Protection des données clients : la priorité n° 1 selon l'étude nCipher 2020 sur les tendances mondiales du chiffrement

Face à l'accélération des initiatives de digitalisation des entreprises, services cloud et Internet des Objets (IoT) en tête, ainsi qu'à l'essor des volumes et des types de données, la protection des données personnels des client s'avère la priorité n° 1 des professionnels du secteur informatique. C'est ce que révèle l'étude 2020 sur les tendances mondiales du chiffrement menée par le Ponemon Institute. Pour la quinzième édition de son enquête multinationale sur les modalités et les motifs d'adoption du chiffrement dans les entreprises, l'institut a collaboré avec nCipher Security, société du groupe Entrust Datacard figurant parmi les leaders mondiaux sur le marché des modules de sécurité matériels (HSM).

Ce communiqué de presse contient des éléments multimédias. Voir le communiqué complet ici : https://www.businesswire.com/news/home/20200407005309/fr/

Risques, moteurs d'adoption et priorités

Pour la première fois, la protection des données clients s'avère le premier moteur d'adoption du chiffrement (54 % des sondés), au détriment de la conformité arrivée en quatrième position (47 %). Priorité historique du secteur, la conformité réglementaire marque le pas depuis 2017, signe que le chiffrement n'est plus une exigence, mais un choix proactif visant à protéger les informations critiques.

L'erreur humaine reste considérée comme le principal risque d'atteinte aux données sensibles (54 %), nettement devant la crainte d'un piratage informatique (29 %) ou d'un comportement malveillant des employés (20 %). En comparaison, les menaces jugées les moins importantes sont notamment les interceptions gouvernementales (11 %) et les requêtes de données en application de la loi (12 %).

Défi n° 1 : l'analyse des données

Face à la prolifération des données issues de la digitalisation, des services cloud, des solutions de mobilité, des objets connectés et de l'avènement des réseaux 5G, l'analyse des données continue de représenter le défi majeur entravant la planification et l'exécution d'une stratégie de chiffrement, comme le déclarent 67 % des sondés. Et cette proportion va très probablement augmenter vu l'essor du télétravail engendré par la pandémie en cours. De fait, les employés sont amenés à utiliser des données à leur domicile, ainsi qu'à créer des copies supplémentaires sur leurs appareils privés et dans le Cloud.

Blockchain, calcul quantique et adoption des nouvelles technologies de chiffrement

Selon cette étude, 48 % des sondés ont adopté des stratégies de chiffrement à l'échelle de leur entreprise, contre 45 % en 2019. Le chiffrement se généralisant peu à peu, comment les

entreprises envisagent-elles l'avenir ? À court terme, 60 % d'entre elles prévoient le recours à la blockchain, en priorité dans les scénarios d'utilisation suivants : cryptomonnaie/portefeuilles dédiés, mouvements d'immobilisation, identité, chaîne logistique et contrats intelligents.

D'autres technologies font beaucoup parler d'elles, mais ne figurent pas encore dans les tablettes des entreprises informatiques. Ainsi, pour la plupart des professionnels du secteur, l'adoption généralisée du calcul sécurisé multi-parties et du chiffrement homomorphique n'aura pas lieu avant au moins cinq ans pour le premier et six pour le second. Il faudra attendre plus de huit ans pour que les algorithmes post-quantiques deviennent monnaie courante.

Confiance, intégrité, contrôle

Le recours aux modules de sécurité matériels (HSM) continue d'augmenter. De fait, 48 % des sondés déclarent en déployer pour créer un environnement consolidé et inviolable offrant un degré supérieur de confiance, d'intégrité et de contrôle, côté données et côté applications. Les entreprises implantées en Allemagne, aux États-Unis et au Moyen-Orient sont plus susceptibles de recourir aux HSM, tandis que les entreprises australiennes, allemandes et américaines sont les plus enclines à attribuer de l'importance à ces équipements dans le cadre de leurs activités de chiffrement ou de gestion stratégique.

Le recours aux HSM ne se limite plus aux scénarios classiques comme l'infrastructure à clés publiques (ICP), les bases de données et les protocoles de sécurisation des applications et des réseaux (TLS/SSL). L'exigence d'un chiffrement fiable imposée par les nouvelles initiatives digitales s'est traduite par un essor significatif des HSM aux fins suivantes : chiffrement des mégadonnées (+17 %), signature de code (+12 %), racine de confiance IoT (+10 %) et signature de document (+7 %). En outre, 35 % des sondés déclarent utiliser les HSM pour sécuriser l'accès aux applications hébergées sur un cloud public.

