ÉTAT DES LIEUX DE L'AUTOMATISATION PKI

Rapport 2021

ÉTAT DES LIEUX DE L'AUTOMATISATION PKI : LE RAPPORT

La PKI est au cœur de presque toutes les technologies. Utilisateurs, serveurs, appareils, IoT, applications et services DevOps, signature de documents numériques… son rôle est essentiel en matière d'identification et d'authentification.

Le problème, c'est qu'une telle infrastructure devient aujourd'hui impossible à gérer manuellement. D'après une récente étude du Ponemon Institute, le nombre de certificats PKI gérés par les entreprises augmenterait en effet de 43 % chaque année[1]. Ajoutez à cela une durée de validité raccourcie, et toutes les conditions sont réunies pour en compliquer la gestion.

Pour faire un point complet sur la situation à l'échelle internationale, DigiCert a demandé au cabinet d'études ReRez Research d'interroger des responsables informatiques en charge de la PKI dans 400 entreprises. L'étude dresse un constat globalement tourmenté, tout en faisant ressortir les schémas suivis par les entreprises les plus en pointe dans la gestion PKI.

Le nombre de certificats PKI gérés par les entreprises a augmenté de **43 %**

QU'EST-CE QUE L'AUTOMATISATION PKI ?

Voici les principaux domaines d'application de l'automatisation PKI tels que nous les avons présentés aux sondés :

- Découverte de certificats numériques existants
- Émission de nouveaux certificats numériques
- Renouvellement des certificats numériques sur le point d'expirer
- Révocation des certificats numériques lorsque cela est nécessaire
- Automatisation de la signature de code
- Procédure d'enrôlement des certificats clients
- Vérification d'identité (pour la signature de document, par exemple)
- Automatisation d'activités de provisionnement (ex. : LDAP et Exchange)
- Toute autre activité pratique liée à la gestion PKI

1 Étude 2020 sur les tendances mondiales en matière de PKI et d'IoT conduite par le Ponemon Institute

UNE CROISSANCE RAPIDE QUI PROVOQUE LA CONFUSION

L'entreprise type de notre étude gère globalement plus de 50 000 certificats. Il s'agit principalement de certificats utilisateur et serveur, suivis par les certificats pour serveurs web, appareils mobiles et e-mails. Les certificats publics, émis par des Autorités de certification (AC) publiques, sont un tiers plus nombreux que les certificats privés, émis par une AC interne.

Une entreprise type gère actuellement plus de **50 000** certificats.

Cette très forte hausse comparée aux années précédentes explique en grande partie les difficultés de gestion qu'affrontent les entreprises. Concrètement, deux tiers d'entre elles ont subi des pannes dues à l'expiration soudaine de certificats, tandis qu'une sur quatre a essuyé cinq ou six pannes de ce type au cours des six derniers mois.

Pourquoi ? Notamment en raison de l'augmentation de la charge de travail : presque deux tiers des entreprises interrogées se disent « préoccupées », voire « très préoccupées » par le temps passé à gérer les certificats. À cela s'ajoute un manque certain de visibilité. Dans 37 % des entreprises interrogées, au moins trois départements se partagent la gestion des certificats. D'où une confusion inévitable. Toujours selon l'étude, une entreprise type compte jusqu'à 1 200 certificats non gérés ; près de la moitié (47 %) des entreprises interrogées reconnaissent découvrir fréquemment des certificats non autorisés, c'est-à-dire implémentés hors de tout cadre de gestion et à l'insu du département IT. L'automatisation PKI semble être la réponse évidente à ces problèmes. Nous avons donc voulu savoir où en étaient les entreprises dans ce domaine.

