Conformité : prenez les devants

ADOPTEZ UNE APPROCHE MÉTHODIQUE DE LA SÉCURITÉ WEB ET DE LA CONFORMITÉ RÉGLEMENTAIRE

Conformité : prenez les devants

Introduction : meneur ou suiveur, la balle est dans votre camp

La conformité constitue non seulement un enjeu majeur, mais aussi un véritable défi pour les entreprises. Dans une étude réalisée par le consortium IT Policy Compliance Group, dont la mission consiste à aider les professionnels de la sécurité informatique à atteindre leurs objectifs en matière de politique et de conformité réglementaires, 70 % des sondés se disaient soumis à de multiples dispositifs réglementaires, auxquels s'ajoutent des obligations contractuelles et autres normes sectorielles.[1]

Parallèlement, les pressions budgétaires se font croissantes, conséquence directe d'une conjoncture économique difficile qui contraint les entreprises à agir sur les coûts. Par ailleurs, l'émergence des services Cloud complique encore davantage le casse-tête de la conformité. Face à ces défis et aux délais particulièrement serrés, de nombreuses entreprises optent pour une approche cloisonnée, axée sur de simples checklists.

Ce choix délibéré de la réactivité s'avère néanmoins contre-productif, puisqu'il engendre, à terme, une augmentation des coûts de conformité, une hausse des manquements constatés lors des audits, une multiplication des interruptions de service et des risques accrus de perte de données. Pour éviter ces écueils et gagner une longueur d'avance dans un environnement réglementaire en constante évolution, les entreprises ont donc besoin de solutions qui les aident à mettre en œuvre une approche résolument proactive. Elles deviendront ainsi les actrices — et non plus les spectatrices — de leur conformité.

Conformité et effet « 2.0 »

De nombreuses entreprises peinent encore à se conformer à la kyrielle d'obligations réglementaires qui ont vu le jour au cours des 15 dernières années. Des lois SOX (Sarbanes-Oxley), GLBA (Gramm-Leach-Bliley Act), HIPAA (Healthcare Information Portability and Accountability Act) au standard PCI (Payment Card Industry) et autres directive européennes, la liste semble s'allonger à l'infini. À cela s'ajoute aujourd'hui une nouvelle vague de règlementations qui viennent pour la plupart renforcer, voire modifier les obligations existantes, comme l'illustre le tableau 1. Devant un tel constat, les entreprises doivent se rendre à l'évidence : l'utilisation de checklists et les stratégies de gestion cloisonnée de la sécurité et de la conformité ne leur permettent plus de faire face à ces évolutions constantes.

Tableau 1. Exemples de règlementations « 2.0 » et conséquences sur la sécurité informatique et la conformité

Règlementation	Date	Obligations/conséquences
BÂLE II	2009	Obligation pour les banques de recourir à un dispositif de cryptage afin de limiter les risques de divulgation ou d'altération de données sensibles stockées ou en transit.
FISMA 2.0	2010	Obligation d'exercer une surveillance continue des systèmes informatiques dans le cadre du programme de sécurité de l'information imposé aux agences fédérales américaines. Les DSI des agences concernées avaient jusqu'à la fin de l'exercice fiscal 2012 pour mettre en œuvre des logiciels de surveillance continue de la sécurité de leurs réseaux.
PCI DSS 2.0	2011	Nouvelle norme encadrant les programmes de sécurité des règlements par carte, entrée en vigueur début 2011. Les entreprises avaient l'obligation de passer à la nouvelle version avant début 2012.
Loi HITECH	2011	Obligation pour les prestataires de santé, assureurs, centres d'échanges d'informations et partenaires de parvenir à une « utilisation pertinente » des technologies de gestion des dossiers médicaux électroniques, d'ici fin 2015. En cas de violation des données, les organismes sont tenus d'informer l'ensemble des personnes concernées dans un délai de 60 jours, à moins que les données soient « indéchiffrables », à savoir protégées à l'aide d'un cryptage fort.

1. Symantec : « Financial Services Information Security and IT Risk Management », 2008 - http://eval.symantec.com/mktginfo/enterprise/brochures/b-brochure_financial_services_10_2008_14163207.en-us.pdf

De la fragmentation des règlementations sur la cybersécurité

Tout a commencé en 2003, avec la loi californienne sur la confidentialité des informations personnelles (SB1386). Son entrée en vigueur déclencha à l'époque un véritable effet boule de neige qui vit l'adoption par d'autres États de nouvelles lois en matière de notification des atteintes à la protection des données. À tel point qu'aujourd'hui, la quasi-totalité des États américains se sont dotés de dispositifs juridiques comparables à la loi SB1386. Ainsi, le Massachusetts a promulgué une législation préventive obligeant les personnes physiques ou morales, qui stockent ou utilisent des informations personnelles, à mettre en place un dispositif de protection des données documenté, faisant l'objet d'audits réguliers[2]. Une source de complexité accrue pour les entreprises dont les activités dépassent les frontières de leur État.

