Votre banque est-elle suffisamment sûre ?

Cinq questions sur le chiffrement à poser à votre directeur informatique aujourd'hui.

IBM

Le défi des violations de données pour les banques

« La sécurité joue un rôle critique. Nous devons protéger les données de nos clients – c'est notre bien le plus précieux. »

Chester Gorski
Directeur de la technologie et des opérations
Techcombank

Quelle est l’importance de la menace de violation de données pour les banques ?

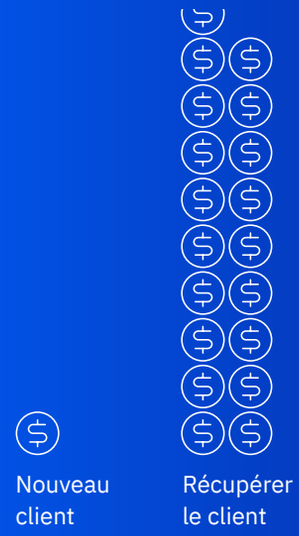
Voici quelques statistiques édifiantes :

- Suite à une violation, des banques renommées peuvent avoir à dépenser jusqu’à **18,6 fois le coût initial** d’acquisition des clients pour les récupérer[1]
- Il peut falloir aux banques jusqu’à **19,5 mois** pour retrouver le nombre de clients d’origine après une violation. Ces deux statistiques proviennent d’un rapport Solitaire Interglobal Ltd. (SIL) commandité par IBM®, sur lequel la présente brochure est basée.[2]

Pourtant, même si vous donnez la priorité à la cybersécurité, vous pouvez vous sentir déconnecté(e), en tant que directeur/rice de service, des décisions de l’entreprise en matière de sécurité. De nombreux directeurs de services de banques se sentent exclus des décisions sur les questions, les politiques et les procédures de cybersécurité appliquées par leurs établissements.

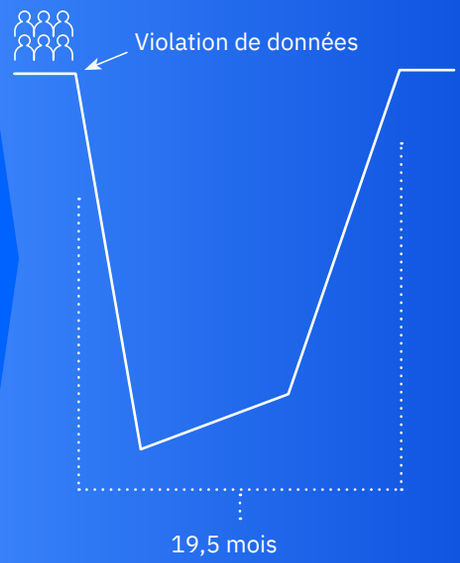
18,6x

le coût initial d’acquisition des clients pour les récupérer après une violation de données.



19,5 mois

pour retrouver le nombre de clients d’origine après une violation.



Comment pouvez-vous vous impliquer davantage dans les décisions touchant à la cybersécurité tout en vous concentrant sur les principales priorités ?

Le chiffrement des données étant une pièce centrale de n'importe quelle stratégie de sécurité, commencez par vous adresser à votre Directeur Informatique. Ce guide vise à vous aider à déterminer les bonnes questions à poser à votre Directeur Informatique pour être mieux informé(e) sur la position de votre banque en matière de cybersécurité.

En savoir plus

Mesurez à quel point vos données d'entreprise sont en sécurité →

Comment le chiffrement peut aider à protéger vos données

Le chiffrement étant une pièce centrale de la sécurité des données, une grande partie de vos questions au Directeur Technique doivent être centrées dessus. Comment le chiffrement assure-t-il, au juste, la sécurité des données ?

En termes simples, *chiffrer* des données consiste à les convertir dans un autre format pour que seules les personnes disposant d'une clé spéciale puissent les lire.[3]

Le chiffrement est peut-être la défense la plus forte contre les violations de données. Reposant sur des algorithmes hautement complexes, le chiffrement protège les données et les rend difficile à déchiffrer sans la bonne clé.[4] Même si un pirate parvient à pénétrer les défenses d'une organisation et à dérober des données chiffrées, il sera incapable d'y accéder s'il ne dispose pas de la clé de chiffrement. (Les solutions de gestion des clés de chiffrement vous aident à mettre cette clé à l'abri des pirates).

