IoT, Authentification et services Cloud, principaux vecteurs de la remarquable croissance de la PKI en France, selon la nouvelle étude d'Entrust

L'étude annuelle sur les tendances PKI et IoT révèle que 2020 sera une année marquée par des défis sans précédent pour la PKI, changements et incertitude dans un monde en pleine évolution.

Paris, France, 13 octobre 2020 – L'infrastructure de protection des données s'accroît rapidement au sein des entreprises en taille, portée et ampleur, ce qui se traduit par une adoption spectaculaire des infrastructures à clé public (PKI), et ce dans le monde entier, révèle la nouvelle étude d'Entrust. La PKI est au coeur de presque toutes les infrastructures IT, permettant de sécuriser toutes sortes d'initiatives numériques critiques telles que le Cloud, le déploiement des terminaux mobiles, les identités et l'Internet of things (IoT).

L'étude annuelle sur les tendances en matière de PKI et d'IoT conduite par le Ponemon Institute à l'instigation de nCipher Security, société du groupe Entrust, s'est appuyée, en France, sur les retours de 106 professionnels. La France est l'un des 17 pays ayant participé à ce rapport regroupant les réponses de 6157 experts en informatique et en technologies de l'information.

En France, ce sont les services basés sur le Cloud public qui favorisent le plus le déploiement d'applications utilisant des PKI (54% en 2020, soit une augmentation de 18% par rapport à 2019). Le pourcentage d'utilisation de la PKI pour des applications situées dans le Cloud public a progressé d'une année sur l'autre de 26% à 87%. Pour l'authentification des utilisateurs en entreprise, le taux de croissance est de 25% pour atteindre 71%. La PKI confirme son rôle critique au sein des applications d'entreprise.

Mais le manque de compétence ainsi qu'une maîtrise imparfaite des capacités de sécurité de l'outil restent parmi les principaux handicaps à surmonter pour répandre l'usage de la PKI, et ce pour 49% des professionnels interrogés. Ce qui n'empêche pas la France d'arriver en seconde place derrière les Etats-Unis en termes d'adoption des plateformes PKI avec 10 applications en moyenne prises en charge.

A noter que les deux plus grands domaines d'évolution, avec une certaine part d'incertitude, sont en France l'Internet des Objets (54%) et les contraintes réglementaires et évolution des normes (41%).

Autorités de Certification interne, un choix typiquement Français

Contrairement à la tendance globale qui tend vers l'utilisation d'Autorités de Certification (AC) externes et les services managés, la France opte plus facilement pour le modèle basé sur une AC interne en passant de 12% à un quota de 68%. De même, l'utilisation d'AC

privées mais gérées en externe n'est que de 24% sur le territoire français à comparer à une tendance mondiale gravitant autour des 43%.

Paradoxalement, les entreprises françaises n'hésitent pas à utiliser des services publics d'AC. Elles possèdent même le taux d'utilisation le plus fort parmi tous les pays ayant participé à l'étude en franchissant la barre des 53%, soit une hausse de 20% par rapport à l'an passé.

Une tendance également confirmée par le nombre de certificats (émis et acquis) gérés par une entreprise qui fait un bond de 73% en passant de 32787 in 2019 à 56760 en 2020. Une situation qui rend encore plus critique la gestion de certificats.

La sécurité des IoT prime en France

Inventorier pour mieux protéger telle est la priorité des experts IT français : selon l'étude, en 2020, l'inventaire des IoT devient ainsi la plus importante des fonctionnalités Sécurité des Objets de l'Internet. Les répondants français ont également affirmé qu'il était important que les modules de sécurité matériels (HSM) gérant les clés privées des Autorités de Certification racine et émettrice soient certifiées FIPS conformément aux préconisations NIST.

L'étude montre également que les experts Français sont placés parmi les meilleurs utilisateurs d'outils pour contrer les principales menaces visant les IoT et le font d'ailleurs plus efficacement que la majeure partie des pays participant à cette analyse. Ainsi le déploiement des correctifs et des mises à jour est au second rang de leurs préoccupations après l'inventaire. En revanche des progrès restent encore à faire au niveau du chiffrement des IoT, des plateformes et des dépôts de données dédiées IoT et ce malgré une faible hausse de 24 à 26% par rapport à l'an passé.