61 % S'INQUIÈTENT DU TEMPS IMPARTI À LA GESTION DES CERTIFICATS

47 % DÉCOUVRENT FRÉQUEMMENT DES CERTIFICATS NON AUTORISÉS

37 % RÉPARTISSENT LA GESTION DES CERTIFICATS ENTRE 3 DÉPARTEMENTS OU PLUS

1 IN 4

A SUBI CINQ OU SIX PANNES LIÉES À LA PKI AU COURS DES SIX DERNIERS MOIS

91 % DES ENTREPRISES VEULENT AUTOMATISER LEUR INFRASTRUCTURE PKI

D'après notre enquête, la plupart des entreprises (91 %) envisagent d'automatiser leur infrastructure PKI. Pour les autres (9 %), le sujet n'est pas à l'ordre du jour. La grande majorité des entreprises (70 %) comptent implémenter une solution dans les 12 mois, tandis que pour un quart, le processus est soit en cours, soit terminé. Pourtant, les obstacles cités sont nombreux, notamment : les coûts, la complexité, les questions de conformité et la résistance au changement de la part des collaborateurs comme de la direction.

TENDANCES

Principaux ressorts de l'automatisation PKI dans les entreprises :

1. Certificats non autorisés
2. Préparation à l'informatique post-quantique
3. Raccourcissement rapide de la durée de validité des certificats, entraînant une hausse brutale des charges de travail
4. Envolée du nombre de certificats sous gestion
5. Progression du télétravail

DIFFICULTÉS

Questions de sécurité incitant les entreprises à automatiser :

1. Lenteur du provisionnement de nouveaux certificats
2. Mauvaise configuration des certificats
3. Surcharge des collaborateurs
4. Prolifération de certificats non autorisés
5. Expiration inopinée de certificats
6. Lenteur, voire absence de révocation des certificats lorsque cela est nécessaire

SANCTIONS

Conséquences de l'absence d'automatisation PKI :

1. Problèmes de conformité
2. Problèmes de sécurité
3. Coûts
4. Interruptions de service
5. Insatisfaction des clients ou des collaborateurs

OBJECTIFS

Les entreprises qui adoptent l'automatisation PKI pour :

1. Plus de sécurité
2. Plus de conformité
3. Plus d'agilité
4. Plus de productivité
5. Moins d'interruptions de service et de coûts

COMPARAISON DU HAUT ET DU BAS DE TABLEAU

Les participants à l'étude ont été invités à évaluer leurs propres capacités sur diverses métriques PKI :

- Prévention des interruptions de service dues à l'expiration inopinée de certificats
- Révocation rapide de certificats en cas de nécessité
- Gestion efficace des certificats numériques
- Réduction des risques de sécurité dus à une mauvaise gestion des certificats
- Réduction des problèmes de conformité dus à une mauvaise gestion des certificats
- Minimisation du nombre de certificats non autorisés
- Respect des accords SLA relatifs à la PKI
- Rapidité d'émission et de révocation PKI

Nous avons attribué une note (positive ou négative) en fonction de chaque réponse, puis nous avons totalisé les scores.

Ensuite, nous avons scindé les participants en trois groupes distincts selon leurs résultats :

1 **LEADERS**

Organisations les mieux notées sur l'ensemble des métriques listées ci-dessus.

2 **INTERMÉDIAIRES**

Organisations obtenant un score moyen sur l'ensemble des métriques listées ci-dessus.

3 **RETARDATAIRES**

Organisations les moins bien notées sur l'ensemble des métriques listées ci-dessus.

Enfin, nous avons comparé les leaders et les suiveurs pour mesurer le fossé qui les sépare et comprendre comment les leaders tirent leur épingle du jeu.

LEADERS VS SUIVEURS

Les personnes interrogées ont évoqué sans détour leurs problèmes de gestion PKI. Certificats non autorisés, pannes dues à l'expiration inopinée d'un certificat… les entreprises font face à de nombreux incidents, mais à des degrés de gravité différents. Nous avons classé les réponses dans trois groupes avant de comparer les deux extrémités du classement. Les différences sont frappantes.