Comme les données chiffrées ne sont généralement pas accessibles par les pirates, cela minimise potentiellement les conséquences de la violation.

Maintenant que nous avons couvert les bases du chiffrement, vous pouvez réfléchir à la façon dont vous allez aborder le sujet avec vos équipes de sécurité informatique et de technologie.

Cinq questions à poser sur le chiffrement des données

Si vous êtes comme la plupart des cadres bancaires, vous savez quelles questions détaillées poser au sujet des risques métier et process. Par contre, bien que que le chiffrement et la sécurité des données soient tout aussi importants dans l'environnement actuel, vous pouvez avoir moins d'expérience dans ces questions. Les questions et réponses suivantes, basées sur une étude SIL commanditée par IBM, peuvent vous aider à mener des discussions productives avec votre Directeur Informatique.

1

Quelle quantité de données chiffrons-nous, et où se trouvent-elles ?

Est-ce que nous chiffrons tout ?

Sommes-nous *vraiment* à l'abri des cyber-attaques ?

Si votre banque est comme beaucoup d'autres, elle ne chiffre qu'un minimum de données.[5] C'est parce que de nombreuses banques pensent, à tort, que chiffrer toutes les données est excessivement coûteux et gourmand en ressources, quelle que soit la plate-forme utilisée. Un chiffrement fragmentaire crée la nécessité de suivre de près où vous chiffrez, ce que vous chiffrez et le coût en temps et en ressources de ces activités.

Votre équipe informatique suit-elle à la trace toutes les données chiffrées ? Peut-elle garantir que chaque donnée sensible est protégée ? Et comment est-elle arrivée à cette conclusion ? Ce sont là les questions difficiles que vous devez poser à votre Directeur Informatique. Le Directeur Informatique a beau être confiant dans la stratégie de cybersécurité de votre banque, si vous ne chiffrez que les données les plus sensibles, votre banque est une cible potentielle pour les pirates informatiques.

2

Sur quels critères décidons-nous quelles données doivent être chiffrées en priorité ?

Opter pour un chiffrement sélectif contraint votre banque à faire des choix difficiles quant aux données à chiffrer. Comment votre banque prend-elle ces décisions ? Certaines données, comme les numéros de carte de crédit et de sécurité sociale, doivent être chiffrées en vertu de la loi, et du fait de leur caractère hautement sensible. Cependant, il vaut la peine de regarder au-delà de ces cibles évidentes. Ainsi, des informations moins sensibles, comme les noms et les dates de naissance, peuvent elles aussi aider les pirates à usurper l'identité des clients.

Le chiffrement coûte du temps, de l'argent et des ressources informatiques, et vous et votre Directeur Informatique devez peser le pour et le contre du chiffrement de chaque nouvel ensemble de données, et être parés pour les coûts potentiels, modifications d'application et réductions du niveau de service requis.[6]

3

Qui est responsable de la stratégie de chiffrement ?

Qui doit être impliqué ?

Vous pensez peut-être que le service informatique ou sécurité est responsable du chiffrement de bout en bout. Toutefois, d'autres parties prenantes peuvent avoir à être impliquées, voire prendre le processus en main. Après tout, les données chiffrées concernent tous les services de l'organisation, de l'informatique à la finance, en passant par la comptabilité et les ressources humaines. Il est probable que les responsables de ces services voudront avoir leur mot à dire quant à la façon dont ces données sont chiffrées et gérées. Tient-on compte de ces parties prenantes ? Et communiquent-elles entre elles sur le chiffrement des données comme elles le devraient, ou travaillent-elles individuellement avec le Directeur Informatique sur différentes stratégies ?

4

Que nous coûte le chiffrement des données ?

Est-ce une affectation efficace de nos fonds ?

Surtout, notre chiffrement est-il efficace ?

