La cyberéthique non-existante de Meta

Raphael Nga Beauregard

François-Xavier Leclerc

Sanders Bernavil

Robin Boucher

Groupe #3

Présenté à

Mohamed Rida Allah

Éthique en Cybersécurité

Septembre 2024

College Cumberland

Montreal, QC

Table des matières

Lorsqu'on parle d'un sujet aussi important que la cyberéthique, il est facile d'assumer que les entreprises la respectent dû à leurs missions professionnelles ou tout simplement dû aux lois en place. Malheureusement, beaucoup d'entreprises de nos jours exercent le contraire et font l'effort de voler l'information personnelle de leurs clients à des fins de profits. Le cas le plus majeur de ce crime est la société Meta, créatrice de Facebook, Instagram et WhatsApp. Étant l'une des plus grandes compagnies du monde, Meta prend avantage de son pouvoir et ignore une grande majorité des morales et conceptions présentes dans la cyberéthique. Il y a tellement de façons dont Meta ne respecte pas la vie privée des ses utilisateurs qu'un seul document ne pourrait pas en rendre justice.

Pourquoi Meta?

1. Nous avons choisi Meta qui regroupe plusieurs plateformes dont Facebook, Instagram, WhatsApp, Messenger en plus de quelques autres. Cette entreprise regroupe des plateformes qui sont très présentes dans notre quotidien il serait donc intéressant d'en connaître davantage sur son éthique en cybersécurité.

2. Alors, la politique de cybersécurité de Meta, malgré des prétentions ambitieuses, semble souvent plus une vitrine qu'une véritable protection. Le chiffrement et les contrôles d'accès sont régulièrement mis en question par des incidents récurrents, comme les fuites de données que Facebook a subi à partir de 2014, un siphonage de données de 87 millions d'utilisateurs via la société Cambridge Analytica à des fins de manipulation électorale (source: Serge Escalé). Nous pouvons voir que l'éthique est souvent une façade, avec une transparence limitée et une conformité aux régulations qui semble plus axée sur la gestion de la réputation que sur un réel engagement envers la protection de la vie privée des utilisateurs.

3. En 2022, Meta a souffert 1.4 milliards de dollars dans un procès lié à la collecte illégale de données biométriques de ses usagers. (Source: Reuters) La compagnie a en effet capturé des milliards de données de reconnaissance faciale sans le consentement de plusieurs millions de personnes habitant au Texas, ce qui est illégal selon une loi signée par l'État en 2009. Cette loi exige que toute compagnie informe ses usagers de quelconque collecte de données biométriques à des fins commerciales. (Source: Hyperproof.io). Les données étaient collectées à partir de photos et de vidéos partagées sur les médias sociaux afin de suggérer de «taguer» des personnes automatiquement sur les publications. Cet incident démontre le refus catégorique de la compagnie de prendre au sérieux la vie privée de ces usagers; ce n'est pas la première fois, et certainement pas la dernière que Meta viole l'intimité de ses utilisateurs. Un porte-parole de la compagnie a affirmé «nous explorons les opportunités futures afin de renforcer nos investissements financiers au Texas, incluant potentiellement le développement de centres de recherche» (Source: Reuters), démontrant l'hypocrisie et le manque de prise de responsabilité de Meta dans cette affaire. Toute personne devrait avoir le droit et la possibilité d'opter hors d'une telle fonctionnalité, mais ce n'est malheureusement pas toujours le cas.

4. Les risques potentiels liés aux renseignements personnels dans l'environnement numérique de Meta sont spécifiques à sa nature et à ses opérations. Les principaux risques que nous pouvons constater sont la compromission des données personnelles par des cyberattaques, la collecte excessive de données, la mauvaise gestion des permissions, la vulnérabilité dans les systèmes de sécurité informatique, etc. Les stratégies pour les atténuer sont le renforcement des mesures de sécurité, une gestion rigoureuse des permissions et des accès, une formation et sensibilisation auprès des employés, etc.

5. Pour protéger les renseignements personnels, l'entreprise peut mettre en œuvre des stratégies telles que le chiffrement avancé des données, des contrôles d'accès rigoureux, et des formations continues en cybersécurité pour ses employés. Bien sûr, ces pratiques sont essentielles pour la protection des renseignements personnels, par contre, Meta a certainement un retard considérable et une confiance à retrouver. Pour pouvoir se rattraper Meta a la nécessité de mettre en place un protocole rigoureux car c'est une obligation éthique envers ses utilisateurs.

Les dangers d'une fuite sur le DarkWeb

6. Considérant les montagnes d'informations que Meta collecte de ses utilisateurs grâce à leurs espions numériques placés dans des millions de site web (Vox's Sara Morrison), une fuite d'information des serveurs de Meta seraient sans doute l'échappe d'information la plus grande de l'histoire de l'Internet. Ce serait les noms, les adresses, les numéros de téléphones, les mots de passe et les informations de paiements, grâce au service Meta Pay, de milliards d'utilisateurs. Même si on exclut les espions que Meta utilise sur des sites tertiaires, les services de Meta, tels que Instagram et WhatsApp, cumulent eux-même des milliards d'utilisateurs partout dans le monde. Le danger potentiel d'une échappée sur le darkweb est très grand, et c'est pourquoi Meta investit grandement dans le domaine de la cybersécurité (Meta's Michel Protti) et même la vie privée, quoique ça reste à désirer pour le moment considérant que leurs espions numériques sont encore actuellement actifs. Instagram et Facebook, deux médias sociaux faisant partie de l'entreprise, collectent chacun des données de reconnaissance faciale, vocale, de langue, d'environnement et de produits, ainsi que vos images et tous vos contacts. (Source: Clario)