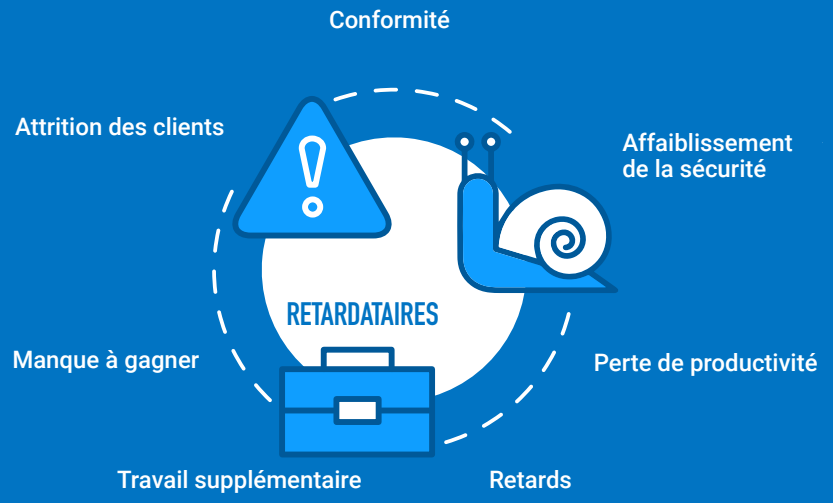
Les leaders se démarquent dès le départ. En particulier, un tiers d'entre eux (33 %) pensent que l'automatisation PKI est de première importance. Le groupe de tête obtient de meilleurs résultats (2 ou 3 fois supérieurs) dans les domaines suivants :

- Réduction des risques de sécurité PKI
- Prévention des interruptions de service de la PKI
- Limitation des certificats non autorisés
- Respect des accords SLA relatifs à la PKI
- Gestion des certificats numériques
- Émission et révocation des certificats
- Conformité

À l'opposé, les retardataires sont fortement pénalisés par manque de compétences en gestion des certificats PKI :

- Problèmes de conformité
- Problèmes de sécurité
- Perte de productivité
- Retards
- Surcharge de travail
- Attrition des clients
- Manque à gagner

Qu'est-ce qui distingue les leaders ? Quels enseignements pouvons-nous en tirer ?



PORTRAIT TYPE DES LEADERS DE L'AUTOMATISATION PKI

Les leaders sont deux fois plus nombreux que les autres à se dire préoccupés par le temps que mobilise la gestion des certificats PKI, au détriment d'autres tâches. Ils sont également plus sensibles au problème des certificats non autorisés. Enfin, ils sont convaincus de l'importance de l'automatisation PKI pour l'avenir de leur entreprise. Voilà qui explique sans doute pourquoi ils sont six fois plus nombreux à avoir déjà franchi le pas. Quels enseignements pouvons-nous tirer de ces constats et quels sont les ajustements possibles ?

LE RÈGNE DU CHACUN POUR SOI

Une analyse approfondie des données nous livre des informations surprenantes : de nombreuses entreprises qui, en théorie, devraient gérer plus facilement les certificats PKI sont celles qui ont souvent le plus de mal en pratique.

Prenons un exemple. Les entreprises qui gèrent le moins de certificats sont bien plus nombreuses à subir des pannes liées à l'expiration accidentelle de ces derniers. Par ailleurs, elles obtiennent uniformément de moins bons résultats sur un large éventail de métriques de gestion PKI.

En définitive, malgré le faible volume de certificats à gérer, ces entreprises se disent largement plus préoccupées par la gestion de la PKI que celles qui gèrent des volumes bien supérieurs. Concrètement, elles sont presque 50 % plus nombreuses à se dire inquiètes du temps qu'elles passent à gérer leurs certificats PKI. Autre particularité : elles détiennent également près de deux fois plus de certificats enrôlés dans un programme d'automatisation PKI.

À première vue, cela semble paradoxal. Mais en y regardant de plus près, on remarque que leurs capacités de gestion PKI sont bien moins matures que celles des entreprises qui gèrent plus de 100 000 certificats. Dans les structures à petits volumes, c'est le règne du chacun pour soi : en l'absence de règles, chacun joue sa partition en solo.

> LES ENTREPRISES À PETITS VOLUMES N'APPLIQUENT PAS DE RÈGLES COMMUNES ET CHACUN Y GÈRE LES CERTIFICATS À SA FAÇON.

PORTRAIT TYPE DES LEADERS DE L'AUTOMATISATION PKI

D'après l'étude, les leaders de la gestion PKI possèdent une bien meilleure maîtrise de leur portfolio de certificats, mais se notent paradoxalement moins bien que les entreprises moins préoccupées par cette question. Ils indiquent pourtant subir moins de pannes liées aux certificats ou détecter moins de certificats non autorisés, prouvant par là même qu'ils obtiennent en réalité de bien meilleurs résultats qu'ils ne le pensent.