La mise en œuvre et le maintien d'un chiffrement sélectif exigent des compétences, des ressources et un budget significatifs.[7] Les changements de stratégie de chiffrement peuvent affecter les accords de niveau de service de votre banque et consommer des ressources informatiques qui pourraient être consacrées, à la place, à la création d'excellentes expériences client.[8] Comme le chiffrement mobilise des ressources et un budget significatifs, il est important de le gérer efficacement, tout en garantissant qu'il soit aligné sur la stratégie de l'entreprise. Vérifiez auprès de votre Directeur Informatique que les coûts du chiffrement sont raisonnables et que votre chiffrement atteint les objectifs souhaités.

5

Quels sont les obstacles à un chiffrement intégral ?

Un chiffrement sélectif des données présente différents inconvénients, et ne protège pas pleinement votre banque contre les violations de données. Un chiffrement intégral offre une bien meilleure protection contre les cyber-attaques, mais le tenter sur certaines architectures système est extrêmement complexe, si l'on en croit l'étude SIL commanditée par IBM :

- **C'est cher.** Un chiffrement intégral dans un environnement de serveurs x86 peut présenter un coût prohibitif pour de nombreuses organisations. Incorporer le chiffrement dans toutes les applications peut également engendrer des coûts onéreux, y compris pour les modifications d'application et la main d'œuvre pour s'en occuper en permanence[9]
- **Cela nécessite une puissance de traitement significative.** Les processeurs x86 ne sont généralement pas conçus pour assurer un chiffrement à grande échelle. Le chiffrement de toutes les données peut rapidement épuiser la puissance de traitement de votre serveur, vous laissant sans ressources pour l'exécution des systèmes et applications de base.[10] Même si un chiffrement intégral est réalisable dans certains environnements x86, c'est une option peu pratique en raison de la surcharge système que cela entraîne.[11]

Si votre banque ne chiffre pas toutes ses données – ce qui est probablement le cas – c'est sans doute à cause d'une combinaison de ces difficultés. Demandez à votre Directeur Informatique quels obstacles peuvent empêcher un chiffrement intégral.

Retrouvez votre tranquillité d’esprit avec le chiffrement généralisé

« Le chiffrement généralisé est la nouvelle sensation. C’est la solution miracle qui va révolutionner le secteur. »

Tom Connolly
Directeur Général
BNY Mellon

Imaginez un instant que vous n’ayez plus à vous soucier des cinq questions précédentes.

Est-ce que vous et votre Directeur Informatique ne dormiriez pas mieux la nuit ?

L’étude SIL révèle que le chiffrement de l’intégralité des données d’une plate-forme informatique fait traditionnellement peser sur les ressources un poids prohibitif. Aujourd’hui, avec la bonne plate-forme d’entreprise, il est possible de chiffrer intégralement toutes les données d’application, de base de données et de service cloud facilement, rapidement, et avec un impact minimal sur le budget et les ressources.[12]

Le chiffrement généralisé vous permet de ne plus avoir à répondre aux questions-pièges que nous venons d’aborder. Vous simplifiez vos activités de conformité en mettant en place des stratégies couvrant des ensembles de données, et non plus simplement des éléments individuels. Et vous réduisez votre exposition aux violations en minimisant l’accès de l’administrateur aux données sensibles.[13]

Le chiffrement généralisé vous permet de...

Chiffrer efficacement

Chiffrez toutes les données avec un minimum de ressources de traitement et un impact limité sur les accords de niveau de service.[14]

Chiffrer rapidement

Le chiffrement matériel sur puce dans chaque processeur permet un chiffrement bien plus rapide des données, y compris en bloc.[15]

Chiffrer à moindre coût

Aucune modification d'application n'est requise pour mettre en œuvre le chiffrement généralisé.[16]

Explorez le chiffrement généralisé →

Collaborez pour garantir la cybersécurité →

Success story du chiffrement : Techcombank

Le secteur bancaire vietnamien connaît une croissance rapide, et Techcombank enregistre un développement proportionnel, avec 30 % de clients en plus et une augmentation du trafic en ligne de 70 % par an. Pour étendre son infrastructure en même temps que la demande en toute sécurité, Techcombank a besoin d'une plate-forme informatique d'entreprise offrant un chiffrement généralisé.

