

Livre blanc

Continuité de l'activité et protection des données : l'incontournable gestion des certificats SSL



Continuité de l'activité et protection des données : l'incontournable gestion des certificats SSL

Sommaire

Introduction	3
Défis liés à la gestion des certificats SSL	3
Dangers liés aux certificats corrompus ou arrivés à expiration	4
Vol d'informations personnelles	4
Perte de clients au profit de la concurrence.	6
Multiplication des demandes d'assistance client.	6
Pression accrue sur les départements informatiques	6
Pratiques reconnues en matière de gestion des certificats SSL	7
Conclusion	8
Symantec® Certificate Intelligence Center : recherche et gestion efficaces des certificats SSL	8

Introduction

Depuis près de 15 ans, les certificats SSL jouent un rôle essentiel dans la protection des données acheminées sur Internet ou d'autres réseaux. Des transactions financières en ligne au commerce électronique ou au développement de produits, les certificats SSL permettent aux utilisateurs du monde entier de transmettre des informations sensibles avec l'assurance que celles-ci seront protégées contre toute action malveillante.

Ces quinze dernières années, le réseau Internet a considérablement évolué et pourtant les certificats SSL continuent d'inspirer le même sentiment de confiance. Quelle en est donc la raison ? En deux mots, ces certificats doivent leur succès à leur efficacité dans la protection des données en transit. Selon une estimation, il faudrait environ six trillions d'années (soit environ un million de fois l'âge actuel de la Terre) pour venir à bout du chiffrement 128 bits utilisé par les certificats SSL, quelle que soit la méthode employée.¹ Toutefois, la vigilance étant de rigueur dans le secteur de la sécurité, bon nombre d'autorités de certification dotent d'ores et déjà leurs certificats SSL de la technologie de chiffrement 2 048 bits, ce qui vient encore renforcer la protection des transmissions de données en ligne.

Les clients opérant des transactions sur les sites Web et systèmes protégés par la sécurité SSL n'en restent pas moins exposés à des menaces sérieuses. A cela, une raison majeure : la mauvaise gestion des certificats SSL. Les entreprises ayant à gérer des centaines de certificats issus de différents fournisseurs peuvent facilement en perdre la trace dans leur environnement. Dans ce cas, l'arrivée à expiration de tel ou tel certificat peut passer inaperçue pendant des mois, laissant les visiteurs du site à la merci des pirates.

Parfois, le premier signe indiquant qu'un certificat SSL a été "perdu" est l'appel d'un client qui, constatant l'expiration d'un certificat, se demande s'il est prudent pour lui de poursuivre ses achats sur le site. Il peut s'agir aussi d'un événement plus sérieux, par exemple, un incident de phishing permettant à des cybercriminels de détourner les informations sensibles des clients. Il arrive également qu'une faille de sécurité dans les systèmes d'une autorité de certification se répercute à l'échelle d'une entreprise, notamment quand celle-ci n'est pas en mesure de réagir assez rapidement en raison du manque de visibilité de son stock de certificats SSL.

Dans tous les cas de figure, perdre la trace des certificats SSL peut non seulement coûter très cher mais également nuire à la réputation de l'entreprise. Fort heureusement, la recherche et la gestion des certificats SSL n'est pas nécessairement une tâche complexe ou grande consommatrice de temps.

Le présent document technique passe en revue les problèmes induits par une mauvaise gestion des certificats SSL. Il montre quels dangers ces problèmes représentent pour les entreprises et comment celles-ci peuvent mettre en place un contrôle efficace de leurs certificats.

Défis liés à la gestion des certificats SSL

L'entreprise d'aujourd'hui est un environnement complexe englobant souvent plusieurs réseaux internes et des sites Web accessibles au public. Plusieurs dizaines (voire plusieurs centaines) de certificats SSL distincts peuvent donc être déployés au même moment dans une entreprise donnée.

