Livre blanc

Enquête IDC : les investissements PKI contribuent à renforcer la sécurité des entreprises et moderniser leurs processus métiers

En partenariat avec : DigiCert Inc.

Frank Dickson Robyn Westervelt
janvier 2021

AVANT-PROPOS

Dans le sillage des multiples initiatives de transformation digitale (DX) des entreprises, les professionnels et opérationnels de sécurité informatique sont soumis à une pression croissante pour gérer la sécurité et la résilience de leurs systèmes critiques. Pour desserrer l'étau et affecter plus efficacement les ressources dans des environnements hybrides et multicloud toujours plus étendus, les directeurs des systèmes d'information (DSI), responsables sécurité des systèmes d'information (RSSI) et autres architectes de sécurité se penchent désormais sur la question des implémentations d'infrastructure à clés publiques (PKI), souvent mal intégrées et mal gérées.

De nombreuses organisations ont choisi de miser sur une infrastructure PKI pour la résilience qu'elle leur apporte en termes de cybersécurité. Elle leur permet en effet d'automatiser l'application des règles et politiques de sécurité des données au moyen de certificats numériques et du chiffrement à clé publique. L'infrastructure PKI établit des connexions validées et fiables entre des systèmes et fournit aux utilisateurs un accès transparent aux ressources sensibles. Progressivement, elle s'est étendue à la protection des documents, du courrier électronique et de l'intégrité du code via des certificats cryptographiques de signature. Elle protège aussi les ressources et les utilisateurs au moyen de certificats de terminaux servant à authentifier les identités numériques.

Face aux énormes enjeux, les équipes de sécurité comptent sur les technologies PKI et les testent abondamment. Elles y recourent notamment pour atténuer les risques liés à la multiplication des services cloud utilisés par les entreprises. La complexité de ces environnements se traduit en effet par une fragmentation de l'infrastructure de sécurité, créant ainsi des failles dans lesquelles les attaquants ne tardent pas à s'engouffrer. Pour les RSSI, cet enjeu est prioritaire. C'est ce que révèle le rapport IDC sur les services data pour le cloud hybride, fruit d'une enquête de plus de 400 spécialistes de la gestion des données et de la sécurité informatique en Europe et en Amérique du Nord. D'après les résultats, environ 78,9 % des entreprises déclarent recourir à la gestion des clés d'entreprise dans différents domaines :

- **Sécurisation des accès distants :** authentification forte des salariés et partenaires pour sécuriser les accès à un réseau sans fil ou un VPN
- **Sécurisation des environnements BYOD :** protection des initiatives BYOD non gérées et accès sécurisé aux ressources de l'entreprise sans impact sur l'expérience mobile des utilisateurs
- **Sécurisation de l'authentification :** authentification forte des utilisateurs pour sécuriser l'accès aux applications contenant des informations sensibles
- **Sécurisation des e-mails :** envoi d'e-mails chiffrés et signés numériquement depuis tous les appareils de l'entreprise
- **Intégrité de la signature de document :** validation de l'intégrité et de l'authenticité des signatures numériques sur les documents importants

- **Sécurisation des objets connectés (IoT) :** identification des terminaux et établissement de la racine de confiance pour préserver l'intégrité des logiciels et du firmware sur les objets connectés sensibles
- **Signature de code et de binaires numériques (dont les containers) :** validation de la provenance et de la véracité des éléments logiciels et de code

À l'heure où les organisations continuent de miser sur les technologies PKI pour faire face sur de nombreux fronts, les attaques gagnent inexorablement en sophistication et en fréquence. Les équipes de sécurité doivent donc mettre en place des approches plus exhaustives et coordonnées pour accompagner l'évolution des stratégies d'entreprise.

Au cœur des stratégies de transformation digitale, la transformation informatique doit s'articuler autour des deux grands axes que sont la sécurité et la disponibilité des données. L'infrastructure PKI joue un rôle clé pour maintenir l'intégrité, la disponibilité et la résilience de l'infrastructure informatique d'une entreprise. Le problème, c'est que la gestion de la protection des données se complique sans cesse dans des environnements de plus en plus hybrides et face à des menaces de plus en plus diverses et sophistiquées. Les récents cas de cyberattaques largement relayés dans les médias illustrent bien les problèmes que posent les environnements d'entreprise actuels, extrêmement distribués et complexes. Les attaquants profitent par exemple de coûteuses erreurs de configuration qui laissent des serveurs de bases de données exposés à l'Internet public. Ils continuent d'exploiter les mots de passe faibles et les identifiants par défaut ou volés, tout en guettant sans cesse la moindre faille dans la gestion des données sur des environnements distribués. Plus de 30 % des personnes interrogées font état de difficultés d'intégration de leurs environnements hybrides et multicloud à leur infrastructure informatique existante. Pour 37 %, la complexité des solutions de sécurité est la troisième plus grande menace pour leur entreprise dans les deux prochaines années, derrière la sophistication des attaques et les risques liés à l'adoption du cloud. Le problème est souvent aggravé par une mauvaise gestion des environnements opérationnels PKI, qui nuisent à la productivité des utilisateurs, érodent la confiance des clients et des partenaires, voire aboutissent à des incidents de sécurité et des compromissions de données dont les conséquences peuvent être très coûteuses.

