Le paysage du SSL

Conseils en matière de gestion des certificats pour mener à bien une mutation capitale

Résumé : le paysage du SSL évolue et une gestion fragmentée peut coûter cher aux entreprises

Avec le raccourcissement imminent des cycles de renouvellement des certificats SSL (Secure Sockets Layer), les entreprises ne peuvent pas se permettre de retarder la transition vers l'automatisation des certificats. Elles ne peuvent pas non plus se permettre de compromettre la sécurité de leurs noms de domaine avec une gestion fragmentée des certificats SSL.

La sécurité des noms de domaine est sur le point d'entrer dans la phase de mutation la plus importante de son histoire. Les entreprises risquent alors d'accuser un retard considérable en matière de protection de leurs marques en ligne et de leurs identités numériques. Plus concrètement, la suppression de la validation des e-mails WHOIS en ce début d'année, ainsi que le raccourcissement imminent de la durée de validité des certificats et des périodes de réutilisation de la validation du contrôle de domaine (DCV) à compter de mars 2026, entraîneront des changements majeurs dans le fonctionnement des entreprises.

D'ici 2029, la durée de vie des certificats SSL et TLS (Transport Layer Security) passera de 367 jours à seulement 47 jours, ce qui signifie que les entreprises habituées à disposer d'environ un an pour renouveler un certificat devront désormais le faire près de huit fois par an. Par ailleurs, les périodes de réutilisation du DCV passeront de 367 jours à seulement 10 jours d'ici 2029.

Ces évolutions surviennent à un moment où les certificats DV, peu coûteux et faciles à obtenir, dominent le marché. Les cybercriminels profitent de ces certificats bon marché ou gratuits pour donner une apparence authentique à leurs sites Web frauduleux lorsqu'ils usurpent l'identité de marques en utilisant les mêmes types de certificats, afin d'inciter les clients à cliquer sur des liens malveillants et à compromettre leurs données.

D'autre part, certaines entreprises accordent une importance croissante à la sécurité ; toutefois, notre rapport annuel intitulé « Rapport sur la sécurité des noms de domaine » révèle qu'une grande partie des entreprises sont encore exposées à des risques majeurs liés à la sécurité des noms de domaine. Nos recherches ont révélé que plus des deux tiers de toutes les entreprises du Global 2000 ont mis en place moins de la moitié des mesures de sécurité recommandées.

Pour ce rapport « Paysage du SSL », nous avons analysé les tendances et les modèles d'utilisation de plus de 802 000 certificats numériques liés à 2,4 millions de noms de domaine afin de comprendre comment les entreprises supervisent les certificats SSL et comment cela influe sur la garantie d'intégrité de ces noms de domaine. Nos recherches et nos échanges avec des dirigeants d'entreprise nous ont permis de constater que les entreprises ignorent ou retardent la mise en place d'une réponse stratégique au raccourcissement des cycles de vie des certificats SSL et des périodes de réutilisation DCV. Ce rapport offre un aperçu détaillé de ces problèmes, ainsi que des mesures à prendre pour les éviter.

Trop de marques optent pour des certificats plus faciles à obtenir

Un certificat SSL authentifie la légitimité et la sécurité d'une marque en ligne, en validant les informations d'identification du certificat et en chiffrant la connexion entre le serveur d'un site Web et le navigateur d'un utilisateur.

Les certificats SSL présentent deux fonctions principales :

- **La sécurité :** le chiffrement assure la protection des identifiants de connexion, des numéros de carte de crédit et d'autres données sensibles.
- **La confiance :** les utilisateurs font confiance à un site certifié, détenu par une entité légitime qui le gère, et dont le transfert de données est sécurisé. Le niveau d'authentification varie selon les niveaux de validation d'un certificat.