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

Bien souvent, il s'agit en outre d'une combinaison de certificats différents les uns des autres et issus d'autorités de certification bien distinctes. Par exemple, une entreprise installera les certificats SSL d'un fournisseur aussi réputé que fiable sur son site Web accessible à la clientèle et déploiera des certificats auto-signés ou de marques à valeur ajoutée sur son Intranet.

Certaines autorités de certification fournissent des outils permettant de gérer leurs propres certificats mais ceux-ci procurent rarement la visibilité suffisante pour suivre l'ensemble des certificats d'un environnement, toutes autorités de certification confondues. Loin de faciliter l'administration, les divers portails de gestion rendent le suivi d'un grand nombre de certificats SSL issus d'autorités de certification différentes plus problématique encore. Les administrateurs doivent constamment surveiller leurs certificats SSL sur des systèmes multiples et regrouper leurs propres rapports pour obtenir une vue complète de leur stock de certificats.

Pour comble de difficulté, les politiques de sécurité mises en place par les entreprises exploitant des réseaux distribués varient parfois d'un groupe à l'autre. Par exemple, le Groupe A aura besoin de certificats SSL Extended Validation pour protéger les données dont il assure la gestion, tandis que le Groupe B fera appel à un autre type de certificats SSL, provenant d'une autorité de certification différente. Ou bien, autre scénario plus courant encore, le Groupe A aura besoin de certificats SSL 2 048 bits tandis que le Groupe B se contentera de certificats 1 024 bits. S'ajoutant à des politiques diversifiées et aucun moyen unique d'obtenir une vue complète des certificats SSL déployés dans l'entreprise, ces incohérences peuvent être la cause de risques pour la sécurité et du non-respect des exigences réglementaires ou internes.

Le problème est rendu encore plus aigu lorsque les employés en charge de la sécurité SSL changent de poste ou quittent l'entreprise. A moins que ceux-ci ne dressent la liste précise des certificats SSL dont ils assuraient la gestion et transmettent cette information aux autres membres de l'équipe, ces certificats risquent de passer inaperçus lorsque de nouveaux membres prennent la relève. Les équipes informatiques d'une entreprise étant surchargées de travail et souvent à cours de ressources, non seulement le suivi manuel des certificats SSL constitue un fardeau pour ces dernières mais il est propice à l'erreur humaine.

Tous ces facteurs créent un environnement dans lequel des certificats SSL peuvent être perdus ou passer inaperçus. La marche de l'entreprise peut s'en trouver perturbée et les risques pour la sécurité des clients accrus.

Dangers liés aux certificats corrompus ou arrivés à expiration

La présence d'un certificat SSL corrompu ou arrivé à expiration dans un environnement réseau peut avoir de graves répercussions. Un seul de ces certificats peut suffire pour exposer l'entreprise (et, plus grave encore, ses clients) aux agissements de cybercriminels. Les exemples ci-après ne représentent que quelques-uns des risques encourus en présence d'un certificat SSL corrompu ou obsolète.

Vol d'informations personnelles

Grâce aux nombreux titres de journaux qui, d'année en année, rendent compte des violations de données, et aux efforts de sensibilisation des associations de consommateurs, le grand public est plus que jamais conscient du danger que

représente le vol d'identité. Une étude récente a montré que 64 % des américains se sentaient "très concernés" ou "extrêmement concernés" par ce risque, 31 % d'entre eux se déclarant "extrêmement concernés".²