7. Explorons maintenant la possibilité que les renseignements collectés par Meta soient compromis sur le «dark web», quelles seraient les conséquences? L'entreprise assure à ses utilisateurs que ces

données sont privées, cependant il a été prouvé à plusieurs reprises qu'elles peuvent être vendues ou volées. C'est tout de même un énorme risque de sécurité, car si des pirates informatiques malicieux obtiennent l'accès à toutes ces données sur le dark web, il leur serait possible de frauder, grâce aux informations de paiements disponibles sur Meta Pay, ou encore de cibler des usagers plus efficacement dans des arnaques. Avec toutes les informations personnelles et les renseignements de produits utilisés par ses usagers, il serait facilement possible de se présenter en tant que Facebook, ou n'importe quelle autre compagnie dans un courriel. Cela pourrait permettre d'introduire des virus sur les appareils de quiconque à partir d'un lien malveillant, ou encore de faire croire qu'on a manqué un paiement d'une compagnie et qu'il faut payer un frais exorbitant. Avec les arnaques, il suffit d'être créatif.

8. Pour se protéger contre les menaces du Darkweb, Meta aurait intérêt à mettre en place une politique de cybersécurité très rigoureuse des systèmes de surveillance avancés pour détecter les activités suspectes et les fuites de données sur le Darkweb (BA_INFO). Il lui faudrait aussi développer des protocoles de chiffrement robuste pour la protection des données, limiter l'accès aux données sensibles par un contrôle d'accès et former des employés sur les meilleures pratiques en matière de sécurité. Ensuite, lors d'une violation de données, il est primordial d'avoir un plan de réponse efficace pour traiter l'incident. Pour s'assurer que Meta est bien protégé contre les menaces du Darkweb, il lui faudra constamment mettre à jour des protocoles de défenses contre les nouvelles vulnérabilités.

9. Il faudra faire bien attention à tester le nouveau système de sécurité de façon poussée afin qu'une brèche de données sur le Darkweb ne se reproduise pas une deuxième fois. L'enjeu éthique le plus

important ici sera de protéger la vie privée de nos clients au meilleur de notre habilité, sinon la compagnie pourrait en souffrir.

10. Pour que Meta intègre l'éthique en cybersécurité dans ses politiques et pratique pour se protéger contre les menaces du Darkweb, il lui faut tout d'abord définir des principes éthiques clairs sur la confidentialité, la sécurité des données, la transparence et la communication avec les utilisateurs. Il est important d'avoir une surveillance éthique constante. C'est-à- dire, utiliser les outils et technologies pour surveiller les activités suspectes en respectant les droits des utilisateurs et en évitant la surveillance excessive. Finalement, il est important pour Meta de faire des révisions en continu des mises à jours possibles des politiques et des pratiques en fonction des évolutions technologiques et des nouvelles menaces.

En dernier lieu, Meta est argumentativement l'entreprise la plus puissante du monde grâce à l'information auquel elle a accès, mais cela la rend aussi la compagnie la plus lucrative pour les pirates informatiques. Bien que Meta fait des efforts pour protéger les informations personnelles que ses espions obtiennent, l'information est toujours et sera toujours à risque. La meilleure option en termes de sécurité sera toujours l'abstinence de collecter autant d'informations non nécessaires au service demandé par un utilisateur, mais considérant l'histoire de vie privée de Meta, le future semble sombre…

Bibliographie

Sara, Morrison. « Le Pixel de Meta envoie discrètement des informations sensibles des sites web d'hôpitaux à Facebook ». *Vox*, 16 juin 2022, www.vox.com/recode/23172691/meta-tracking-privacy-hospitals. Consulté le 9 septembre 2024.

Protti, Michel (Meta). « Investir dans la protection de la vie privée ». *About Facebook*, 19 janvier 2024, about.fb.com/news/2024/01/investing-in-privacy/. Consulté le 9 septembre 2024.

Reuters. « Meta Platforms paiera 1,4 milliard de dollars pour régler un procès au Texas concernant les données de reconnaissance faciale ». *Reuters*, 30 juillet 2024, www.reuters.com/technology/cybersecurity/meta-platforms-pay-14-bln-settle-texas-lawsuit-over-facial-recognition-data-2024-07-30/. Consulté le 9 septembre 2024.

Clario. « Which Companies Collect the Most Data? » *Clario*, 2024, www.clario.co/blog/which-company-uses-most-data/. Consulté le 9 septembre 2024.

Hyperproof. « Texas Biometric Privacy Law: What You Need to Know ». *Hyperproof*, 2024, hyperproof.io/texas-biometric-privacy-law/#:~=Since%202009%2C%20Texas%20has%20had,consented%20to%20such%20data%20collection. Consulté le 9 septembre 2024.

Meta. « Meta Pay : Simplifier les paiements en ligne ». *Meta*, 2024, about.meta.com/technologies/meta-pay/. Consulté le 9 septembre 2024.

Serge Escalé. « Les enjeux de cybersécurité du Métavers de Meta (ex-Facebook) » 28 mars 2022 https://itsocial.fr/contenus/articles-decideurs/les-enjeux-de-cybersecurite-du-metavers-facebook/ Consulté le 10 septembre 2024.

Remunzo. « La violation des données de Facebook expliquée » https://remunzo.com/fr/facebook-fuite-de-donnees/ Consulté le 10 septembre 2024.

BA_INFO. « Le Dark Web : comment protéger votre entreprise de cette menace grandissante ? » 17 octobre 2023

https://www.ba-info.fr/le-dark-web-comment-proteger-votre-entreprise-de-cette-menace-grandissante/

consulté le 10 septembre 2024