Les infrastructures PKI sous-tendant les applications critiques sont « extrêmement efficaces »

Dans les échanges menés au cours de cette enquête, les technologies PKI dégagent une impression très majoritairement positive, car elles peuvent s'intégrer parfaitement à une variété d'applications métiers. Les déploiements PKI sont salués pour différentes raisons : leur capacité à gérer à grande échelle des accès distants à des applications de paiement complexes et à des terminaux de point de vente (POS) ; leur intégration à une variété de systèmes back-end, dont les référentiels d'analytique sous-tendant les systèmes de chiffrement ; et la signature numérique de documents pour préserver l'intégrité des contrats au moyen d'un système personnalisé de gestion de contenus.

Les RSSI et les architectes sécurité sont très majoritairement en faveur des technologies PKI, qu'ils jugent « extrêmement efficaces » dès lors qu'elles sont correctement mises en œuvre et gérées de façon proactive. La plupart des personnes interrogées gèrent de multiples implémentations PKI intégrées à Active Directory et à des applications métier spécifiques. Elles ont assuré ou supervisé la gestion de plateformes PKI pendant suffisamment longtemps pour l'avoir vu croître et évoluer au sein de leur entreprise. Elles sont aussi passées par de nombreuses mises à jour de leurs implémentations PKI existantes pour maintenir un niveau de sécurité élevé. IDC offre aux directions informatiques quelques pistes pour renforcer l'efficacité de leurs solutions PKI :

- Évaluer la capacité de l'entreprise à attirer, former et fidéliser des architectes sécurité pour gérer les implémentations PKI existantes, et déterminer si l'équipe informatique possède l'expertise nécessaire pour évoluer vers de nouveaux objectifs nécessitant le déploiement de certificats numériques à grande échelle.
- Évaluer l'intérêt de services PKI managés pour rationaliser la gestion et réduire la complexité. Une fois l'environnement PKI conçu et implémenté, tout changement de spécification ou de processus peut être fastidieux. L'investissement initial est donc crucial.

MÉTHODOLOGIE

Cette enquête IDC a interrogé des RSSI et architectes de sécurité de plusieurs grandes entreprises à propos de leur infrastructure PKI existante et de sa capacité à accompagner l'adoption du cloud et les stratégies de transformation digitale de leur organisation. Les perspectives tirées de ces entretiens ont été recoupées avec les données d'une nouvelle enquête sur les défis de la sécurisation des environnements hybrides et multicloud. L'étude a identifié une amélioration de l'efficacité et une baisse des coûts de gestion pour une variété d'implémentations PKI managées et sur site, parmi lesquelles on retrouve la signature de code pour valider l'authenticité des mises à jour logicielles sur les objets connectés, la signature de documents pour éliminer le papier et les processus manuels, la sécurisation des e-mails, la sécurisation des accès distants et l'authentification des utilisateurs et des terminaux pour l'accès aux ressources sensibles des entreprises.

ÉTAT DES LIEUX

PKI : les fonctionnalités essentielles pour contrer les attaques et protéger les ressources critiques

Pour réduire leurs coûts et éliminer la redondance et la fragmentation de leurs infrastructures, de nombreuses organisations se tournent vers des spécialistes des infrastructures PKI. Objectif : rationaliser, centraliser et automatiser la gestion des certificats numériques. Ces fournisseurs peuvent alors les accompagner de plusieurs manières, notamment en automatisant la gestion d'une ou plusieurs implémentations PKI couvrant plusieurs départements, ou au travers d'un service PKI managé qui garantit fiabilité et maintenance proactive.

D'après l'enquête, la réduction des coûts et les gains d'efficacité sont fréquemment cités parmi les raisons justifiant un investissement PKI. Pourtant, les implémentations PKI sont principalement motivées par les faiblesses et les vulnérabilités issues de la complexité de mise en œuvre et de gestion des produits de sécurité. D'après l'enquête IDC sur les services data pour le cloud hybride, presque 40 % des personnes interrogées dans différents domaines (sécurité informatique, gestion des données et métiers) citent deux défis de taille : la sophistication croissante des attaques et la complexité accrue de la gestion et la maintenance des produits de sécurité. Une autre étude IDC révèle par ailleurs que les équipes de sécurité sont confrontées à des défis croissants en matière de protection et de confidentialité. Non seulement elles doivent respecter et gérer des lois et réglementations toujours plus nombreuses, mais elles doivent en plus faire face à la montée en puissance de cyberattaques ciblées et polymorphes visant les ressources critiques de leur entreprise.

Outre l'atteinte à la réputation, les coûts directs et les sanctions réglementaires évoquées plus haut, les cyberattaques peuvent causer des interruptions de service, la divulgation de secrets commerciaux ou la perte définitive de données. Toujours selon une étude IDC, le coût moyen d'une interruption de service s'élève à 250 000 $ par heure. Si l'on compare le coût de logiciels de prévention des attaques et de restauration des systèmes avec la facture d'une seule heure d'interruption, le calcul est vite fait. Dans de nombreux cas, la réglementation impose aux entreprises de déclarer publiquement la compromission de données dont elles ont été victimes, avec pour conséquence une érosion durable de leur réputation et une perte définitive d'une partie de leur clientèle. L'étude IDC montre que presque la moitié des compromissions de données portent atteinte à la réputation des entreprises touchées, ce qui accroît encore les coûts de remédiation et de restauration.