Une PKI à la française

Pour les entreprises françaises, les points les plus importants au sein d'une architecture PKI sont par ordre d'importance : les environnements et bâtiments sécurisés (59%), l'authentification à facteurs multiples pour les administrateurs (50%) et enfin pour 33% des répondants, les pratiques de sécurité formelles et documentées.

L 'adoption massive de HSM (module de sécurité matériel) a été poussée par l'augmentation du nombre d'Autorité de Certification racine en ligne (à hauteur de 48%) alors que l'usage conseille l'AC racine hors ligne comme la bonne pratique historique. Une habitude peu à peu détrônée du fait de cette arrivée massive de HSM. Les AC émettrices en légère baisse (5%), avec 46% en 2020 et les AC racine hors ligne en progrès de seulement 3% mais toujours en deçà du score global de 39% ont également impactés l'adoption des HSM.

Contrairement à la nouvelle tendance générale qui annonce le déclin de l'OCSP en termes de révocation de certificats, l'utilisation de cette technique croît en France de 13% pour atteindre 72%, soit le plus fort taux de croissance de l'étude. Cependant le taux d'utilisation de la liste automatisée de révocation des certificats, CRL, croît tout de même de 20% sur la même période.

Une autre spécificité française, 10% de plus d'utilisation d'un simple de mot de passe pour la PKI que la tendance globale avec 33%.

La France est également l'un des pays où l'on emploie le moins de spécialistes PKI et pourtant le second pays parmi les 17 ayant participé à cette étude à s'appuyer sur des fournisseurs de services pour cette fonction.

Téléchargez votre exemplaire ici

Méthodologie de l'étude 2020 « Tendances Mondiales de la PKI et l'IoT »

L'étude « 2020, Tendances Mondiales de la PKI et l'IoT » donne un état des lieux la maturité de la PKI, des enjeux et de l'influence de l'IoT sur l'évolution de la PKI. Le rapport résume les résultats de la cinquième étude annuelle à laquelle ont participé 1934 professionnels de la Sécurité IT, répartis dans 17 pays et régions : Australie, Brésil, France, Allemagne, Hong Kong, Inde, Japon, Mexique, Moyen Orient (Arabie Saoudite et Emirats Arabes Unis), Hollande, fédérations de Russie, Corée du Sud, Asie du Sud-Est (Indonésie, Malaisie, Philippines, Thaïlande et Vietnam), Suède, Taïwan, Royaume Uni et Etats-Unis.

Cette étude 2020 est le cinquième rapport annuel consacré aux tendances de la PKI et de l'IoT, commandité par nCipher Security, société du groupe Entrust et leader du marché des modules matériels de sécurité (HSM). nCipher renforce l'autonomie des entreprises d'envergure mondiale, en conférant à leurs informations et applications critiques les bases de confiance, d'intégrité et de contrôle indispensables.

À propos de nCipher Security
Leader du marché des modules matériels de sécurité (HSM) à usage général, nCipher Security, société du groupe Entrust, renforce l'autonomie des entreprises d'envergure mondiale, en conférant à leurs informations et applications critiques les bases de confiance, d'intégrité et de contrôle indispensables. Si l'environnement digital actuel, en constante mutation, améliore l'expérience client, confère un avantage concurrentiel et améliore l'efficacité opérationnelle, il multiplie aussi les risques pour la sécurité. Nos solutions de chiffrement sécurisent les technologies émergentes – cloud, IdO, blockchain, paiement électronique – et aident à respecter les nouvelles obligations de conformité, en utilisant la même technologie éprouvée que celle dont dépendent aujourd'hui les entreprises mondiales pour se protéger contre les menaces pesant sur leurs données sensibles, leurs communications réseau et leurs infrastructures d'entreprise. Nous conférons à vos applications critiques la base de confiance nécessaire, en préservant l'intégrité de vos données et en vous donnant un contrôle total, aujourd'hui, demain et à tout moment. www.ncipher.com
Suivez-nous sur LinkedIn, Twitter, Facebook et Instagram (nCipherSecurity).