PARADOXE DE L'AUTOÉVALUATION

Un autre fait intéressant concerne les entreprises « très préoccupées » par la gestion des certificats PKI. Celles qui subissent objectivement le moins de problèmes ont tendance à se noter plus sévèrement.

Prenons le cas des entreprises qui considèrent la gestion de la PKI comme difficile. Elles sont trois à cinq fois plus nombreuses à affirmer être préoccupées, voire extrêmement préoccupées, dans de nombreux domaines tels que la rapidité d'émission de nouveaux certificats, les erreurs accidentelles de configuration de certificats et la découverte de certificats non autorisés.

Pourtant, c'est aussi dans ces entreprises que l'on recense le moins de certificats non autorisés (seulement deux-tiers de ce que constatent les entreprises qui affirment n'être pas préoccupées). En outre, elles ont subi bien moins de pannes liées à l'expiration accidentelle de certificats (une seule au cours des six derniers mois contre trois à cinq pour les entreprises qui ne se disent pas préoccupées).

Ce phénomène est fréquent dans les enquêtes liées à la sécurité. Il s'explique comme suit : les entreprises les plus attentives sont aussi les plus conscientes de leurs points faibles et de leurs erreurs. Elles ont donc tendance à se noter plus sévèrement que les autres. Mais leur vigilance paye, et elles s'en sortent bien mieux que les autres.

> LES ENTREPRISES PRÉOCCUPÉES PAR LA GESTION DES CERTIFICATS PKI SUBISSENT OBJECTIVEMENT LE MOINS DE PROBLÈMES, MAIS ONT TENDANCE À SE NOTER PLUS SÉVÈREMENT.

NOS RECOMMANDATIONS

Dans un contexte de réduction des durées de validité, d'évolution des standards cryptographiques et d'adoption généralisée des certificats numériques dans l'ensemble de leurs processus métiers, les entreprises ont beaucoup à gagner d'une automatisation de leur portfolio de certificats PKI. Mais avant de sauter le pas, quels sont les critères à prendre en compte ? Réponse dans ce schéma des principaux domaines de gestion des certificats qui pourront profiter de l'automatisation.

GESTION DES CERTIFICATS

IDENTIFICATION
Dressez un inventaire de votre portfolio de certificats.

REMÉDIATION
Corrigez les clés et les certificats non conformes à votre politique d'entreprise.

PROTECTION
Appliquez les bonnes pratiques d'émission et de révocation pour renforcer votre protection. Standardisez et automatisez les processus d'enrôlement, d'émission et de renouvellement.

SUIVI
Surveillez votre environnement pour détecter des changements.

AUTOMATISATION DU PROCESSUS DE GESTION DES CERTIFICATS

IDENTIFICATION
Repérez les certificats non gérés ou gérés manuellement.

ADOPTION
Adoptez un logiciel d'automatisation qui centralise et gère ce processus.

SUIVI
Centralisez la visibilité et le contrôle pour un monitoring précis.

PROCESSUS TYPES DE GESTION DES CERTIFICATS

- Serveurs web
- Identité et gestion des appareils
- Signature de code
- Signatures numériques
- Identité et accès

MÉTHODOLOGIE

Le cabinet ReRez Research a effectué une enquête auprès de 400 informaticiens travaillant dans des entreprises de plus de mille salariés aux États-Unis, en EMEA, en Asie-Pacifique et en Amérique latine. L'échantillon était composé de directeurs informatiques, responsables de la sécurité informatique et informaticiens généralistes. Tous avaient comme point commun de gérer les certificats numériques des utilisateurs, des serveurs et des appareils mobiles pour des ETI et des grands groupes.

Vous souhaitez évaluer les besoins de votre entreprise et connaître les solutions adaptées à votre situation ? Nos experts de l'automatisation PKI se tiennent à votre disposition. Découvrez également la plateforme d'automatisation qui vous aidera à prendre un bon départ.