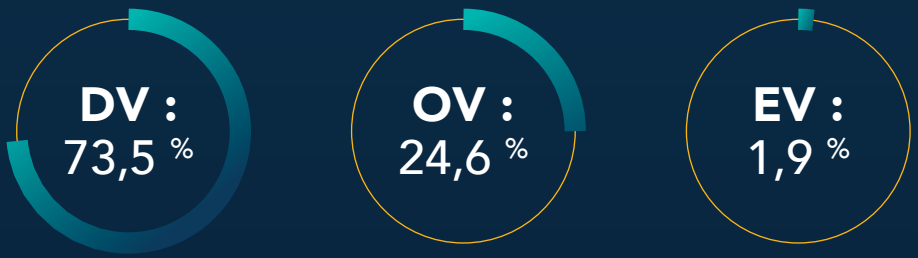
Nos recherches révèlent toutefois que cet état idéal de sécurité et de confiance constitue davantage l'exception que la norme ; en effet, la grande majorité des marques en ligne choisissent des types de certificats plus faciles à obtenir afin de réduire la charge de travail et de gagner du temps.

Il existe trois niveaux de validation du certificat SSL :

- **La validation de domaine (DV).** Il s'agit des certificats les moins chers et les plus rapides à obtenir. Une validation de domaine (DV) vérifiera uniquement que l'acheteur du certificat contrôle le nom de domaine. Tout titulaire d'un nom de domaine peut obtenir un certificat SSL, quelle que soit l'utilisation qu'il compte faire de ce nom de domaine.
- **La validation d'organisation (OV).** La validation d'organisation (OV) remplit les mêmes fonctions que la validation de domaine (DV) tout en authentifiant certaines informations relatives à l'entreprise, telles que son certificat d'enregistrement commercial.
- **La validation étendue (EV).** Le certificat de validation étendue (EV) est le plus complet et le plus rigoureux des certificats, renforcé par une vérification approfondie des capacités juridiques, physiques et opérationnelles de l'entreprise.

Dans le cadre de nos recherches, nous avons constaté que les DV représentent les trois quarts (73,5 %) des certificats, contre près d'un quart (24,6 %) de certificats OV. Les certificats EV représentent moins de 2 % (1,9 %).

Distribution par types de certificats :



Au vu de la distribution, il n'est pas surprenant que les certificats DV soient les plus populaires, car ils sont plus faciles et plus rapides à acheter. Lorsque les entreprises font appel à des fournisseurs proposant ces certificats à bas prix, les cybercriminels peuvent utiliser les mêmes certificats provenant des mêmes fournisseurs pour légitimer leurs sites frauduleux et gagner la confiance des utilisateurs grâce au protocole HTTPS (Hypertext Transfer Protocol Secure). Les fraudeurs ont gagné en technicité par rapport à l'époque où les sites Web frauduleux comportaient des fautes de frappe et des erreurs grammaticales. Les acteurs malveillants sont très doués pour dissimuler leur identité, et la facilité d'accès aux certificats DV ne fait que renforcer leur capacité à se faire passer pour des entreprises légitimes.

Historiquement, les sites utilisant des certificats EV affichaient une barre verte indiquant aux visiteurs que le site était sécurisé par une entreprise ayant fait l'objet d'une vérification approfondie. L'indicateur de barre verte n'est plus pris en charge par les principaux navigateurs, ce qui a entraîné une baisse de l'adoption des certificats EV.

Ces données soulèvent plusieurs questions : les services informatiques ont-ils une stratégie claire concernant le type de certificat à obtenir pour chaque type de ressource Web ? Ou bien acquièrent-ils simplement des certificats DV par facilité et rapidité ?

Plusieurs fournisseurs entraînent des risques multiples

Nombre de fournisseurs	% d'entreprises analysées
1	22,4 %
2	18,5 %
3	16,6 %
4	15,8 %
5	12,2 %
6	7,4 %
7	4,1 %
8	1,9 %
9	1,0 %
10 ou plus	0,3 %

Nos recherches montrent que près de **60 % des entreprises** font appel à au moins trois fournisseurs de certificats, et qu'une entreprise en comptait même 13.

Le classement ci-dessus révèle que la grande majorité des entreprises a recours à plusieurs fournisseurs de certificats.

En réalité, environ 60 % des entreprises font appel à trois fournisseurs ou plus, ce qui peut engendrer d'importants problèmes de gestion. Cette situation peut aboutir à l'absence d'une approche centralisée et à des processus fragmentés et contre-productifs, dont l'impact se fera sentir de manière exponentielle avec le raccourcissement des cycles de vie et des périodes de réutilisation des DCV.

Le recours à un seul fournisseur accélère considérablement le renouvellement des certificats et la résolution des problèmes, tout en améliorant leur efficacité. Avec un seul fournisseur, dès qu'un problème lié au protocole SSL survient, les membres de l'équipe de sécurité n'ont qu'à se tourner vers un seul et même endroit pour le résoudre.

