Données biométriques : des risques de sécurité

Rien de ce qui constitue notre vie numérique n'est totalement dépourvu de failles, pas une semaine ne se passe sans qu'un piratage massif ne soit révélé. C'est par millions que nos données d'internautes sont exposées, y compris et peut-être surtout quand nous les confions plus ou moins aveuglément aux grandes entreprises du numérique.

Quelques exemples parmi tant d'autres : les iPhones, Facebook, Yves Rocher, Option Way, la Gendarmerie…

Dans la course jamais gagnée à la sécurité, les mots de passe sont notoirement fragiles, de sorte que les entreprises passent désormais au stade supérieur et cherchent à utiliser nos données biométriques.

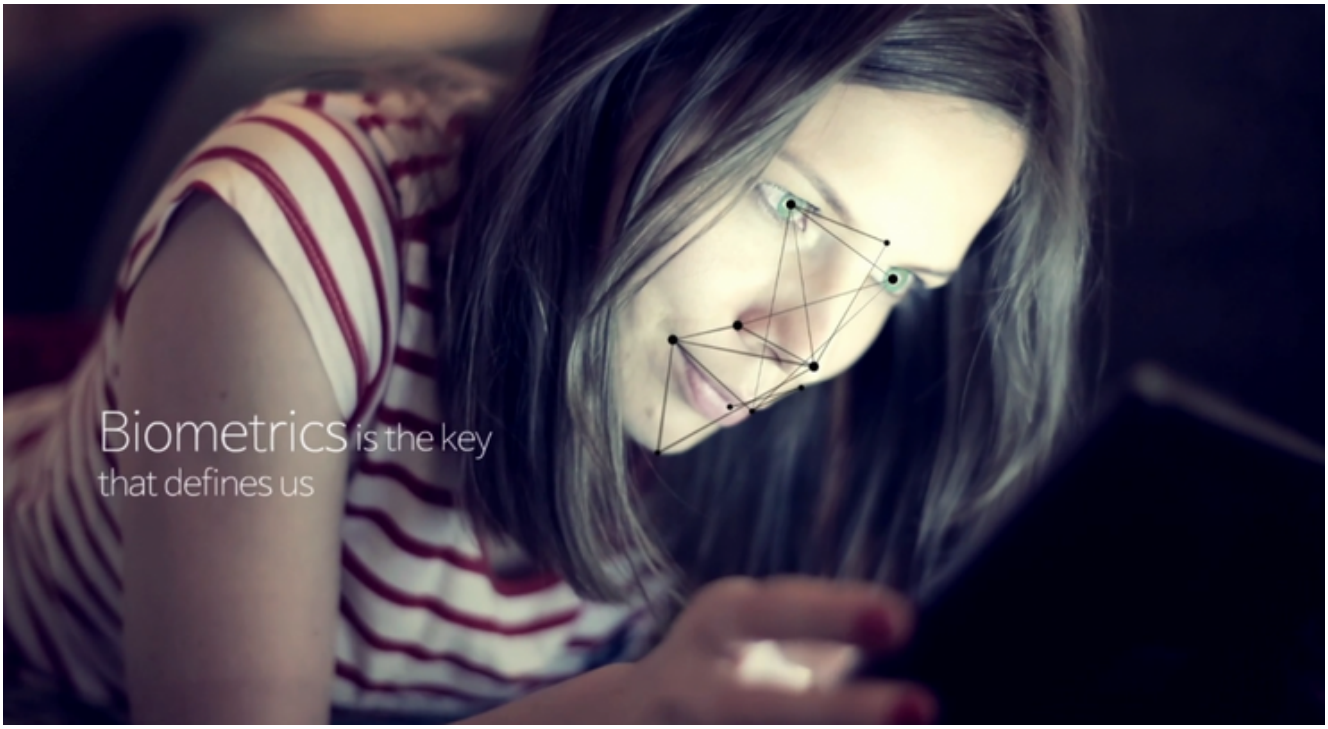
Cependant, comme le souligne Glyn Moody dans l'article ci-dessous, si l'on peut changer un mot de passe piraté, il est impossible de changer des données biométriques compromises…

Source : A major security breach raises a key question: what happens when your biometric data is exfiltrated from a system?

Traduction Framalang : goofy, Penguin, Fabrice, FranBAG, Mannik

Une importante faille de sécurité soulève une question clef : que se passe-t-il lorsque vos données biométriques ont fuité d'un système ?

par Glyn Moody



« Les données biométriques nous définissent » – Image provenant de Suprema.