En savoir plus

Découvrez comment Techcombank sécurise ses données →

Conclusions

La sécurité de l'entreprise est au cœur des préoccupations des chefs de service, et le chiffrement est la pierre angulaire de la stratégie de cybersécurité de nombreuses banques. Poser les bonnes questions sur la cybersécurité à votre Directeur Informatique vous permettra d'être au fait de sa stratégie. Pour cette même raison, vous devez savoir quelles sont les meilleures solutions de chiffrement disponibles pour votre organisation. En choisissant la bonne plate-forme d'entreprise et en opérant un chiffrement généralisé de ses données, votre banque peut assurer plus efficacement leur sécurité.

Une meilleure sécurité des données profite à tous. Elle rassure le client, et garantit que votre innovation et votre croissance ne sont pas freinées par les menaces de piratage.

Découvrez comment conserver la confiance des clients grâce à une infrastructure sécurisée

Lire le résumé de l'étude →

Notes de fin de document

1 « Si une organisation tente de faire revenir des clients qui sont partis, les coûts de ces efforts, tels que rapportés par des organisations financières bien établies, peuvent atteindre 18,6 fois le coût initial d'acquisition du client. » - « Trusted Actions », Solitaire Interglobal Ltd, page 2, URL : https://www.ibm.com/account/reg/us-en/signup?formid=urx-34507,

2 « Retrouver le même nombre de clients financiers qu'avant une violation peut prendre jusqu'à 19,5 mois. » - « Trusted Actions », Solitaire Interglobal Ltd, page 2, URL : https://www.ibm.com/account/reg/us-en/signup?formid=urx-34507,

3 *Encryption Concepts*, IBM

4 IBID, IBM

5 « Seules 2,13 % des données d'entreprise dans les data centers sont chiffrées. » – Pervasive Encryption – A New Paradigm for Protection, Solitaire Interglobal Ltd, page 20, URL : https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

6 « En se basant sur la charge moyenne pour chaque plate-forme du groupe d'étude, ce déploiement se traduirait par l'ajout de jusqu'à 12,2 fois le nombre de serveurs actuels. Une telle hausse du nombre de plates-formes augmenterait substantiellement le coût des opérations. L'impact pour l'organisation adoptant cette solution serait considérable, et l'on assisterait à une forte hausse des dépenses en matériel, en logiciels et en ressources humaines. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 21, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

7 « En se basant sur la charge moyenne pour chaque plate-forme du groupe d'étude, ce déploiement se traduirait par l'ajout de jusqu'à 12,2 fois le nombre de serveurs actuels. Une telle hausse du nombre de plates-formes augmenterait substantiellement le coût des opérations. L'impact pour l'organisation adoptant cette solution serait considérable, et l'on assisterait à une forte hausse des dépenses en matériel, en logiciels et en ressources humaines. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 21, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

8 « En se basant sur la charge moyenne pour chaque plate-forme du groupe d'étude, ce déploiement se traduirait par l'ajout de jusqu'à 12,2 fois le nombre de serveurs actuels. Une telle hausse du nombre de plates-formes augmenterait substantiellement le coût des opérations. L'impact pour l'organisation adoptant cette solution serait considérable, et l'on assisterait à une forte hausse des dépenses en matériel, en logiciels et en ressources humaines. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 21, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

9 « En se basant sur la charge moyenne pour chaque plate-forme du groupe d'étude, ce déploiement se traduirait par l'ajout de jusqu'à 12,2 fois le nombre de serveurs actuels. Une telle hausse du nombre de plates-formes augmenterait substantiellement le coût des opérations. L'impact pour l'organisation adoptant cette solution serait considérable, et l'on assisterait à une forte hausse des dépenses en matériel, en logiciels et en ressources humaines. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 21, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

10 « En se basant sur la charge moyenne pour chaque plate-forme du groupe d'étude, ce déploiement se traduirait par l'ajout de jusqu'à 12,2 fois le nombre de serveurs actuels. Une telle hausse du nombre de plates-formes augmenterait substantiellement le coût des opérations. L'impact pour l'organisation adoptant cette solution serait considérable, et l'on assisterait à une forte hausse des dépenses en matériel, en logiciels et en ressources humaines. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 21, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

11 (1) « D'après une récente étude SIL, les organisations qui déploient le chiffrement généralisé sur IBM Z peuvent réduire le temps de traitement de jusqu'à 91,7 %. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 22, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