Par ailleurs, collaborer avec un seul fournisseur permet de réduire les risques. Plutôt que de jongler entre plusieurs dates limites de renouvellement émanant de divers fournisseurs, un seul fournisseur fiable garantit des notifications de renouvellement en temps utile. La gestion par de multiples fournisseurs peut également entraîner une perte de rentabilité par rapport à ce que peut procurer la centralisation des certificats autour d'un seul fournisseur.

Les principaux fournisseurs ne sont pas des entreprises professionnelles spécialisées

Les trois principaux fournisseurs de certificats :

Let's Encrypt, Google®, et Amazon®

Total combiné : 66 % de tous les certificats analysés

Ces trois fournisseurs délivrent la majorité des certificats DV (89 %) utilisés par les entreprises analysées. Leurs offres à bas prix séduisent les entreprises qui cherchent à réduire leurs dépenses, cependant elles constituent également une excellente source de certificats pour les noms de domaine frauduleux que l'équipe chargée de la lutte anti-fraude de CSC a supprimés. Cette accessibilité qui attire les honnêtes entreprises est également à la portée des acteurs malveillants.

Principaux fournisseurs de certificats de noms de domaine frauduleux démantelés par CSC :

Google | Let's Encrypt | Cloudflare® | Amazon

En quête de rentabilité et de rapidité, les entreprises optent pour ces fournisseurs grand public. Cependant, ceux-ci ne garantissent pas l'assistance corporate professionnelle nécessaire pour aider les entreprises à se préparer aux évolutions futures du secteur SSL. Cette approche à court terme engendre également des complications inutiles en raison du raccourcissement des cycles de renouvellement des certificats.

Les entreprises ne peuvent se permettre d'ignorer ou de retarder leurs préparatifs pour cette période de 47 jours. En attendant la dernière minute, celles-ci devront faire face à une transition extrêmement complexe et perturbatrice. Elles risquent de ne pas être en mesure de faire face à la fréquence accrue des renouvellements de certificats et des DCV. Les renouvellements manqués pourraient entraîner la panne de noms de domaines et d'applications entiers, fondement même des opérations commerciales.

En anticipant et en faisant appel à un fournisseur de certificats SSL corporate professionnel, les entreprises éviteront des situations stressantes et coûteuses. Un partenaire expérimenté proposera une stratégie proactive et efficace en matière de certificats ; il fournira des outils d'automatisation pour remplacer les processus manuels chronophages et garantira une absence totale d'interruptions dues à une expiration. Grâce à ces outils, un agent peut demander, recevoir et installer un certificat dans le cadre d'un processus de renouvellement automatisé.

Toutefois, l'intégration des outils d'automatisation dans les systèmes demande du temps. Il ne suffit pas de les acheter dans le commerce et de les installer, il faut aussi tenir compte de certaines nuances. Par exemple, les composants du système actuel peuvent ne pas être compatibles avec les outils, obligeant ainsi les entreprises à les remplacer. Voilà pourquoi ignorer ou déprioriser les cycles de renouvellement plus rapides conduira à un chaos évitable et coûteux.

Trois étapes vers une automatisation optimale

Soucieuses d'éviter les interruptions dues à une expiration, les entreprises reconnaissent progressivement leur incapacité à gérer les certificats SSL sans automatisation. Elles ont tenté de procéder manuellement, en suivant les expirations à venir à l'aide de tableurs et en gérant les tarifs de renouvellement annuels actuels. Mais le paysage est sur le point de changer, et c'est là que l'automatisation entre en jeu.

Comme nous l'avons mentionné, l'intégration automatisée n'est pas une mince affaire. La multiplication des fournisseurs de certificats et des négligences au fil du processus engendrera des blocages et une véritable lourdeur. Pour maintenir efficacement le cap, nous recommandons les étapes suivantes :

Standardisez et documentez les processus.

Les collaborateurs se succèdent. Les situations évoluent. Néanmoins, la gestion des certificats nécessite des pratiques normalisées qui demeurent cohérentes au fil du temps. Avant de passer à l'intégration automatisée, veillez à mettre en œuvre ces pratiques et à les documenter afin que les collaborateurs actuels et futurs puissent les suivre. Incluez les difficultés rencontrées en cours de route afin que les collaborateurs soient informés des problèmes survenus et de la méthode employée pour les résoudre.