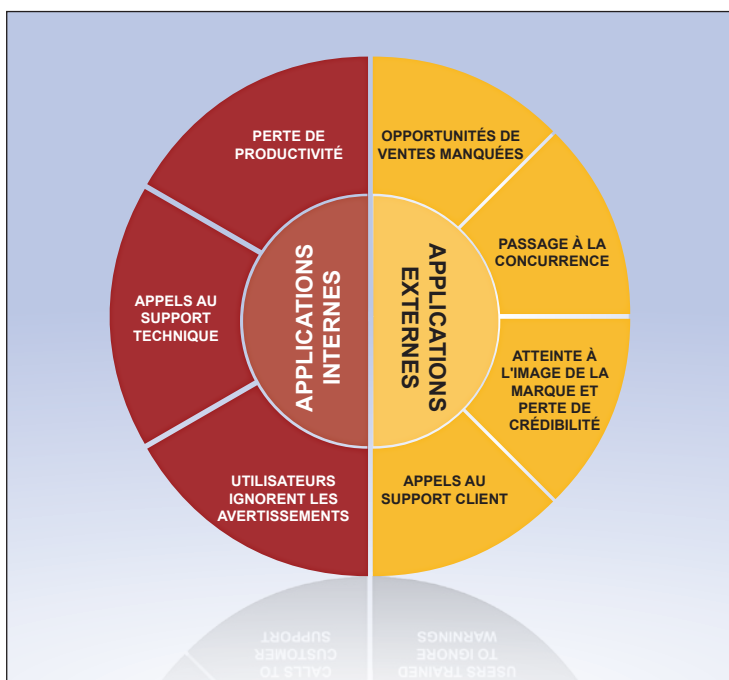
Dans ce contexte, le risque que représentent les attaques de phishing est une préoccupation majeure. Dans ce type d'attaque, un pirate détourne l'identité d'une entreprise légitime (en profitant d'une faille de sécurité due à l'absence ou à l'expiration de certificats SSL) et crée un faux site Web semblable, voire parfaitement identique, au site réel. Des clients peu méfiants accèdent à ce site et y saisissent des informations confidentielles, telles que leurs numéros de carte de crédit ou de sécurité sociale. Le site factice transmet alors directement ces données au pirate qui, éventuellement, les vend à d'autres cybercriminels.

Même lorsqu'il s'agit d'incidents mineurs, les attaques de phishing ou les violations de données peuvent exacerber les inquiétudes et constituer une sérieuse menace pour l'entreprise.

Au-delà de ces pertes immédiates, le phishing et les violations de données peuvent également entacher la réputation de l'entreprise et semer le doute parmi les clients et les prospects quant au niveau de confiance qui peut lui être accordé. Les experts estiment qu'après une violation de données, pas moins de six mois sont nécessaires pour stabiliser les ventes et rétablir la confiance des clients dans le réseau de l'entreprise³. Et même après tout ce temps, la réputation de la société reste souvent fragile.

Des violations de données de plus en plus coûteuses

Si le tort causé à la réputation d'une entreprise est parfois difficile à évaluer, l'impact économique de telles violations est plus simple à déterminer. Selon une récente étude américaine, le coût moyen des violations de données est évalué à 7,2 millions de dollars par événement, soit environ 214 dollars par enregistrement compromis,⁴ des chiffres qui, selon les prévisions, devraient continuer de croître.



Conséquences en cas d'expiration inattendue d'un certificat SSL et avertissements émis par les navigateurs

2. "Identity theft fears weigh on Americans" (La peur du vol d'identité saisit les Américains) par Tim Greene, Network World, 12/04/2010

3. "Sony Data Breach Exposes Users to Years of Identity-Theft Risk" (La faille de sécurité chez Sony expose pour des années les utilisateurs au risque de vol d'identité) par Cliff Edwards et Michael Riley, BusinessWeek.com, 3/05/11

4. "Cost of a data breach climbs higher" (Le coût des violations de données est en hausse), Ponemon Institute, ponemon.org, 8/03/11

Perte de clients au profit de la concurrence

L'expiration des certificats SSL constitue un autre sujet de préoccupation pour les entreprises. L'expiration d'un certificat SSL peut nuire à l'activité de l'entreprise de diverses autres manières. Le plus souvent, elle provoque tout simplement une baisse de trafic lorsqu'une fois informés de cette expiration par des messages d'avertissement, les clients quittent votre site afin de poursuivre leurs achats de produits et services sur des sites protégés par des certificats SSL valides.