Pour les entreprises comme pour les consommateurs, la médiatisation croissante des compromissions de données sonne comme autant de rappels de l'importance des identifiants pour la sécurité. D'innombrables études ont montré que les vulnérabilités et les problèmes de configuration, qui découlent souvent de l'excès de complexité, contribuent aux incidents de sécurité. En réduisant la fragmentation et le cloisonnement des implémentations PKI, il est possible de limiter les erreurs humaines et les failles des systèmes dont profitent les attaquants pour faire main basse sur des données. Correctement déployée et gérée, une solution PKI compte parmi les armes les plus puissantes dans l'arsenal des entreprises pour éviter des compromissions de données coûteuses et dommageables en termes d'image. Un nombre croissant d'entreprises remodèlent leurs stratégies de chiffrement et de gestion des clés pour obtenir une meilleure lecture de la situation et, partant, renforcer leur dispositif de sécurité.

Les professionnels de la sécurité interrogés dans cette enquête considèrent les technologies PKI comme une composante essentielle et éprouvée pour le chiffrement des données et la validation de leur intégrité et de celle des transactions. Ils ajoutent qu'elles sont indispensables pour vérifier l'identité des utilisateurs et des terminaux dans leur entreprise. L'infrastructure PKI dresse des remparts qui compliquent sérieusement la tâche des attaquants tentant d'accéder aux ressources critiques. Elle répond également aux impératifs d'évolutivité indispensables à des processus métiers extrêmement complexes et exigeants en termes de performances, tout en améliorant la productivité des utilisateurs et la fidélisation des clients grâce à sa transparence.

Un des sujets abordés lors des entretiens concerne le conflit permanent entre l'application de mesures de sécurité d'une part et les réticences des utilisateurs face à ces mesures d'autre part. Pour atténuer ce problème, les professionnels de la sécurité s'adressent de plus en plus à des prestataires PKI pour créer une solution PKI fiable et en harmonie avec l'infrastructure informatique et de sécurité existante, une fois identifiés les risques d'une mise en application dans l'entreprise. Pour les organisations qui choisissent de concevoir et mettre en place une solution PKI, la sécurité devient alors un levier de fonctionnalité et de productivité. Lorsqu'elle est déployée dans les règles de l'art, une solution PKI de nouvelle génération peut simplifier l'exécution de tâches nécessitant une authentification. Les procédures de sécurité autrefois laborieuses, et sources de tensions chez les utilisateurs, sont dans une large mesure automatisables. Les questions de sécurité sont souvent au cœur des enjeux lors des conclusions d'un audit, d'une compromission de données ou d'un incident de sécurité, voire, comme c'est souvent le cas, pour se conformer à une réglementation ou une politique interne. Aujourd'hui, les organisations font appel à des outils reposant sur l'infrastructure PKI (authentification multifacteur, chiffrement, sécurisation des utilisateurs mobiles, etc.).

Certains RSSI interrogés pour cette enquête ont été chargés par leur DSI de réduire les coûts et de soutenir les initiatives « cloud-first », avec un budget réservé pour établir un bilan de leur infrastructure PKI. Ils ont identifié et documenté les implémentations PKI commençant à montrer des signes de faiblesse sous la pression imposée par les rapides avancées technologiques et la croissance de l'activité. Dans certaines situations, la maintenance de l'infrastructure existante de ces organisations laissait à désirer, du fait de la pénurie de compétences en sécurité IT. Certaines organisations conservaient des implémentations PKI fragmentées, héritées de fusions et d'acquisitions ou résultant d'unités opérationnelles faisant jeu à part pour des questions de sécurité ou de processus. Les problèmes de complexité sont pratiquement toujours exacerbés par la nature évolutive et distribuée des ressources des environnements d'entreprise. L'*enquête d'IDC sur les services data pour le cloud hybride* indique que les organisations restent confrontées à ces problèmes. Les organisations considèrent les solutions PKI comme un défi considérable, aussi difficile que la mise en œuvre et la gestion du chiffrement ou le déploiement et la configuration des plateformes de prévention des pertes de données.

CAS D'USAGE D'UNE SOLUTION PKI

Les études de cas ci-dessous présentent comment les organisations capitalisent sur l'infrastructure PKI pour répondre à leurs besoins particuliers.

Certificats numériques : essentiels à la stratégie de mobilité d'une entreprise et aux besoins d'accès à distance de ses salariés

Une entreprise internationale de tests électroniques utilise une combinaison de certificats d'utilisateurs et de terminaux pour octroyer l'accès aux ressources sensibles depuis les ordinateurs portables et appareils mobiles personnels des salariés (BYOD) ou de l'entreprise. Le faible turnover de ses salariés et l'inventivité de ses ingénieurs en sont les résultats. C'est ce qu'estime le RSSI, qui se félicite d'utiliser les certificats numériques pour maintenir un dispositif de sécurité efficace tout en offrant aux collaborateurs des aménagements de télétravail flexibles.

« Nous avons estimé que les certificats représentaient la meilleure solution pour une variété de nos cas d'usage, mais aussi parce que tous nos partenaires possèdent des certificats pour le VPN, de même que les utilisateurs en BYOD sur leurs appareils mobiles », explique le RSSI.