Formez-vous et formez vos collaborateurs.

De nombreux éléments de l'automatisation doivent être assimilés avant même leur mise en œuvre. Le fait de s'associer à un seul fournisseur de certificats expérimenté facilite grandement le processus d'apprentissage ; ce fournisseur connaît bien ces composants et saura sensibiliser les clients en conséquence.

Un fournisseur unique peut, par exemple, conseiller ses clients dans leur décision d'acheter une « solution d'automatisation à grande échelle » ou opter pour une solution moins coûteuse et moins ambitieuse. Plusieurs outils informatiques sont disponibles, certains en open source et d'autres conçus avec des interfaces de programmation d'applications (API) de fournisseurs, qui se sont imposés comme des alternatives à une solution unique globale. Un fournisseur hautement qualifié permet aux clients de prendre des décisions éclairées quant aux démarches à entreprendre.

Pensez à tout prendre en compte.

Dans le cadre d'une initiative d'intégration automatisée, les équipes omettent parfois certains éléments. C'est une erreur. Une approche fragmentaire entraîne inévitablement des lacunes flagrantes qui entraveront le succès de l'intégration. Il est donc essentiel de prendre en compte l'intégralité du flux de travail.

Conclusion

Les certificats sont omniprésents et les entreprises ne peuvent s'en passer. Un simple message d'avertissement indiquant qu'un site n'est pas sécurisé suffit à faire fuir les clients vers la concurrence. Pourtant, la plupart des entreprises ne maîtrisent pas correctement leur inventaire de certificats. Au vu des évolutions prévues dans le secteur, les entreprises sont contraintes de mettre en place des systèmes d'automatisation et de s'y préparer.

La convergence du raccourcissement des cycles de vie et des périodes de réutilisation du DCV laisse présager une cyber-tempête sans précédent : les entreprises qui tardent à planifier leur renouvellement devront faire face à des coûts et des risques supplémentaires lors de leur passage aux nouvelles normes. En décidant de centraliser vos solutions auprès d'un seul partenaire certifié et éprouvé, vous bénéficierez d'une transition plus fluide et plus sûre, optimisée par l'automatisation.

Découvrez la gamme flexible de solutions de gestion des certificats numériques de CSC destinée aux entreprises présentant des besoins variés.

Discutons +33 (0)1 40 41 65 30 | cscdbs.com/fr

À propos de CSC

CSC est le partenaire de confiance des entreprises du classement Forbes Global 2000 (Interbrand®) et 100 Best Global Brands en matière de sécurité et de veille sur les menaces et propose des solutions de gestion de la sécurité des domaines et, de protection des marques en ligne et contre la fraude. Les entreprises internationales investissent considérablement dans leur stratégie de sécurité. C'est la raison pour laquelle notre plateforme DomainSec℠ peut les aider à identifier leurs failles en matière de cybersécurité et leur permettre de protéger leurs actifs numériques et leurs marques en ligne. En s'appuyant sur la technologie exclusive de CSC, les entreprises peuvent consolider leur stratégie de sécurité pour se protéger contre les vecteurs de cybermenaces qui pèsent sur leur patrimoine numérique, et éviter les pertes de revenus catastrophiques et les atteintes à la réputation de leurs marques. CSC propose également une protection de la marque en ligne (une combinaison de la surveillance de la marque en ligne et des activités de mise en œuvre) et une vue multidimensionnelle des différentes menaces à l'extérieur du pare-feu ciblant des noms de domaine spécifiques. Des services de protection contre la fraude, qui luttent contre l'hameçonnage dès les premiers stades de l'attaque, viennent compléter nos solutions. Basée à Wilmington (Delaware) aux États-Unis depuis 1899, CSC possède des bureaux sur tout le territoire des États-Unis, mais également au Canada, en Europe et dans la région Asie-Pacifique. CSC est une entreprise d'envergure mondiale, ce qui nous permet d'intervenir là où sont nos clients en mettant à leur disposition nos équipes d'experts dans chacune de nos activités. Consultez notre site à l'adresse suivante : cscdbs.com/fr.

DBS02132026