Autre exemple de la propagation pandémique de ce type de législation : la directive européenne relative à la protection des données à caractère personnel (1995/46/CE)[3]. Ce texte établit des principes communs de protection et de confidentialité des données et fixe un cadre réglementaire que chaque État membre de l'UE doit ensuite transposer dans sa propre législation nationale.

Pour se conformer à ces lois, les entreprises doivent prendre les mesures nécessaires — qu'elles soient d'ordre technique ou procédural — en vue d'empêcher tout traitement non autorisé ou illicite et de prévenir tout risque de perte ou de destruction des données personnelles. Par ailleurs, ces lois interdisent le transfert de données à caractère personnel vers un pays ou territoire situé en dehors de l'Espace économique européen, à moins qu'il assure un niveau adéquat de protection des droits et des libertés des personnes concernées par le traitement de ces données.

Dans le monde, plusieurs États ont légiféré sur la protection et la confidentialité des données en vue de faciliter l'accès aux marchés européens. Leurs lois suivent généralement les dispositions de la directive européenne 1995/46/CE, lui conférant *de facto* un statut de standard international en la matière. Dans la grande majorité des cas, elles exigent le recours à des mécanismes de contrôle technique, de type cryptage, afin de protéger les données personnelles contre les risques de vol, de perte et d'exposition.

Tableau 2. Exemples de législations en matière de protection et de confidentialité des données dans le monde

Pays	Législation	Année
Argentine	Loi sur la protection des données personnelles	2000
Chili	Loi sur la protection de la vie privée	1999
Hong Kong	Ordonnance relative à la confidentialité des données personnelles[4]	1996
Japon	Loi sur la protection des informations personnelles	2003
Taïwan	Loi sur la protection des données personnelles traitées par voie informatique	1995
Singapour	(Proposition de) loi en faveur de la protection des données[5]	2012
Afrique du Sud	Loi sur les communications et les transactions électroniques[6]	2002
Corée du Sud	Loi sur la promotion de l'utilisation des réseaux d'information et de communication et la protection de l'information[7]	2002
Inde	Dispositions relatives aux technologies de l'information (pratiques et procédures de sécurité raisonnables et réglementation concernant les données et informations personnelles sensibles)[8]	2011

2. Commonwealth of Massachusetts : « 201 CMR 17.00 Compliance Checklist », décembre 2009 - http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf

3. Union européenne : Directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, novembre 1995 - http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

4. G&A Management Consultants Limited : « Privacy of Personal Data in Hong Kong » - http://privacy.com.hk/

5. ZDNet Asie : « S'pore sets data protection law for 2012 », 16 février 2011 - http://www.zdnetasia.com/spore-sets-data-protection-law-for-2012-62206733.htm

6. Parlement de la République d'Afrique du Sud : « Electronic Communications and Transactions Act, 2002 », 31 décembre 2001 - http://www.internet.org.za/ect_act.html

7. Réseau d'information en ligne de l'Organisation des Nations Unies sur l'administration et les finances publiques : « Act on Promotion of Information and Communication Network Utilization and Information Protection », 31 décembre 2001 - http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf

8. BNA International Global Law Watch : « Analysis: Data Privacy in India », 23 mai 2011 - http://www.globallawwatch.com/2011/05/analysis-data-privacy-rules-in-india/

Conformité + Cloud Computing = Complexité[9]

Le Cloud Computing figure en tête des priorités de nombreux DSI[10]. Pour preuve, l'adoption des services Cloud s'accélère en entreprise, à tel point que Gartner Research estime qu'au cours des prochaines années, les dépenses cumulées dans ce domaine devraient atteindre 112 milliards de dollars US à l'échelle planétaire[11].

Parallèlement, d'après une enquête IDC réalisée auprès de dirigeants informatiques, la sécurité arrive en tête des freins à l'adoption de services Cloud[12]. De son côté, Gartner Research identifie sept facteurs de risque de sécurité[13] associés au Cloud Computing en entreprise. Le tableau 3 énumère ces sept points et leurs implications à l'heure du choix d'un service Cloud.