Ne sachant pas toujours comment fonctionne exactement le chiffrement à clé publique, les clients se fient habituellement aux marques de sécurité SSL visibles (telles que la barre verte "Extended Validation" et le Sceau de confiance SSL) pour savoir s'ils peuvent naviguer en toute sécurité sur un site donné.⁵ Dans le cas d'un site marchand, ou autre type de site accessible au public, l'expiration de certificats SSL engendre une perte de confiance des clients qui se traduit par une baisse de chiffre d'affaires.

Multiplication des demandes d'assistance client

Aujourd'hui, bon nombre de sociétés offrent divers outils en ligne, menus téléphoniques automatisés et autres options de libre-service permettant aux clients d'obtenir des réponses à leurs questions. Cependant, lorsqu'un client en visite sur un site a un doute quant à la sécurité de ses données personnelles, soit il cesse toute transaction (comme nous l'avons vu plus haut), soit il contacte l'assistance clientèle.

Le coût par appel varie selon les secteurs d'activité mais il est un fait certain : si les appels sont nombreux, le cumul de ces coûts peut représenter une somme importante au fil du temps. Non seulement les appels d'assistance trop nombreux grèvent les ressources financières d'une entreprise mais ils alourdissent la charge du centre d'appel et détournent le personnel qui, pendant ce temps, n'est pas en mesure de répondre à des demandes de clients plus lucratives.

Les coûts et inconvénients liés aux appels à l'aide des clients peuvent facilement être évités par une mise à jour permanente du dispositif de sécurité, notamment des certificats SSL.

Pression accrue sur les départements informatiques

Tout comme les clients, qui contactent l'assistance clientèle en cas de doute sur la sécurité d'un site Web, les employés font souvent appel au département informatique lorsque des messages leur signalent l'expiration de certificats SSL. Ces demandes d'assistance constituent un fardeau supplémentaire pour des départements informatiques déjà débordés.

Parfois, les employés se contentent d'ignorer les avis d'expiration, ce qui a pour effet de laisser les ressources concernées sans protection en cas d'attaque. Cela crée également un précédent ennuyeux du point de vue du respect des règles de sécurité, car cela donne l'impression que le personnel a tendance à négliger les procédures de sécurité internes.

Ces deux scénarios peuvent être évités en assurant la mise à jour des certificats de sécurité SSL dans toute l'entreprise.

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

Pratiques reconnues en matière de gestion des certificats SSL

Fort heureusement, il existe des services qui facilitent la recherche et la gestion des certificats SSL dans toute l'entreprise. Certaines solutions sont supposées réduire la charge liée à la gestion SSL mais ne permettent pas de rechercher des certificats indépendamment des autorités de certification émettrices. D'autres permettent ce type d'analyse mais sont dépourvues d'une interface utilisateur intuitive facilitant la navigation.

Voici quelques-unes des fonctions clés à prendre en considération pour rechercher la solution qui répond le mieux à vos besoins :

- **Possibilité d'analyser automatiquement votre environnement** : bien qu'il soit possible d'analyser les réseaux manuellement, cette approche prend bien trop de temps et de ressources humaines pour être applicable à l'échelle de l'entreprise. Veillez à sélectionner un service qui permette à votre équipe d'effectuer des analyses automatiques capables de détecter tous les certificats SSL, quel que soit son fournisseur.
- **Interface conviviale** : les informations difficilement accessibles ou lisibles ne vous sont d'aucune utilité ; c'est pourquoi vous devez rechercher un outil qui facilite la navigation et présente les données de telle sorte qu'elles soient aisément compréhensibles au premier coup d'œil.
- **Capacités de délégation** : dans un environnement d'entreprise typique, la gestion de la sécurité est confiée à plusieurs employés. Il est donc essentiel de trouver une solution de recherche de certificats qui permette aux administrateurs d'octroyer plusieurs niveaux d'accès et de déléguer des tâches à divers employés, d'un bout à l'autre du réseau.
- **Alertes et reporting** : l'arrivée à expiration d'un certificat SSL rend les données vulnérables, aussi est-il important de trouver un service qui envoie des alertes avant que le renouvellement ne devienne urgent. Etre en mesure de générer des rapports faciles à lire et à comprendre est également essentiel. Avec des fonctionnalités de reporting avancées, vous disposerez d'une vue approfondie et complète des certificats de votre réseau et votre équipe transmettra plus efficacement les informations importantes aux autres membres du personnel (les cadres de la société, par exemple).
- **Flexibilité et évolutivité** : les réseaux d'entreprise étant des environnements dynamiques en constante évolution, votre service de recherche de certificats devra être doté de paramètres configurables tels que la durée de l'analyse, les adresses IP à configurer, etc. Ce service devra en outre être évolutif, en prévision d'une croissance future.
- **Rapidité** : l'analyse d'un réseau ne peut être efficace que si elle est rapide. Si cette analyse prend trop de temps, le statut de certains certificats SSL risque de changer avant qu'elle ne s'achève. Il en résultera une vue inexacte du stock de certificats SSL.