Objectif : le Cloud

Quatre-vingt-trois pour cent des sondés déclarent procéder au transfert de données sensibles vers le Cloud ou planifier une telle migration dans les 12 à 24 prochains mois, les entreprises installées aux États-Unis, au Brésil, en Allemagne, en Inde et en Corée du Sud étant les plus adeptes de cette pratique.

Au cours des 12 prochains mois, les sondés prévoient un essor considérable du marché des HSM pour la génération et la gestion des clés de chiffrement BYOK (Bring Your Own Key), ainsi que l'intégration croissante avec les solutions de sécurisation des accès cloud CASB (Cloud Access Security Broker) pour gérer les clés et les opérations cryptographiques. D'après les résultats de l'enquête, les fonctionnalités de chiffrement revêtant le plus d'importance dans le Cloud sont les suivantes :

- Prise en charge du protocole d'interopérabilité de gestion des clés KMIP (Key Management Interoperability Protocol) (67 %)
- Intégration SIEM (Security Information and Event Management) (62 %)
- Contrôles d'accès granulaire (60 %)
- Journaux d'audit d'utilisation des clés (55 %)
- Contrôle d'accès des utilisateurs disposant de privilèges (50 %)

« Aux yeux des consommateurs, les marques se doivent de protéger les données du client contre toute atteinte et de veiller aux intérêts de ce dernier. Cette enquête prouve que les dirigeants informatiques prennent ces attentes au sérieux : en effet, ils classent pour la première fois la protection des données client en tête des moteurs de croissance du chiffrement », souligne Larry Ponemon, PDG du Ponemon Institute. « Le recours au chiffrement atteint un taux record cette année : 48 % des sondés ont déclaré que leur entreprise met en œuvre un projet unifié de chiffrement à grande échelle. En sus, 39 % des sondés attestent que leur structure applique un projet ou une stratégie ciblant certains types d'applications et de données. »

« À l'ère numérique, l'impact de la pandémie actuelle souligne à quel point la sécurité et l'identité sont devenues essentielles pour les entreprises et les particuliers, au travail comme à la maison », précise John Grimm, vice-président en charge de la stratégie chez nCipher Security. « Les professionnels subissent une pression permanente liée à deux objectifs : garantir une sécurité maximale et optimiser la fluidité d'accès. Il leur incombe de protéger leurs données client, leurs informations métier essentielles et leurs applications, tout en assurant la continuité des activités. Les solutions de sécurité nCipher offrent aux clients un gage de confiance quant à l'intégrité et à la fiabilité de leurs données, de leurs applications et de leur propriété intellectuelle. »

Autres tendances majeures :

- L'Allemagne (66 %) enregistre le taux le plus élevé d'entreprises disposant d'une stratégie de chiffrement généralisée, devant les États-Unis (66 %), la Suède (62 %), Hong Kong (60 %), les Pays-Bas (56 %) et le Royaume-Uni (54 %).
- Le chiffrement porte avant tout sur les données liées au paiement (54 % des sondés) et les enregistrements financiers (54 % des sondés).
- Les données les moins souvent chiffrées sont les informations de nature médicale (25 % des sondés) : un résultat surprenant au vu de la sensibilité de ces données et des récentes failles de sécurité très médiatisées dans le secteur de la santé.
- Le recours extensif au chiffrement connaît la plus forte hausse dans les secteurs de l'industrie manufacturière (49 %), du tourisme (44 %) et des biens de consommation (43 %).

Pour télécharger l'étude 2020 sur les tendances mondiales du chiffrement, cliquez ici.

Méthodologie de l'étude 2020 sur les tendances mondiales du chiffrement

Fondée sur les travaux de recherche du Ponemon Institute, l'étude 2020 sur les tendances mondiales du chiffrement se penche sur le comportement des entreprises en termes de conformité, de gestion des risques accrus auxquels elles sont exposées et de recours au chiffrement pour la protection de leurs données et applications métier essentielles. L'enquête a été menée auprès de 6 457 professionnels informatiques exerçant dans une multitude de secteurs, au sein de 17 pays/régions : Allemagne, Asie du Sud-Est (Indonésie, Malaisie, Philippines, Thaïlande et Vietnam), Australie, Brésil, Corée du Sud, États-Unis, Fédération de Russie, France, Inde, Japon, Hong Kong, Mexique, Moyen-Orient (Arabie saoudite et Émirats arabes unis), Royaume-Uni, Taïwan et deux nouvelles régions représentées pour la première fois : les Pays-Bas et la Suède.

À propos de nCipher Security

Leader du marché des modules matériels de sécurité (HSM) à usage général, nCipher Security, société du groupe Entrust Datacard, 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