La tâche la plus ardue avec les technologies PKI est la mise en place de chaînes de confiance et la couverture de tous les clients. Il n'existe aucune interopérabilité entre les différentes implémentations PKI de l'entreprise, tout simplement parce que ni les équipes de développement et d'étude, ni les services marketing et commerciaux n'en ont envie. Les opérations de l'entreprise sont fondées sur une chaîne de confiance distincte pour chaque implémentation PKI, alors qu'une approche centralisée serait probablement plus efficace et économique : il lui suffirait en effet de déployer une seule chaîne de confiance.

Dans un souci de maintien d'une sécurité stricte, l'implémentation PKI de l'entreprise pour l'accès mobile et VPN est presque entièrement adaptée aux profils de certificats côté Microsoft. Pour atténuer le risque de vol de certificats et d'attaques par force brute visant à accéder aux ressources critiques, l'entreprise a développé un lien personnalisé sur ses certificats. Lorsque les utilisateurs se connectent, ils sont seulement invités à saisir un mot de passe et non un certificat. Les certificats fonctionnent donc uniquement pour des utilisateurs individuels. Cette relation bijective rend impossible l'utilisation simultanée d'un certificat et d'un mot de passe. « Pour moi, c'est un élément de sécurité essentiel dans le déploiement de certificats », estime le RSSI.

Une solution PKI renforce l'authentification et la sécurité des e-mails pour un industriel

Pour ce fabricant international de produits de grande consommation, la cybersécurité n'a jamais été une priorité absolue. Il n'existait aucune méthode fiable et efficace d'authentification des utilisateurs pour l'accès aux ressources sensibles ou les connexions à distance. Ces faiblesses patentes sont restées longtemps sans réponse de la part de l'entreprise. Jusqu'au jour où une attaque par ransomware, sous forme d'un malware SamSam, a finalement attiré l'attention de la maison-mère du fabricant. La direction a alors décidé de prendre des mesures immédiates, dont un investissement dans une solution PKI pour la sécurité des e-mails et l'authentification des utilisateurs.

Les attaquants à l'origine du malware SamSam avaient facilement identifié et ciblé une vulnérabilité sur les serveurs FTP de l'entreprise, puis lancé une attaque par force brute visant à craquer les mots de passe faibles puis établir une première tête de pont. Cette intrusion a contraint l'entreprise à interrompre presque toute sa production, soit un coût de plusieurs millions de dollars par jour. Comme aucune sauvegarde digne de ce nom n'était en place, les salariés ont dû récupérer de la propriété intellectuelle (PI) sur des supports papier, tandis qu'une partie a été rétablie à partir de sauvegardes sur bande. Pour renforcer son infrastructure de sécurité, l'entreprise s'est engagée dans de lourds investissements, dont une solution PKI pour sécuriser les e-mails.

« J'ai été embauché pour élaborer un programme de sécurité complet. Des politiques étaient en place, mais rien de plus », se rappelle le RSSI, entré en fonction peu après l'attaque pour mettre en place un programme de sécurité aligné sur les standards en vigueur dans la maison-mère du fabricant. « Nos applications n'étaient pas à jour et notre infrastructure de sécurité était soit mal configurée, soit inexistante. Lorsque nous avons su exactement où étaient nos données sensibles, nous avons réalisé qu'il nous fallait mettre en place les outils adéquats. C'est pourquoi nous avons reconstruit notre infrastructure de sécurité autour d'une solution PKI moderne assurant l'authentification et la sécurisation des e-mails pour tous nos utilisateurs, indépendamment du lieu et de l'appareil utilisé. »

L'équipe de sécurité devait s'assurer que le transfert des e-mails et des fichiers de données était sécurisé. En coopération avec le siège, elle a déployé une solution PKI en parallèle à la migration vers Microsoft Office 365 pour remplacer un environnement Lotus Notes obsolète. Après avoir imposé l'authentification à deux facteurs, le fabricant a utilisé les certificats clients pour éliminer les mots de passe faibles et valider l'identité des 1300 comptes Office 365, intégrant pour cela l'infrastructure PKI à Microsoft Active Directory Federated Services.

L'entreprise a activé les certificats S/MIME, qui par défaut peuvent être utilisés pour le chiffrement et les signatures numériques des utilisateurs, le tout assorti d'une fonctionnalité permettant de demander un accusé de réception des messages envoyés aux autres salariés, aux partenaires ou aux collaborateurs externes.

Une appliance de messagerie contrôle les messages entrants et sortants, tandis que des proxys web sont en place pour protéger les e-mails et le web. Cette méthode a nettement amélioré le dispositif de sécurité du fabricant, car l'activation de S/MIME peut contrer les attaques par interception (MITM, man-in-the-middle), avec l'avantage supplémentaire de chiffrer des données sensibles de propriété intellectuelle si nécessaire.

Outre les outils de sécurité, l'entreprise a investi dans la formation et les actions de sensibilisation. « Nos collaborateurs savent qu'ils doivent chiffrer le contenu dès lors qu'il est confidentiel, voire ultra-confidentiel, même lorsqu'ils envoient un message en interne », confirme le RSSI.

La maison-mère du fabricant a collaboré avec un spécialiste PKI pour réaliser l'implémentation et la configurer de façon à bloquer les e-mails malveillants. Quelques problèmes ont surgi lorsque les politiques de sécurité existantes ont rejeté ou isolé le trafic chiffré, perturbant ainsi la remise des e-mails. Avec le recul, le RSSI considère que la gestion du programme de formation aurait pu être mieux planifiée. « Les salariés ont accepté les nouvelles politiques et les changements dans leurs processus à cause de l'incident du malware », constate-t-il. Aujourd'hui, le programme de sécurité de l'entreprise est encore en phase de maturation.
Un exercice de recherche et classification des données a été déployé et des améliorations ont été apportées à la sécurité périmétrique de ses ressources sur site.

