att göra hanteringen enklare förvärrar flera hanteringsportaler problemet med att spåra ett otal SSL-certifikat i en miljö med flera certifikatutfärdare. Administratörer måste konstant övervaka sitt SSL-certifikatbestånd via flera system och sammanställa sina egna rapporter för att få en övergripande bild av sina SSL-certifikat.

För att komplicera saken kan företag med distribuerade nätverk ha en säkerhetspolicy som skiljer sig från grupp till grupp. Det innebär i praktiken att Grupp A kanske kräver Extended Validation SSL-certifikat för att skydda den information den hanterar, medan Grupp B använder en annan typ av SSL-certifikat från en annan certifikatutfärdare. Eller Grupp A kanske kräver 2 048-bitars SSL-certifikat medan Grupp B använder 1 024-bitars certifikat, ett scenario som blir allt vanligare. Med olika policyer och utan någon enhetlig metod att få en övergripande bild av SSL-certifikaten inom ett företag kan dessa inkonsekvenser leda till säkerhetsrisker och brott mot regelkrav och företagspolicyn.

Ytterligare en sida av problemet: fundera på vad som händer om de anställda som är ansvariga för att hantera SSL-säkerheten byter arbetsuppgifter eller lämnar företaget. Om de inte väldigt noga dokumenterar vilka certifikat de hanterar och förmedlar det till sina kollegor kanske dessa SSL-certifikat inte uppmärksammas när en ny person tar över. Eftersom IT-teamen på företagen är upptagna och pressade vad gäller resurser är manuell spårning av SSL-certifikat inte bara en belastning, utan även utsatt för den mänskliga faktorn.

Alla dessa faktorer bidrar till en miljö där SSL-certifikat kan försvinna eller förbises. En sådan miljö kan leda till driftstopp för ett företag och skapa säkerhetsrisker för kunderna.

Faror med utgångna och oövervakade SSL-certifikat

Ett utgångnet eller oövervakat SSL-certifikat i en nätverksmiljö kan få allvarliga återverkningar. Det krävs bara ett utgångnet eller oövervakat certifikat för att exponera ett företag – och kanske ännu viktigare, dess kunder – för Internetbrottslingar. Nedanstående information är bara exempel på konsekvenser som kan följa av utgångna och oövervakade SSL-certifikat.

Stöld av kundinformation

Tack vare årtal av nyhetsrubriker om dataintrång samt utbildningsinsatser av stödgrupper för kunder och företag är nu allmänheten mer orolig för identitetsstöld än någonsin tidigare. En nyligen genomförd studie visar att 64 procent av

amerikanska medborgare är mycket eller extremt oroliga för att någon ska stjäla deras identitet, där 32 procent beskriver sin oro som extremt orolig.²

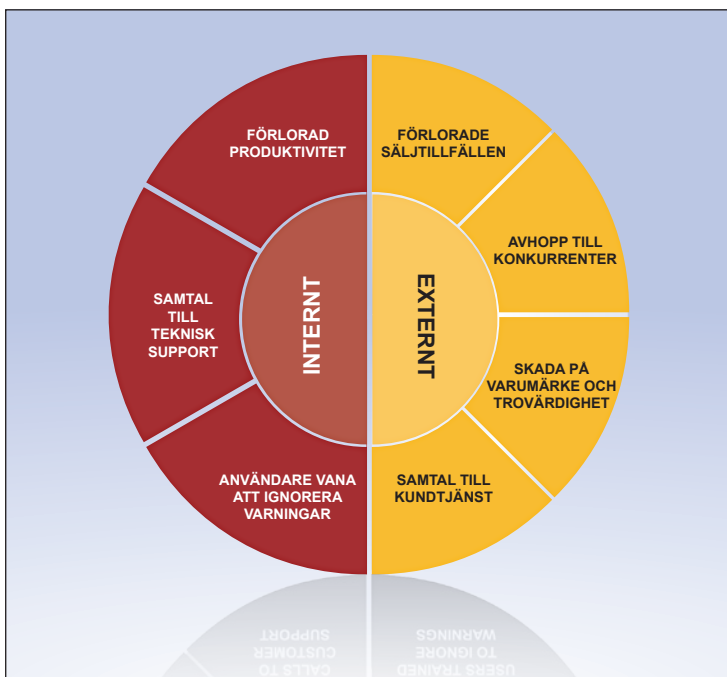
I detta sammanhang är risken för nätfiske, så kallat phishing, något man oroar sig mycket för. Vid nätfiske, så kallat phishing, antar hackaren identiteten av en legitim verksamhet och utnyttjar företagets brist på autentisering från obefintliga eller utgångna SSL-certifikat och skapar en falsk webbplats som är väldigt lik – men inte identisk med – den äkta webbplatsen. Aningslösa kunder anger sedan konfidentiell information som kreditkortsnummer eller personnummer på webbplatsen. Den falska webbplatsen skickar uppgifterna direkt till hackaren som i sin tur kan sälja informationen till andra brottslingar.