11 (2) « Les innovations dans la pile logicielle, de leur côté, s'appuient sur ces fonctions de chiffrement pour permettre aux organisations de protéger les données d'entreprise et client contre les menaces internes et externes, sans besoin de modifications d'application, et sans affecter les accords de niveau de service. » - extrait de l'IBM Journal of Research & Development R&D Volume 62 No 2/3 Paper 2 « Enabling pervasive encryption through IBM Z stack innovations », page 2, URL : https://ieeexplore.ieee.org/document/8270590/

12 (1) « D'après une récente étude SIL, les organisations qui déploient le chiffrement généralisé sur IBM Z peuvent réduire le temps de traitement de jusqu'à 91,7 %. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 22, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

12 (2) « Les innovations dans la pile logicielle, de leur côté, s'appuient sur ces fonctions de chiffrement pour permettre aux organisations de protéger les données d'entreprise et client contre les menaces internes et externes, sans besoin de modifications d'application, et sans affecter les accords de niveau de service. » - extrait de l'IBM Journal of Research & Development R&D Volume 62 No 2/3 Paper 2 « Enabling pervasive encryption through IBM Z stack innovations », page 2, URL : https://ieeexplore.ieee.org/document/8270590/

13 « Cela offre un chiffrement basé sur des stratégies conjugué à un contrôle d'accès, et encourage une séparation des rôles, garantissant que la sécurité reste la responsabilité des administrateurs sécurité (et non des administrateurs stockage ou autres acteurs). La granularité accrue permet un plus haut de gré de finesse dans l'application du chiffrement, pour que les utilisateurs puissent mieux déterminer quelles données sont protégées et comment. La capacité de chiffrer les données en bloc pour réduire les frais généraux atténue encore davantage les risques causés par une mauvaise identification ou classification des données sensibles, et simplifie le processus d'audit (en procédant à un chiffrement généralisé et en réduisant le nombre d'intervenants humains auditables pouvant consulter les données déchiffrées). - extrait de l'IBM Journal of Research & Development R&D Volume 62 No 2/3 Paper 2 « Enabling pervasive encryption through IBM Z stack innovations », page 4, URL : https://ieeexplore.ieee.org/document/8270590/

14 (1) « D'après une récente étude SIL, les organisations qui déploient le chiffrement généralisé sur IBM Z peuvent réduire le temps de traitement de jusqu'à 91,7 %. » - extrait du rapport de recherche Solitaire « Pervasive Encryption - A New Paradigm for Protection », page 22, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

14 (2) « Les innovations dans la pile logicielle, de leur côté, s'appuient sur ces fonctions de chiffrement pour permettre aux organisations de protéger les données d'entreprise et client contre les menaces internes et externes, sans besoin de modifications d'application, et sans affecter les accords de niveau de service. » - extrait de l'IBM Journal of Research & Development R&D Volume 62 No 2/3 Paper 2 « Enabling pervasive encryption through IBM Z stack innovations », page 2, URL : https://ieeexplore.ieee.org/document/8270590/

15 Corroboration : « L'architecture mainframe IBM permet de réaliser le chiffrement jusqu'à 18,4 fois plus vite, pour seulement 5 % du coût des solutions d'autres plates-formes » et « Les mêmes activités standard sur Z prennent jusqu'à 85,80 % de temps en moins que celles effectuées sur d'autres plates-formes », extraits du rapport de recherche Solitaire « Pervasive Encryption, the New Paradigm for Protection », page 28 sur https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03452USEN&

16 « Les innovations dans la pile logicielle, de leur côté, s'appuient sur ces fonctions de chiffrement pour permettre aux organisations de protéger les données d'entreprise et client contre les menaces internes et externes, sans besoin de modifications d'application, et sans affecter les accords de niveau de service. » - extrait de l'IBM Journal of Research & Development R&D Volume 62 No 2/3 Paper 2 « Enabling pervasive encryption through IBM Z stack innovations », page 2, URL : https://ieeexplore.ieee.org/document/8270590/

IBM United Kingdom Limited
PO Box 41, North Harbour
Portsmouth, Hampshire PO6 3AU
Royaume-Uni

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland est enregistrée en Irlande sous le numéro de société 16226

65019165-FRFR-00