Ce n'est pas un secret, la sécurité des mots de passe est souvent déplorable. Les bons mots de passe, ceux qui sont longs et qui mélangent minuscules, majuscules, chiffres et caractères spéciaux, sont difficiles à se mémoriser, à moins d'utiliser un gestionnaire de mots de passe, ce que peu de gens semblent faire. Résultat, les gens ont tendance à choisir des mots de passe faciles à se rappeler, tels que des noms ou des dates de naissance ou encore des absurdités comme « motdepasse » et « 1234 ». Les tentatives pour détourner les personnes de tels mots de passe restent vaines, et en conséquence de nombreuses entreprises et organisations essayent de régler le problème en se débarrassant totalement des mots de passe. L'alternative, utiliser les techniques biométriques telles que la lecture des empreintes digitales, de l'iris et la reconnaissance faciale, est arrivée à maturité et est de plus en plus utilisée. Une des principales sociétés de développement de contrôles d'accès par biométrie s'appelle Suprema :

> *La gamme étendue de produits Suprema comprend des systèmes de contrôle d'accès biométriques, des solutions de temps et de présence, des lecteurs d'empreintes digitales, des solutions d'authentification mobiles et des modules d'empreintes digitales embarqués. Suprema a consolidé son statut de marque mondiale de premier ordre dans le secteur de la sécurité physique et possède un réseau mondial de ventes dans plus de 130 pays. Suprema se classe en première place concernant les parts de marché dans la région EMEA*[1] *et a été*

> *nommée parmi les 50 principaux fabricants mondiaux dans le secteur de la sécurité.*

D'après le site web de la société, 1,5 million de leurs systèmes sont installés dans le monde, utilisés par plus d'un milliard de personnes. Au vu de la position de Suprema dans ce secteur, une information concernant une fuite de données à grande échelle dans leur principal produit, BioStar 2, est particulièrement préoccupante : « *Lors d'un test la semaine dernière, les chercheurs ont trouvé que la base de données de Biostar 2 n'était pas protégée et en grande partie non-chiffrée. Ils ont été capables d'effectuer des recherches dans la base de données en manipulant le critère de recherche URL dans Elasticsearch pour accéder aux données.* » Un message sur la page d'accueil de Suprema indique : « *cet incident concerne un nombre limité d'utilisateurs de l'API BioStar 2 Cloud. La grande majorité des clients de Suprema n'utilise pas l'API BioStar 2 Cloud comme solution de contrôle d'accès et de gestion de temps et de présence.* » C'est peut-être vrai, mais les déclarations des chercheurs à propos de ce qui a été découvert sont inquiétantes à lire :

> *Notre équipe a été capable d'accéder à plus de 27,8 millions d'enregistrements pour un total de 23Go de données, qui incluent les informations suivantes :*
>
> - *Accès aux panneaux, tableau de bord, contrôles back office et permissions des administrateurs clients*
> - *Données des empreintes digitales*
> - *Informations de reconnaissance faciale et images d'utilisateurs*
> - *Noms, identifiants et mots de passe d'utilisateurs non chiffrés*
> - *Enregistrements des entrées et des sorties de zones sécurisées*
> - *Fiches d'employés, incluant les dates d'entrée dans l'entreprise*
> - *Niveau de sécurité et habilitations d'employés*
> - *Détails personnels, dont l'adresse du domicile et de messagerie privée d'employés*
> - *Structures et hiérarchies des fonctions dans l'entreprise*
> - *Terminaux mobiles et informations sur les systèmes d'exploitation*

Le fait que des mots de passe, y compris ceux de comptes disposant de droits administrateurs, aient été enregistrés par une entreprise de sécurité sans être chiffrés est incroyable. Comme le signalent les chercheurs, tous ceux qui ont

trouvé cette base de données pouvaient utiliser ces mots de passe administrateurs pour prendre le contrôle de comptes BioStar 2 de haut niveau avec toutes les permissions et habilitations complètes des utilisateurs, et modifier les paramètres de sécurité d'un réseau entier. Ils pouvaient créer de nouveaux comptes, les compléter avec des empreintes digitales et scans faciaux ainsi que se donner eux-mêmes accès à des zones sécurisées à l'intérieur de bâtiments. De même, ils pouvaient changer les empreintes digitales de comptes possédant des habilitations de sécurité afin d'octroyer à n'importe qui la possibilité d'entrer dans ces zones.