Conclusion

Les certificats SSL jouent un rôle essentiel dans la protection des données en transit. En dépit de son efficacité et de sa fiabilité, la sécurité SSL reste en partie perméable aux attaques pour une raison bien simple : la mauvaise gestion des certificats SSL.

Dans un environnement comptant de nombreux certificats issus d'autorités de certification différentes, une vue exhaustive de la sécurité SSL est indispensable. Connaître le statut de tous les certificats déployés sur les sites et réseaux permet de mieux maîtriser les coûts de service client mais aussi d'alléger l'administration de la sécurité SSL. Les équipes informatiques surchargées de travail disposent ainsi de plus de temps pour les autres projets stratégiques de l'entreprise.

Une gestion rigoureuse des certificats SSL permet également de prévenir des risques beaucoup plus graves, tels qu'un incident de phishing majeur ou toute autre violation de données. De tels incidents peuvent non seulement s'avérer très coûteux mais aussi ternir pour longtemps votre réputation auprès des clients.

Symantec® Certificate Intelligence Center : Recherche et gestion efficaces des certificats SSL

Le Symantec Certificate Intelligence Center aide les administrateurs à rechercher et gérer les certificats SSL plus efficacement. Offrant une visibilité élargie et de puissants moyens de gestion, le Symantec Certificate Intelligence Center facilite le suivi des certificats SSL.

Son interface intuitive permet aux administrateurs de configurer des analyses automatiques autorisant une recherche rapide des certificats, quelle que soit l'autorité émettrice. Les utilisateurs peuvent également configurer des alertes qui préviennent les administrateurs lorsque l'expiration des certificats SSL devient imminente.



Le tableau de bord convivial du Symantec Certificate Intelligence Center

Solution évolutive, le Symantec Certificate Intelligence Center s'adapte aux changements rapides du réseau tandis que l'entreprise se transforme et prend de l'ampleur. Les fonctionnalités de reporting avancées procurent en outre aux responsables une visibilité complète de la sécurité SSL, au travers de données simples à comprendre et à transmettre dans toute l'entreprise.

Pour découvrir comment le Symantec Certificate Intelligence Center peut simplifier la recherche et la gestion de vos certificats SSL, rendez-vous sur le site <http://www.verisign.fr/ssl/symantec-certificate-intelligence-center/index.html>

Informations supplémentaires

Visitez notre site Web

<http://www.verisign.fr>

Pour contacter un spécialiste produit

0800 90 43 51 ou

+41 (0) 26 429 77 24

A propos de Symantec

Symantec est un leader mondial des solutions de sécurité, de stockage et de gestion des systèmes pour aider les particuliers et les entreprises à sécuriser et gérer leur environnement informatique. Nos logiciels et services permettent d'assurer une protection plus complète et plus efficace contre davantage de risques à différents points et d'instaurer ainsi la confiance, quel que soit l'endroit où les informations sont utilisées ou stockées. La société Symantec, dont le siège social est basé à Mountain View en Californie, est présente dans 40 pays. Des informations supplémentaires sont disponibles à l'adresse www.symantec.fr.

Symantec

Tour Egée,

17, avenue de l'Arche

92671 Courbevoie Cedex,

France



Services d'authentification
VeriSign