La PKI au service de la sécurisation des demandes de prêt et de l'intégration aux fonctions analytiques avancées

Pour moderniser ses processus de prêt et améliorer son expérience client, une grande banque s'est tournée vers une solution PKI managée dans une double optique : protéger ses documents de prêt numérisés et s'assurer de leur chiffrement intégral dans le cadre de ses obligations de conformité. Comptant pour une part importante de l'investissement, la sécurité ne devait pas interférer avec l'objectif global consistant à créer une expérience dynamique et simple pour les nouveaux clients.

La banque a évalué des solutions de sécurité susceptibles de soutenir sa stratégie d'accélération de ses processus d'octroi de prêt, de la demande jusqu'à la clôture du dossier. L'équipe d'évaluation s'est alors mise en quête de solutions PKI suffisamment flexibles pour un déploiement sur le terrain et suffisamment ouvertes pour s'intégrer à l'infrastructure back-end existante. Les réticences de collaborateurs dans certains services ont joué en faveur d'une solution simple d'utilisation, robuste, peu consommatrice de ressources et performante malgré son intégration à plusieurs autorités de certification.

La banque devait concevoir une solution capable de transformer ses big data non structurées en contenu structuré compatible avec le moteur d'intelligence artificielle de son assistant virtuel. Elle disposait des ressources nécessaires pour missionner des data scientists et une équipe de développement sur cette tâche. Côté sécurité des données, le choix d'une solution PKI s'est imposé.

Un service PKI était nécessaire pour l'intégration au logiciel de conformité interne, chargé de suivre le processus d'intégration de nouveaux clients. Les exigences de sécurité imposaient également la haute disponibilité, des fonctions performantes de reprise d'activité et une instance dédiée du service PKI pour interagir avec le cloud privé virtuel de la banque. La solution PKI devait en plus assurer le chiffrement des documents de prêt, tout en s'intégrant au référentiel de contenu de la banque et à un environnement d'analytique avancée, fortement sollicité pour les actions de fidélisation et l'amélioration des offres de services de la banque.

« Toute interruption de service était hors de question et nous devions impérativement garder le contrôle total de la propriété des clés », signale le RSSI à IDC. « Nous savons qu'une solution PKI est le meilleur moyen de répondre aux exigences de sécurité de ressources d'importance vitale. Nous avons constaté de nombreuses améliorations au niveau des métiers. Cela nous donne confiance dans nos capacités à sécuriser ces transactions critiques et à tenir nos obligations de conformité. »

L'implémentation exige une base de code côté serveur et s'appuie sur des agents installés sur les terminaux pour les opérations de chiffrement et de signature numérique lors de la création et de l'envoi de documents. L'ensemble du processus est suivi et journalisé sur le web au moyen du protocole HTTPS. Les collaborateurs créent les documents sur le terminal, mais le référentiel réside sur le serveur.

Le référentiel de contenu de la banque et un environnement d'analytique avancée sont en cours d'intégration avec un nouvel assistant virtuel destiné à automatiser le processus de signature de l'emprunteur et à dissiper l'angoisse habituellement associée aux procédures de prêt. Les opérations de numérisation, impression et télécopie des demandes de prêt n'ont plus lieu d'être.
Dès que la solution PKI valide l'identité de l'emprunteur, inutile pour ce dernier de se rendre dans une agence pour finaliser les documents auprès d'un conseiller ou d'un banquier. Désormais, le demandeur peut réaliser chez lui toute la procédure, en toute sécurité sur le web. Aujourd'hui, la solution monte en capacité pour englober jusqu'à 20 000 personnes, notamment les juristes, experts du risque et de la conformité, conseillers en prêts, clients et autres acteurs du processus.

« La mise en œuvre de la solution PKI exige une planification soigneuse », prévient le RSSI. « La rationalisation et la centralisation d'une infrastructure de sécurité se justifient pleinement, mais les obstacles politiques demeurent, notamment le risque d'exposition des données », poursuit-il. « Si vous mettez tous vos œufs dans le même panier, vous risquez de vous faire pirater. Pour la centralisation, votre solution d'analyse du comportement des utilisateurs doit pouvoir faire abstraction de tous les silos ».

Une banque régionale se tourne vers une solution PKI managée pour la mobilité et la vérification étendue

Il avait fallu de nombreuses années à cette grande banque régionale pour bâtir son programme PKI, gérant elle-même l'infrastructure nécessaire à son autorité de certification (AC) interne. Mais elle avait de plus en plus de difficultés à recruter, former et fidéliser des professionnels compétents pour gérer son infrastructure de sécurité. D'après un responsable sécurité de la banque interrogé par IDC, la complexité de la gestion d'un programme PKI fragmenté a poussé certains membres de l'équipe de sécurité au départ.

