digicert®

BONNES PRATIQUES DE GESTION DES CERTIFICATS TLS : LA CHECKLIST

L'an dernier, 60 % des entreprises ont connu des problèmes de certificats qui ont sérieusement impacté leur activité[1]. Outre leur coût direct pour les grandes entreprises (5 600 $ par minute en moyenne)[2], ce genre de panne porte aussi gravement atteinte à leur réputation et leur croissance.

Aujourd'hui plus que jamais, il est indispensable de définir et appliquer des protocoles draconiens pour la gestion des certificats numériques de votre entreprise.

C'est dans cette optique que nous avons dressé cette checklist de bonnes pratiques, structurée autour des quatre étapes fondamentales à la connaissance, la couverture et la maîtrise parfaites du cycle de vie de vos certificats.

digicert®

IDENTIFICATION

Définissez une base de référence de tous les certificats émis

Sans un inventaire rigoureux de vos certificats, vous vous exposez à des risques de sécurité. D'où l'importance de recenser tous les certificats émis par votre Autorité de certification (AC). Entre vos AC internes et les certificats installés sur les différents équipements de votre réseau, dresser un tel inventaire est loin d'être une formalité. Pour qu'aucun certificat TLS ne passe à travers les mailles du filet, la meilleure solution consiste donc à effectuer un scan de votre réseau.

Localisez les emplacements de tous vos certificats

Ne vous contentez pas de lister uniquement les certificats émis : si un certificat est installé sur un équipement non autorisé, il pourra divulguer des données chiffrées à votre insu. C'est pourquoi il est essentiel de localiser et vérifier les serveurs hébergeant tous vos certificats, et de consigner toutes ces informations dans votre inventaire.

Nommez des responsables pour chaque certificat et domaine

L'expiration inopinée est l'une des principales causes de pannes liées aux certificats. Il s'avère donc essentiel de répertorier tous les acheteurs de certificats et de mettre en place les processus de renouvellement et de transfert de responsabilité en cas de départ de l'acheteur.

Identifiez les versions des systèmes d'exploitation et applications installés sur les serveurs web

Les hackers exploitent sans mal la moindre faille des systèmes d'exploitation. C'est le cas de Heartbleed, une vulnérabilité dans la bibliothèque cryptographique OpenSSL qui permet à quiconque connecté à Internet d'accéder à votre système. Vous avez donc tout intérêt à inclure les informations relatives à vos systèmes d'exploitation et applications dans vos inventaires.

Recensez les suites cryptographiques et les versions de certificats TLS sur les serveurs web

Une suite cryptographique est un ensemble d'algorithmes qui sous-tendent le chiffrement TLS chargé de sécuriser les connexions réseau. Les cybercriminels ont tendance à cibler les versions anciennes du protocole TLS ou des suites cryptographiques obsolètes. Il est donc important d'inclure les versions dans vos inventaires.

[1] https://www.venafi.com/blog/majority-businesses-still-experience-outages-are-you-protecting-your-certificates
[2] https://www.venafi.com/blog/what-if-you-could-guarantee-eliminating-outages-your-organization

REMÉDIATION

- [ ] **Supprimez les hachages, les clés et les suites cryptographiques trop faibles**
Il se peut que vos sites web internes soient encore protégés par des algorithmes de hachage obsolètes, de type MD5 et SHA-1. Si c'est le cas, vous devez les mettre à jour. Seules les versions TLS 1.2 et 1.3 sont recommandées. Utilisez de préférence des méthodes de chiffrement récentes comme AES.

- [ ] **Contrôlez l'émission et la distribution de certificats Wildcard**
Parce qu'ils sont faciles à gérer et peuvent protéger plusieurs sous-domaines, les certificats Wildcard sont particulièrement attractifs. Mais attention : si leurs clés privées sont compromises, des hackers peuvent alors exploiter n'importe quel système du domaine couvert. La révocation et la réémission des certificats peut alors coûter cher et prendre du temps. En revanche, si toutes les conditions sont strictement respectées, alors les certificats Wildcard offrent un bon moyen de conjuguer sécurité et flexibilité.

- [ ] **Déployez des certificats adaptés à chaque cas d'usage**
Tous les certificats ne se valent pas. Pour vos systèmes internes, des certificats TLS privés font l'affaire. Mais pour les sites publics, des certificats OV (Organization Validation) ou EV (Extended Validation) sont indispensables. Quant aux certificats de validation de domaine (DV) de base, ils sont peu fiables et donc peu recommandés pour le transfert d'informations sensibles.

- [ ] **Contrôlez tous les certificats d'usine**
Les certificats d'usine, c'est-à-dire livrés avec les machines des constructeurs informatiques, ne sont pas considérés comme fiables par les navigateurs. Il s'agit en général de certificats auto-signés, expirés ou qui utilisent des clés faibles et qui ne sont pas voués à être déployés sur des réseaux en production. Et pourtant, les entreprises en détiennent souvent des milliers. Heureusement, les dernières générations de plateformes de gestion des certificats vous aideront à automatiser le remplacement des certificats d'usine.

- [ ] **Veillez à l'installation des correctifs les plus récents sur tous les serveurs web**
Pour protéger vos systèmes d'exploitation et serveurs web contre les attaques les plus malveillantes, vous devez impérativement y installer les correctifs de sécurité les plus récents.