Tableau 3. Le Cloud Computing et ses sept facteurs de risque de sécurité selon Gartner

Problème	Enjeu
Responsabilité	Les entreprises sont responsables de la sécurité et de la confidentialité des données électroniques protégées, même lorsque ces dernières sont hébergées par un fournisseur de services Cloud tiers.
Contrôle des accès	Les entreprises doivent s'assurer que leurs fournisseurs de services Cloud ont instauré des procédures d'embauche, de supervision et de contrôle des accès adaptées à la délégation des opérations d'administration.
Provenance des données	De nombreux fournisseurs SaaS font appel à des solutions de stockage basées sur le Cloud (Amazon, Rackspace, etc.) et certains ont recours à des services de datacenter en dehors de leurs frontières. Par conséquent, les entreprises doivent interroger leurs fournisseurs sur la localisation de leurs datacenters et leur adhésion à une charte de confidentialité rigoureuse.
Architectures multi-locataires	Nombre de Clouds publics sont hébergés dans des environnements mutualisés. Dans ce contexte, les hébergeurs doivent garantir la ségrégation des données et l'isolation du réseau, pour une sécurisation complète de l'architecture multi-locataires (« multi-tenant »).
Restauration des données	Le Cloud Computing n'est pas à l'abri d'éventuelles défaillances. Les entreprises doivent donc s'assurer qu'en cas de sinistre, leur fournisseur sera capable de restaurer rapidement l'ensemble des données et des services.
Surveillance et reporting	La surveillance et la journalisation de l'activité du Cloud public sont particulièrement complexes. Il incombe donc aux entreprises de vérifier en amont que leur fournisseur de services Cloud est en mesure non seulement de surveiller le trafic sur les réseaux physique et virtuel, mais aussi de procéder aux investigations et aux audits de conformité nécessaires.
Continuité d'activité	Les acteurs du secteur technologique — en particulier les start-ups — vont et viennent. Par conséquent, les entreprises doivent se renseigner de manière concrète sur la stabilité financière de leurs interlocuteurs, ainsi que sur la portabilité de leurs données. Avec un double objectif : d'une part, éviter tout phénomène d'enfermement et, d'autre part, se prémunir contre la perte de données en cas de faillite ou de rachat du prestataire.

9. Commonwealth of Massachusetts : « 201 CMR 17.00 Compliance Checklist », décembre 2009 - http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf

10. Gartner Research : « EXP Worldwide Survey », 19 janvier 2010 - http://www.gartner.com/it/page.jsp?id=1283413

11. Gartner Research : « Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010 », 22 juin 2010 - http://www.gartner.com/it/page.jsp?id=1389313

12. IDC Research : « New IDC IT Cloud Services Survey: Top Benefits and Challenges », 15 décembre 2009 - http://blogs.idc.com/ie/?p=730

13. Gartner Research : « Assessing the Security Risks of Cloud Computing », 3 juin 2008 - (http://www.gartner.com/DisplayDocument?id=685308

Autre point de complication, lorsque les entreprises passent d'un service Cloud unique à une multitude de services gérés par divers fournisseurs, elles doivent faire face à une multiplication des problèmes chez des opérateurs dotés d'infrastructures, de politiques d'exploitation et de compétences différentes en matière de sécurité. Devant la complexité des enjeux de confiance et de conformité qui entourent le Cloud, une méthode universelle et fiable doit s'imposer pour sécuriser les données en transit vers le Cloud, en provenance du Cloud ou en périphérie du Cloud.

La solution : une approche méthodique de la sécurité et de la conformité réglementaire

Les certificats SSL et de signature de code protègent les transactions et les données en ligne via des mécanismes d'authentification, de cryptage et de vérification d'identité. Dans un contexte d'expansion et d'évolution constantes du cadre réglementaire, ces solutions ont connu un essor fulgurant.

Conséquence : la prolifération de certificats sur différents sites rend leur administration et leur gestion particulièrement difficiles pour les entreprises. Sans oublier la rotation des effectifs informatiques, qui peut entraver le contrôle et l'identification des administrateurs techniques ou de toute autre personne disposant d'un accès aux certificats.

Parallèlement, les budgets informatiques sont régulièrement revus à la baisse, tandis que les exigences de conformité aux politiques de sécurité internes et externes vont croissant. Or, pour maîtriser leur parc étendu de certificats SSL et de signature de code, les DSI se trouvent face à un certain nombre d'enjeux que nous détaillons dans le tableau 4.

Tableau 4. Enjeux de la gestion des certificats SSL et de signature de code

Problème	Enjeu
Visibilité et contrôle	L'étendue et la ségrégation des réseaux d'une part, la diversité des opérations d'autre part, placent les administrateurs devant une double difficulté : déterminer la situation exacte de chaque certificat détenu par l'entreprise et gérer leur cycle de vie de manière homogène. La plupart des fournisseurs ne proposent pas de référentiel central pour le suivi et la gestion des certificats. Or, les processus manuels, basés sur des tableurs ou sur SharePoint, ne se prêtent pas à une gestion à grande échelle et sont sources d'incohérences et de surcoûts.
Continuité d'activité	L'expiration impromptue des certificats peut perturber les activités des entreprises et accroître les appels au support technique. Dans une telle situation, les entreprises ne sont pas à l'abri d'une défaillance majeure de leurs systèmes en ligne, avec à la clé un manque à gagner considérable. De même, si elles tardent à renouveler leurs certificats expirés, elles s'exposent à des sanctions pour non-conformité, sans parler de la détérioration de leur image de marque.
Opérations informatiques	Lorsqu'elle relève d'un processus manuel, la gestion trans-entreprise des certificats SSL et de signature de code s'avère fastidieuse et chronophage. Nombre d'administrateurs informatiques doivent piloter un vaste écosystème d'applications et de systèmes d'exploitation, avec chacun des modes de gestion hétérogènes. Dans ce contexte, le suivi de la localisation et de la date d'expiration de chaque certificat peut rapidement tourner au casse-tête, en particulier lorsqu'ils émanent de différents fournisseurs.