De fait, l'équipe informatique interne peinait à gérer une multitude d'implémentations PKI qui entravaient l'authentification utilisateur. Différentes solutions avaient été déployées en presque 10 ans : prise en charge des cartes à puce, solution pour l'accès VPN et l'accès des appareils mobiles, ainsi qu'un système parallèle chargé du chiffrement et de la signature des e-mails. La complexité de ces solutions hétéroclites se répercutait souvent sur l'expérience utilisateur, notamment en raison d'un mécanisme dépassé pour l'émission de certificats. L'AC interne ne parvenait pas à publier de nouvelles listes de contrôle d'accès dans les temps, tandis que les utilisateurs n'arrivaient pas à s'authentifier sur le réseau. Cette anomalie était due tantôt à la défaillance matérielle d'un module de sécurité, tantôt à un problème de serveur Windows, tantôt à autre chose. « Il peut se produire beaucoup de choses », concède un ingénieur de sécurité.

« Nous craignions d'avoir atteint un point où nous risquions à tout moment une paralysie du réseau. Si aucun de nos utilisateurs ne peut accéder à certaines applications ou s'authentifier en raison de l'indisponibilité de l'infrastructure PKI, notre équipe sera dans de beaux draps », confie l'ingénieur sécurité à IDC.

Aujourd'hui, la banque a éliminé toute complexité pour les utilisateurs d'appareils mobiles et VPN. Pour ce faire, elle a intégré l'infrastructure PKI à une nouvelle plateforme de gestion des appareils mobiles, réduisant les identifiants à une seule application de carte à puce pour ces terminaux, le tout sous la surveillance d'un service PKI managé. « L'équipe informatique réduit progressivement le nombre de systèmes redondants, à commencer par la modernisation de ses processus d'octroi de terminaux et l'utilisation de cartes à puce mieux adaptées à Active Directory », explique l'ingénieur en sécurité.

Le choix d'un service PKI managé a également facilité le travail de l'équipe informatique. « L'infrastructure entièrement sur site et le degré de sécurité recherché ont engendré une complexité et une surcharge

de travail extrêmes, ingérable pour nos équipes », constate l'ingénieur sécurité. « À moins de travailler dans une grande structure avec de gros effectifs, la gestion en interne d'un programme PKI n'est probablement pas une bonne idée. »

Par ailleurs, l'équipe informatique interne collabore avec le spécialiste PKI pour intégrer l'émission des certificats à ses cartes à puce. Elle a également remplacé son système disparate par un service managé plus simple pour la sécurisation des e-mails. La banque gère son propre environnement Active Directory et poursuit la consolidation de ses processus de gestion des autorités de certification et d'émission de certificats. Comme la plateforme de gestion des cartes à puce est désormais intégrée à la gestion des certificats numériques, ces derniers servent aussi pour l'accès VPN. L'adoption d'un service PKI managé a grandement simplifié la gestion du cycle de vie des certificats dans les 40 agences, recentrant du même coup les équipes informatiques sur d'autres projets.

Un constructeur high-tech choisit une solution PKI pour l'identification des terminaux, les accès VPN et la création d'un environnement Zero Trust pour ses ressources critiques

Un fournisseur de solutions de gestion d'énergie électrique a verrouillé son environnement en misant entièrement sur les fonctions intégrées des services de certificats Active Directory et en imposant la validation des terminaux gérés via des certificats sur les appareils et son infrastructure PKI. Le but était de sécuriser l'accès aux ressources critiques en établissant une méthode validant l'authenticité des utilisateurs qui demandent un accès VPN à son environnement et en contrôlant l'intégrité des terminaux gérés avant d'accorder cet accès. L'entreprise voulait sécuriser la connectivité et accélérer le processus d'autorisation d'accès des utilisateurs aux ressources de l'entreprise, indépendamment de leur localisation. Les certificats numériques permettent d'appliquer un strict contrôle en exigeant un terminal entièrement géré pour accéder aux ressources critiques. Ils peuvent en plus restreindre l'accès des prestataires et partenaires par l'émission de certificats d'authentification utilisateur configurés à cette fin, qui appliquent les règles de pare-feu nécessaires.

« Notre dispositif de défense s'articule autour de l'extrême difficulté d'extraction des clés depuis les terminaux Microsoft », résume le RSSI de l'entreprise, qui ajoute qu'une série d'investissements est en cours pour établir un environnement Zero Trust. La difficulté de cette gestion est encore accrue par un déploiement continu de terminaux Mac sur son réseau pour le bureau d'études, le marketing et d'autres cas particuliers. L'entreprise collabore donc avec un spécialiste PKI pour concevoir un moyen de déployer un certificat d'authentification sur Mac, tout en s'assurant que la clé privée est stockée de manière sécurisée, sans possibilité d'exportation.

Au fur et à mesure du déploiement, l'entreprise ajoutera des métadonnées dans les nouveaux certificats émis pour permettre l'authentification des terminaux par empreinte digitale. Ces certificats serviront au processus d'authentification et à la connectivité VPN vers sa plateforme sur site de gestion des accès web. L'entreprise apprécie la flexibilité de la plateforme, qui permet aux salariés d'accéder à un portail hébergeant Office 365 et d'autres ressources d'entreprise depuis leur appareil mobile.

L'architecte sécurité en chef de l'entreprise émet cependant des réserves quant à l'authentification par certificat sur les appareils mobiles. « Il ne suffit pas que l'entreprise installe un certificat sur un appareil pour que tout ce qui est sur cet appareil puisse interagir avec le certificat. Si la prise en charge des certificats les plus répandus n'a pas été prévue au moment du développement de l'application, alors l'application ne sera pas compatible », précise-t-il. De fait, l'application peut très bien ne pas communiquer avec le certificat sur le terminal qui l'héberge. En conséquence, l'entreprise travaille à une nouvelle stratégie d'identification des accès cloud qui prend en charge les applications développées en interne, mais aussi les autres applications utilisées par les salariés.