PROTECTION

- [ ] **Standardisez et automatisez les processus d'émission et de renouvellement**
  En automatisant et en standardisant vos protocoles de gestion des certificats TLS (émission, renouvellement, etc.), vous prévenez les erreurs humaines et gagnez du temps. En ce sens, une bonne plateforme de gestion des certificats vous facilitera la tâche.

- [ ] **Installez et renouvelez tous les certificats dans les délais**
  Il est important de prévoir le renouvellement de vos certificats en fonction des contraintes de vos métiers. En règle générale, nous recommandons de renouveler vos certificats au moins 15 jours avant leur date d'expiration. Mais dans certaines entreprises, la procédure de renouvellement doit être engagée trois mois avant.

- [ ] **Veillez à ce que les clés privées ne soient pas réutilisées lors du renouvellement des certificats**
  Que vous utilisiez des certificats DV, OV ou EV, la réutilisation de clés privées augmente le risque de compromission de ces dernières. Créez toujours une nouvelle paire de clés lors du renouvellement d'un certificat.

- [ ] **Installez les certificats et les clés privées de manière sécurisée**
  Créez vos clés privées sur un ordinateur sécurisé et mettez en place une procédure de diffusion via des e-mails chiffrés avec suppression automatique.

- [ ] **Supprimez/révoquez les certificats lors du processus de décommissionnement**
  Mettez en œuvre un dispositif de gestion des suppressions et révocations de vos certificats en cas de changement de propriétaire, de décommissionnement ou de fin de vie de vos systèmes.

SUIVI

- [ ] **Effectuez des scans réguliers des réseaux pour détecter tout changement**
  La gestion manuelle des certificats s'avère de plus en plus difficile : les réseaux évoluent constamment et les portfolios de certificats ne cessent de s'élargir. D'où l'utilité d'outils de scanning réseau pour mettre en évidence tous les problèmes dès leur apparition. Non seulement vous gagnez du temps, mais votre entreprise reste protégée en toutes circonstances.

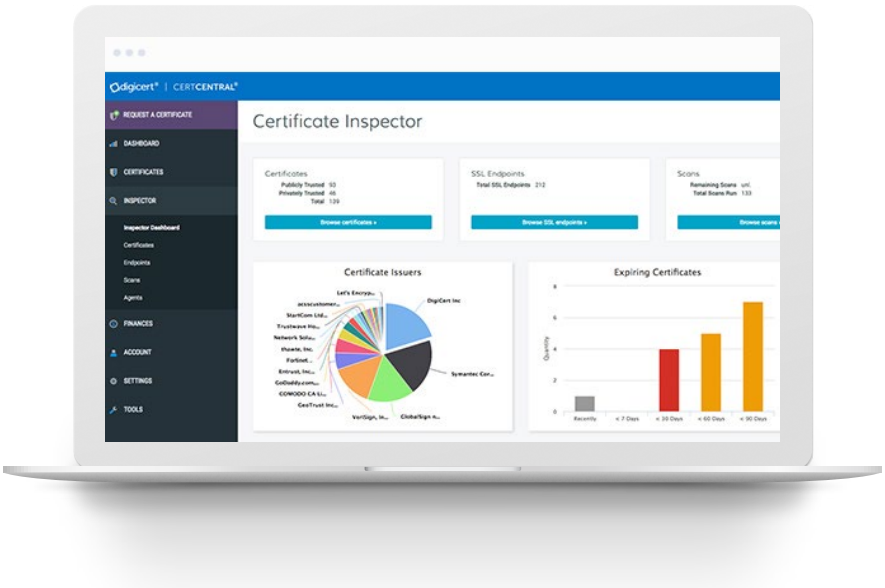
- [ ] **Recherchez les certificats non autorisés dans les logs CT (Certificate Transparency)**
  Tout certificat public non répertorié dans les logs CT sera signalé comme non fiable à vos clients. Le moniteur CT est au TLS ce que le rapport de solvabilité est à la finance. Il permet ainsi de détecter les certificats non autorisés et de les supprimer avant qu'ils ne portent préjudice à vos données ou votre réputation.

- [ ] **Vérifiez le registre CAA pour prévenir les demandes de certificats non autorisés**
  Le registre CAA (Certificate Authority Authorization) est un registre DNS répertoriant les Autorités de certification autorisées à émettre des certificats pour votre domaine. En mettant un tel dispositif en place, vous prévenez les émissions « sauvages » de certificats par des AC peu sûres et non approuvées.

CONCLUSION

Maintenant que vous détenez toutes les clés de la sécurité de votre activité en ligne, n'acceptez rien de moins que la solution la plus fiable du marché :

DigiCert CertCentral



Gérez vos certificats en toute simplicité

Avec DigiCert CertCentral®, vous disposez de tous les outils et fonctionnalités nécessaires pour identifier, rétablir, protéger, suivre, et même personnaliser et automatiser tout votre écosystème de certificats, rapidement et en toute simplicité. Vous pouvez :

- Scanner régulièrement vos réseaux pour détecter tout changement ou nouveau système
- Rechercher les certificats non autorisés dans les logs CT
- Vérifier le registre CAA pour prévenir toute émission non autorisée de certificat

Le tout depuis une console centralisée.

Pour en savoir plus, visitez la page digicert.com/fr/certificate-management