Även ett litet dataintrång eller nätfiskeangrepp kan förvärra rädslan och allvarligt hota företaget.

Förutom dessa omedelbara förluster påverkar nätfiske och dataintrång även företagets rykte och får både nuvarande och blivande kunder att fråga sig om det verkligen går att lita på ett sådant företag. Branshexperter säger att det tar cirka 6 månader att stabilisera försäljning och förtroende för ett företags nätverk efter ett intrång³ – och inte ens då är företagets rykte helt återställt.

De ökande kostnaderna av dataintrång

Det kan vara svårt att mäta skador på ett företags rykte. Det är lättare att påvisa den ekonomiska följden av ett dataintrång. Enligt en nyligen utförd amerikansk studie är den genomsnittliga kostnaden för ett dataintrång 7,2 miljoner USD per fall, eller ca 214 USD per utsatt post⁴, siffror som förutspås öka ytterligare.



Konsekvenser av oväntade upphöranden av SSL-certifikat samt webbläsarvarningar

2. "Rädslan för identitetsstöld är stor hos amerikaner" av Tim Greene, Network World, 2010-04-12
3. "Dataintrång hos Sony utsätter användare för risk för identitetsstöld i flera år" av Cliff Edwards och Michael Riley, BusinessWeek.com, 2011-03-05
4. "Kostnaderna för dataintrång blir allt högre" Ponemon Institute, ponemon.org, 2011-03-08

Tappa kunder till konkurrenter

En annan faktor som ställer till det för företag är utgångna SSL-certifikat i sig. Ett utgångna SSL-certifikat kan leda till förlorade affärer på andra sätt. Vanligast bland dem är att helt enkelt förlora trafik när kunderna ser varningar om förfallna SSL-certifikat och lämnar webbplatsen för att köpa produkter och tjänster på webbplatser med säkra SSL-certifikat.

Kunderna kanske inte vet exakt hur kryptering med publik nyckel fungerar, men synliga tecken på SSL-säkerhet, som ett SSL-sigill eller det gröna fältet för utökad validering, gör det mer troligt att de utför sina transaktioner på en viss webbplats.⁵ Om SSL-certifikat för e-handelswebbplatser eller andra typer av kundinriktade webbplatser förfaller, förlorar de kundernas förtroende vilket leder till förlust av affärer.

Fler samtal till kundsupport

Idag erbjuder många företag webbverktyg, automatiska telefonmenyer och andra självbetjäningsoptioner för att göra det enklare för kunder att hitta den information de behöver. Men om kunderna besöker en webbplats och ifrågasätter om deras privata information är skyddad kommer de antingen att lämna transaktionen (som nämndes ovan) eller kanske att ringa kundtjänst.

Den genomsnittliga kostnaden per supportsamtal varierar mycket mellan olika branscher, men en sak är säker: kostnaden för många samtal blir högre med tiden. Extra supportsamtal dränerar inte bara ett företags ekonomiska resurser, utan är en ytterligare belastning för kontaktcentret och avleder supportpersonal från andra värdefulla kundsamtal.

Den extra kostnaden och besväret med kundfrågor kan enkelt undvikas genom att ha en uppdaterad säkerhet, med bland annat giltiga SSL-certifikat.

Ökad belastning på IT-avdelningen

Precis som kunder ringer kundsupporten när de är osäkra vad gäller en webbplats säkerhet, kontaktar ofta anställda som ser varningar från utgångna SSL-certifikat på intranätet eller andra interna webbplatser IT-personalen för att lösa problemet. Det kan lägga ytterligare börda på en IT-avdelning som redan har för mycket att göra.

I andra fall kanske anställda istället ignorerar varningarna, en situation där den påverkade resursen även fortsatt är sårbar för angrepp. Det leder också till en negativ inställning till att följa säkerhetsstandarder, genom att det skapar ett intryck av att personalen kan bortse från interna säkerhetsåtgärder.

Båda scenarierna kan förebyggas med en uppdaterad SSL-certifikatsäkerhet i hela företaget.

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

Bästa metoder för SSL-certifikatshantering

Som tur är finns det tjänster som gör det enkelt att identifiera och hantera SSL-certifikat i hela företaget. Om vissa lösningar kanske det påstås att de minskar belastningen från SSL-hanteringen, även om du inte kan hitta certifikat från olika certifikatutfärdare med dem. Andra lösningar kan erbjuda möjligheten att söka efter flera certifikatutfärdare, men saknar ett intuitivt, lättnavigerat gränssnitt.