Un prestataire de traitement des paiements sécurise des milliers de terminaux de point de vente avec une solution PKI

Pour les fabricants, il devient impérieux d'ajouter des mécanismes de sécurité matérielle et logicielle aux objets connectés (IoT) pour le chiffrement, l'authentification et l'autorisation, ainsi que pour valider l'intégrité des terminaux au niveau du firmware, du système d'exploitation et des applications. Les certificats numériques représentent les bases de la confiance pour atteindre ce niveau fondamental de sécurité sur les systèmes embarqués.

Un prestataire européen de traitement des paiements sécurise des milliers de terminaux de point de vente (POS) à l'aide d'un service PKI managé qui assure une authentification tierce fiable et mutuelle des appareils sur les réseaux. La nouvelle approche mise en place par ce prestataire nécessite l'installation de certificats numériques pour identifier les appareils et d'un agent capable de communiquer avec la plateforme cloud du prestataire. La plateforme assure le provisionnement, le suivi et la maintenance des terminaux POS, avec un mécanisme sécurisé de rotation des certificats.

L'architecte de sécurité qui supervise l'implémentation affirme que les certificats numériques limitent la fraude au niveau des fabricants, tout en permettant à son entreprise de mieux contrôler l'usage des terminaux. « L'option PKI a été retenue car les certificats peuvent être gérés pendant tout le cycle de vie et leur volume peut augmenter sans problème », souligne-t-il. « Il fallait impérativement déployer une solution inviolable par un attaquant muni de certificats numériques frauduleux », note l'architecte sécurité. Le mécanisme mis en œuvre sécurise les données au repos ou en transit et valide l'identité de l'émetteur et du destinataire des informations.

En plus d'assurer la supervision du provisionnement des terminaux et la gestion des identifiants sur les systèmes POS, la solution permet au prestataire de commercialiser des services de chiffrement pilotés par des politiques et vérifie que les magasins respectent bien les obligations de conformité.

D'autres appareils à haut risque utilisés par le prestataire ne se prêtent pas à une méthode avec agent. Un fabricant de systèmes embarqués collaborant avec la société de traitement des paiements et d'autres commercialise des produits dont l'espace de stockage ou la puissance de calcul n'est pas compatible avec un agent ou un logiciel client. Le fabricant a indiqué à IDC que ses ingénieurs utilisent une solution PKI au moment de la production pour la communication sécurisée de machine à machine et la signature de code. « Nos clients nous ont demandé d'élaborer une méthode pour garantir l'intégrité du code que nous leur envoyons », précise le responsable de l'équipe de sécurité, qui a travaillé avec l'équipe d'ingénierie. L'objectif était de choisir une solution PKI managée plutôt que de l'incorporer à l'implémentation PKI existante du fabricant.

« Nous cherchons des moyens d'automatiser le processus sans surcharger l'équipe travaillant sur nos processus internes », ajoute-t-il.

L'OPTION DIGICERT

DigiCert offre des solutions PKI, IoT et TLS/SSL pour l'identification et le chiffrement. Pensée pour révolutionner la gestion PKI, DigiCert ONE offre un éventail de solutions de gestion adaptées à de nombreux cas d'usage PKI. Cette plateforme flexible peut être déployée sur site, en local ou dans le cloud, et ainsi satisfaire aux exigences en termes de conformité, d'intégrations personnalisées et d'airgap. Quant à l'outil DigiCert Enterprise PKI Manager reposant sur DigiCert ONE, il a été conçu pour la gestion des problématiques liées à l'identification, l'authentification, le chiffrement et l'intégrité des appareils.

Au menu d'Enterprise PKI Manager :

- Enrôlement automatisé et par API des nouveaux utilisateurs et appareils grâce aux certificats numériques
- Intégration à des plateformes MDM/UEM leaders pour un enrôlement et une gestion sécurisés des appareils

- Certificats S/MIME pour l'authentification et le chiffrement des e-mails
- Signature de document sécurisée dans tous les environnements réseau physiques et virtuels de l'entreprise
- Intégration aux autres gestionnaires de workflows DigiCert ONE pour une signature de code sécurisée pour les logiciels et appareils IoT

DÉFIS ET OPPORTUNITÉS

Les entreprises ont engagé des investissements à long terme dans leur infrastructure PKI existante. Les professionnels de la sécurité qu'IDC a interrogés sont unanimes : le processus de rationalisation et d'automatisation d'un écosystème PKI souvent complexe et fragmenté est un projet aux multiples ramifications qui doit s'étaler sur plusieurs années. Cet effort exige un investissement initial et des spécialistes PKI aguerris aux processus métiers et à l'infrastructure informatique de l'organisation, l'emplacement des ressources critiques, mais aussi la tolérance au risque et la stratégie de croissance définies par les dirigeants. Si les projets d'amélioration ne sont pas rigoureusement planifiés et scrupuleusement exécutés, ils peuvent prendre du retard, voire échouer pour de multiples raisons : montée en flèche de la croissance, fusions et acquisitions, adoption de nouvelles technologies, changement de stratégie métier et autres facteurs exogènes.