La solution : simplifier les processus, accroître l'efficacité opérationnelle et limiter les risques.

Comment prendre les devants en matière de conformité

Pour adopter une approche résolument proactive de la conformité et de la sécurité sur le Web, les entreprises doivent s'appuyer sur une solution qui leur permette de gérer l'ensemble de leurs certificats SSL et de signature de code à partir d'un point de contrôle central et sécurisé. Nous dressons ici un rapide inventaire des critères à prendre en considération pour déterminer la solution adaptée à vos besoins :

SCAN AUTOMATIQUE

S'il est possible d'auditer les réseaux manuellement, une telle approche monopolise beaucoup trop de temps et de ressources pour être envisageable dans un environnement d'entreprise étendu et complexe. Optez pour un service capable de lancer des scans automatiques afin de détecter l'ensemble des certificats émis par les différents fournisseurs.

PROCESSUS AUTOMATISÉS

Dans les grandes entreprises, l'émission, le renouvellement et l'installation de certificats SSL et de signature de code ne peuvent s'effectuer manuellement. Vous avez donc besoin d'une solution capable d'améliorer votre productivité via l'automatisation des principaux processus d'administration — tels que les processus d'approbation des demandes de certificats — et d'acheminer les demandes à l'administrateur concerné. À la clé : des économies de temps et d'efforts.

ALERTES, RAPPORTS ET PISTES D'AUDIT

L'expiration des certificats met en péril la sécurité des données. Il est donc essentiel de choisir un service qui génère des préavis à l'approche de la date de renouvellement. La solution doit vous permettre de gérer les risques en organisant vos activités administratives de façon proactive.

FLEXIBILITÉ ET ÉVOLUTIVITÉ

Les réseaux d'entreprise constituent des environnements dynamiques en constante évolution. Par conséquent, un service de recherche de certificats doit comporter des paramètres configurables — durée de l'analyse, adresses IP concernées, etc. Par ailleurs, il doit être suffisamment évolutif pour pouvoir s'adapter à la croissance future.

DÉLÉGATION DES OPÉRATIONS D'ADMINISTRATION

Dans une grande entreprise, il est impératif de déléguer les tâches d'administration et l'octroi des droits d'accès. Si votre compte gère plusieurs entités et unités organisationnelles, vous devez être en mesure d'affecter aux différents administrateurs les rôles et responsabilités appropriés.

Conclusion

Les certificats SSL et de signature de code sont essentiels à la sécurité et la conformité des entreprises. Néanmoins, la complexité croissante du cadre réglementaire s'est traduite par une prolifération des certificats, elle-même à l'origine d'un besoin impérieux de faciliter la recherche et la gestion des certificats à l'échelle de toute l'entreprise.

Pour les moyennes entreprises comme pour les grands groupes confrontés à diverses exigences de sécurité et de conformité, le compte Thawte Certificate Center Enterprise permet d'automatiser les tâches de recherche et de programmer des alertes de préavis d'expiration ou d'opérations de maintenance des certificats.

Pour en savoir plus sur les avantages du compte en termes de simplification de la sécurité et d'approche globale de la conformité, rendez-vous sur :
http://www.thawte.fr/ssl/volume-discount-ssl-certificates/index.html

Pour en savoir plus, contactez nos conseillers commerciaux :

- **Par téléphone**
  - **États-Unis : +1 888 484 2983**
  - **Royaume-Uni : +44 203 450 5486**
  - **Afrique du Sud : +27 21 819 2802**
  - **Allemagne : +49 69 3807 89081**
  - **France : +33 1 57 32 42 68**
- **Par e-mail : Enterprisesales@thawte.com**
- **Sur notre site Web : http://www.thawte.fr/ssl/volume-discount-ssl-certificates/index.html**

Protégez votre activité et inspirez confiance à vos clients grâce à la sécurité renforcée des certificats numériques signés Thawte, leader mondial de la sécurité en ligne. Stabilité, fiabilité, infrastructure éprouvée, support client irréprochable… en 17 ans, Thawte a su s'imposer comme le partenaire international de choix pour les entreprises du monde entier.

UID 191/2/13