För att hitta den bästa lösningen för dina behov ska du titta efter några av de här nyckelfaktorerna i den lösning du överväger:

- **Möjlighet att genomsöka din miljö automatiskt:** Även om det är möjligt att granska nätverk manuellt är den metoden alltför tids- och personalkrävande för att användas i en stor och komplex företagsmiljö. Se till att välja en tjänst som låter teamet utföra automatiska genomsökningar som identifierar SSL-certifikat från alla leverantörer.
- **Ett lättanvänt gränssnitt:** Information som är svår att komma åt eller läsa är inte användbar, så leta efter ett verktyg som erbjuder en panel som är lättnavigerad och presenterar information på ett sätt som är lätt att förstå vid en snabb blick.
- **Delegeringsmöjligheter:** I den typiska företagsmiljön sysselsätter säkerhetshanteringen flera anställda. Av den anledningen är det mycket viktigt att hitta en lösning för certifikatidentifiering som tillåter administratörerna att bevilja olika åtkomstnivåer och delegera uppgifter till olika anställda i hela nätverket.
- **Varningar och rapporter:** Ett förfallet SSL-certifikat innebär en risk för informationen, så det är mycket viktigt att hitta en tjänst som skickar varningar innan ett certifikat behöver förnyas. Dessutom är det mycket viktigt med möjligheten att generera rapporter som är enkla att läsa och förstå. Avancerade rapportmöjligheter ger inte bara en djup, omfattande bild av certifikaten i nätverket, utan tillåter även ditt team att kommunicera viktig information till annan personal – t ex chefer – mer effektivt.
- **Flexibilitet och skalbarhet:** Företagsnätverk är dynamiska, föränderliga miljöer, vilket innebär att en tjänst för certifikatidentifiering ska ha konfigurerbara parametrar, som genomsökningens längd, vilka IP-adresser som ska genomsökas och så vidare. Dessutom måste tjänsten vara skalbar för framtida tillväxt.
- **Tidsanpassning:** Nätverksgenomsökningar måste slutföras snabbt för att vara effektiva. Om en genomsökning av hela nätverket tar för lång tid kan statusen för ett SSL-certifikat ändras innan genomsökningen är slutförd. Det resulterar i en inkorrekt bild av SSL-certifikaten.

Slutsats

SSL-certifikat är oumbärliga för att skydda data som flyttas. Hur stark och pålitlig SSL-säkerheten än är, kan den ändå vara sårbar för angrepp av en enkel anledning: dålig hantering av SSL-certifikaten.

I en företagsmiljö med många certifikat och många certifikatutfärdare är det nödvändigt att få en heltäckande bild av SSL-säkerheten. Att känna till status för varje certifikat över alla webbplatser och nätverk kan inte bara hjälpa till att kontrollera kostnader för kundtjänst, utan även minska bördan av SSL-administrering. Det ger upptagna IT-team mer tid till att koncentrera sig på andra verksamhetskritiska projekt.

Noggrann SSL-hantering kan också förebygga än mer allvarliga konsekvenser, som ett större nätfiskeangrepp eller andra typer av dataintrång som är kostsamma att åtgärda och kan orsaka långsiktig skada på ditt rykte hos kunderna.

Symantec® Certificate Intelligence Center: Stabil SSL-identifiering och -hantering

Symantec Certificate Intelligence Center hjälper administratörer att identifiera och hantera SSL-certifikat mer effektivt. Med djupgående funktioner för synlighet och hantering gör Symantec Certificate Intelligence Center det enkelt att hålla reda på SSL-certifikaten.

Symantec Certificate Intelligence Center har ett intuitivt gränssnitt där administratörerna kan ställa in automatiska genomsökningar som snabbt upptäcker certifikat från alla certifikatutfärdare. Användare kan också ställa in varningar som i förebyggande syfte varnar SSL-ansvariga om vilka certifikat som är på väg att förfalla.



Symantec Certificate Intelligence Centers lättnavigerade panel

Symantec Certificate Intelligence Center är en enkel skalbar lösning som snabbt kan anpassas till förändringar i nätverket i takt med att affärsbehoven förändras och växer. Avancerade rapportfunktioner ger också de ansvariga en omfattande bild av SSL-säkerheten som är lätt att förstå och kommunicera över hela företaget.

För mer information om hur Symantec Certificate Intelligence Center kan hjälpa dig att förenkla identifiering och hantering av SSL-certifikat, gå till:

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

Mer information

Gå till vår webbplats

<http://www.verisign.se>

Om du vill tala med en produktspecialist

Ring 08-585 369 10 eller 040-660 20 80

Om Symantec

Symantec är en världsledande leverantör av lösningar inom säkerhet, lagring och systemhantering. Vi hjälper företag och privatpersoner att skydda och hantera sin information. Våra program och tjänster skyddar mot fler risker på fler ställen, mer heltäckande och effektivt. De ger trygghet oavsett var du använder och lagrar information. Symantecs huvudkontor ligger i Mountain View i Kalifornien och företaget har verksamhet i 40 länder. Mer information finns på www.symantec.com.

Symantec Nordic A.B.

Kista Science Tower
Färögatan 33, Flr 5
161 54 Kista
Sverige