CONCLUSION

Face à l'adoption croissante du cloud et au nombre d'organisations qui gèrent l'accès aux données et aux autres ressources d'entreprise dans des environnements hybrides et multi-cloud, les technologies PKI deviennent incontournables. Elles sont appelées à jouer un rôle central dans la validation de l'intégrité des transactions et l'établissement d'une connexion fiable et sécurisée entre humains et systèmes informatiques. Un constat confirmé par *l'enquête IDC sur les services data* publiée en 2020. En 2020, plus de 95 % des entreprises de plus de 5 000 salariés déclaraient chiffrer des données au repos dans des environnements IaaS and PaaS publics. Plusieurs constats suggèrent les raisons de l'essor des infrastructures PKI :

- **Évolutivité :** Les personnes interrogées pour les besoins de cette étude ont mis en œuvre les technologies PKI à des échelles et volumes considérables, comme en témoigne le nombre d'utilisateurs, de domaines et de demandes d'authentification impliqués. Ces départements informatiques étaient soumis à des contraintes d'évolutivité extrêmes. Les entreprises de l'échantillon comptaient des effectifs allant de 1 000 à 120 000 personnes, et toutes se sont félicitées de la performance et la viabilité de leurs solutions. Elles se sentent prêtes à poursuivre leur développement autour des technologies PKI pour répondre à leurs besoins dans plusieurs domaines : accès distant, connectivité sans fil sécurisée, signature de documents, chiffrement et sécurisation des e-mails.
- **Services PKI managés :** Les difficultés et problèmes existants étaient liés à la multiplicité des implémentations PKI, source de complexité, et à la pénurie de compétences réseau et sécurité pour gérer cette complexité. Ces contraintes stimulent l'adoption de services PKI managés pour épauler les équipes en place et limiter les perturbations par l'automatisation des activités PKI courantes (intégration des nouvelles recrues, émission ou révocation des certificats, etc.).
- **Sophistication des attaques :** Les personnes interrogées ont déclaré que tant qu'une solution PKI est intégrée et fonctionnelle, leurs équipes informatiques préfèrent ne pas y toucher. Pourtant, il est évident que la hausse de la complexité et l'absence de supervision proactive aboutissent à des vulnérabilités et des problèmes de configuration dont les attaquants peuvent profiter. Ils peuvent dès lors mener des attaques par interception (man-in-the-middle) pour surveiller des collaborateurs spécifiques ou, plus communément, voler des données sensibles à des fins crapuleuses.

Cette étude IDC montre qu'une infrastructure PKI est essentielle à la réussite des initiatives de transformation digitale pour une diversité de secteurs d'activité et de scénarios. Les processus métiers actuels peuvent s'appuyer sur une infrastructure PKI pour renforcer l'automatisation, réduire les tensions et rationaliser le traitement des informations digitales et des transactions électroniques. Une implémentation PKI forme également un élément essentiel pour les équipes de sécurité soumises à de nouvelles réglementations sur la sécurité et la confidentialité des données. Les RSSI conviennent qu'une implémentation PKI rationalisée réduit la complexité et que l'option des services PKI managés peut réduire les surcharges et les coûts de gestion, avec à la clé une réorientation des équipes de sécurité vers d'autres activités prioritaires. En corollaire, cette étude confirme que les certificats numériques sont des composants essentiels capables de contrecarrer des attaques ciblées, de veiller à l'intégrité des transactions sensibles et de confirmer l'identité des parties engagées dans une transaction commerciale. L'étude montre une autre facette importante des technologies PKI : utilisées en appui de nouveaux projets d'amélioration de la satisfaction client, elles permettent aux clients d'effectuer des transactions sensibles en toute sécurité depuis leur domicile.

Message de notre partenaire

DigiCert est le leader des solutions PKI, IoT et SSL/TLS de chiffrement et d'identification. Les entreprises les plus innovantes, dont 89 % du Fortune 500 et 97 % des plus grandes banques mondiales, font confiance à DigiCert et à son expertise dans l'identification et le chiffrement des serveurs web, appareils d'entreprise et équipements IoT. DigiCert est reconnue pour sa plateforme de gestion des certificats destinée aux entreprises, son support client rapide et expert, et ses solutions leaders du marché. Pour suivre toute l'actualité et les nouveautés DigiCert, rendez-vous sur www.digicert.com/fr ou suivez-nous sur Twitter @digicert.

À propos d'IDC

International Data Corporation (IDC) est le premier prestataire mondial en études de marché, services de conseil et événements à destination des secteurs de l'informatique, des télécommunications et des technologies grand public. IDC accompagne les professionnels, les dirigeants et les investisseurs du secteur informatique dans leurs décisions d'achats technologiques et de stratégie métier. Plus de 1 100 analystes IDC proposent une expertise locale, régionale et internationale sur les opportunités et tendances technologiques et sectorielles dans plus de 110 pays. Depuis 50 ans, IDC livre à ses clients des éclairages stratégiques qui les aident à atteindre leurs grands objectifs. IDC est une filiale d'IDG, premier groupe mondial de l'événementiel, des études sectorielles et de la presse spécialisée.

Siège mondial

5 Speen Street
Framingham, MA 01701
États-Unis
508.872.8200
Twitter : @IDC
idc-community.com
www.idc.com