Comme le compte administrateur contrôle les enregistrements d'activité, des criminels pouvaient supprimer ou modifier les données afin de masquer leurs opérations. En d'autres termes, accéder à de tels mots de passe permet à n'importe qui d'entrer dans n'importe quelle partie d'un bâtiment considéré comme sécurisé et ce de manière invisible, sans laisser aucune trace de leur présence. Cela permettrait le vol d'objets précieux conservés dans les locaux. Plus sérieusement, peut-être, cela permettrait un accès physique aux services informatiques, de manière à faciliter l'accès futur aux réseaux et données sensibles.

Le problème ne s'arrête pas là. La liste des informations hautement personnelles, telles que les fiches d'emploi, adresses de messagerie et de domicile visibles dans la base de données, pourrait faire courir un véritable risque de vol d'identité et d'hameçonnage. Ça permet aussi l'identification du personnel clé des entreprises utilisant le système BioStar 2. Cela pourrait les rendre plus vulnérables aux menaces de chantage par des criminels. Mais peut-être que le problème le plus sérieux est celui-ci, relevé par les chercheurs :

> *L'utilisation de sécurité biométrique comme les empreintes digitales est récente. Ainsi, la véritable portée du risque de vol d'empreintes digitales est encore inconnue.*

> *Toutefois, il est important de se rappeler qu'une fois volées, vos empreintes digitales ne peuvent pas être changées, contrairement aux mots de passe.*
>
> *Cela rend le vol des données d'empreintes digitales encore plus préoccupant. Elles ont remplacé les mots de passe alphanumériques dans de nombreux*

> *objets de consommation, tels que les téléphones. La plupart de leurs lecteurs d'empreintes digitales ne sont pas chiffrés, ainsi lorsqu'un hacker développera une technologie pour reproduire vos empreintes, il obtiendra l'accès à toutes vos informations personnelles telles que les messages, photos et moyens de paiement stockés sur votre appareil.*

D'après les chercheurs qui ont découvert cette base de données vulnérable, au lieu de stocker un *hash* de l'empreinte digitale – une version mathématiquement brouillée qui ne peut pas faire l'objet de rétro-ingénierie – Suprema a enregistré la version numérique des véritables empreintes des personnes, laquelle peut donc être copiée et directement utilisée pour dans un but malveillant. Il existe déjà de nombreuses méthodes pour créer de fausses empreintes d'assez bonne qualité pour berner les systèmes biométriques. Si les données de l'empreinte complète sont disponibles, de telles contrefaçons ont de bonnes chances de mettre en échec même la meilleure sécurité biométrique.

La possibilité d'une fuite d'autant d'empreintes digitales dans le cas du système BioStar 2 rend la réponse à la question « que se passe-t-il lorsque quelqu'un a une copie de vos données biométriques ? » encore plus cruciale. Comme des personnes le signalent depuis des années, vous ne pouvez pas changer vos caractéristiques biométriques, à moins d'une chirurgie. Ou, comme le dit Suprema sur son site web : « **La biométrie est ce qui nous définit.** »

Étant donné ce point essentiel, immuable, **il est peut-être temps de demander que la biométrie ne soit utilisée qu'en cas d'absolue nécessité uniquement, et non de manière systématique.** Et si elle est utilisée, elle doit obligatoirement être protégée – par la loi – avec le plus haut niveau de sécurité disponible. En attendant, les mots de passe, et pas la biométrie, devraient être utilisés dans la plupart des situations nécessitant un contrôle d'accès préalable. Au moins, ils peuvent être changés en cas de compromission de la base de données où ils sont conservés. Et au lieu de pousser les gens à choisir et se rappeler de meilleurs mots de passe, ce qui est un vœu pieux, nous devrions plutôt les aider à installer et utiliser un gestionnaire de mots de passe.

À propos de Glyn Moody

Glyn Moody est un journaliste indépendant qui écrit et parle de la protection de la vie privée, de la surveillance, des droits numériques, de l'*open source*, des droits d'auteurs, des brevets et des questions de politique générale impliquant les technologies du numérique. Il a commencé à traiter l'usage commercial d'Internet en 1994 et écrivit le premier article grand public sur Linux, qui parait dans Wired en août 1997. Son livre, *Rebel Code*, est la première et seule histoire détaillée de l'avènement de l'*open source*, tandis que son travail ultérieur, *The Digital Code of Life*, explore la bio-informatique, c'est-à-dire l'intersection de l'informatique et de la génomique.