L'authentification biométrique plus sûre grâce à l'identité numérique

Depuis quelques années, l'usage de la biométrie se démocratise. De nombreux projets ont en effet été lancés par certaines entreprises issues de différents secteurs d'activités. Parmi elles, Google a annoncé récemment de nouveaux outils pour renforcer l'authentification biométrique, les aéroports de Roissy et d'Orly viennent d'adopter la reconnaissance faciale ou encore la Société Générale, un peu plus tôt cette année, a lancé un système d'identification des clients par biométrie faciale. La biométrie est une technologie puissante et prometteuse, si elle est combinée à l'identité numérique.

La facilité et la dimension pratique de l'utilisation de la biométrie, pour déverrouiller un appareil mobile ou pour accéder à une application par exemple, semblent avoir séduit le consommateur "digital" d'aujourd'hui, et les fabricants en ont clairement conscience. La quasi-totalité des mobiles disponibles sur le marché sont en effet équipés d'une technologie biométrique, que ce soit un enregistreur de voix, un système de reconnaissance faciale ou encore un scanner d'empreintes digitales.

De manière générale, la biométrie se définit par sa fonction de reconnaissance de l'identité d'un individu, sur la base de ce qu'il est, et non de ce qu'il possède. Mais elle n'est pas infaillible, et les échecs peuvent conduire à des fraudes, des frictions ou encore à des frustrations chez les utilisateurs. Un réel problème, surtout quand on sait que 10 secondes de frictions en ligne suffisent à les convaincre de se tourner vers un concurrent. Pour les organisations du secteur financier par exemple, cela se traduit par une baisse d'au moins 4 % des ventes et du volume global des transactions.

Lorsque la reconnaissance biométrique échoue, la solution de repli classique consiste à revenir à l'utilisation d'un mot de passe ou d'un code en tant que condition préalable à la connexion. Le problème est que, via des violations de données, les fraudeurs ont bien souvent la possibilité d'accéder à ces informations sur le Dark Web. Plus difficile mais pas impossible, il arrive également qu'ils parviennent à associer leurs propres données biométriques à un compte dont ils détiennent les identifiants suite à une attaque, et se connectent alors à la place de l'utilisateur légitime.

Les attaques de prise de contrôle de comptes représentent l'une des menaces les plus inquiétantes pour les entreprises. Si la biométrie a pour but de sécuriser les accès, elle n'a toutefois pas été conçue pour identifier les applications ou les dispositifs compromis, ni pour détecter lorsqu'un utilisateur authentifié devient vulnérable au piratage ou à l'espionnage. Tout comme elle n'est pas capable de reconnaître un logiciel espion ou de stopper une attaque de type "Man-in-the-Middle" - c'est-à-dire une tentative d'interception de communication entre deux systèmes. C'est pourquoi il est pertinent d'allier les technologies biométriques à l'analyse de l'identité numérique qui permet de repérer les menaces, une capacité vitale pour les organisations mais bien souvent négligée. Cette combinaison offre alors une authentification dite "dynamique", basée sur les risques, qui prend en compte un ensemble de caractéristiques contextuelles, notamment liées au comportement de l'utilisateur et de son appareil.

La biométrie protège l'accès à des comptes ou bien à des appareils, mais peut se montrer vulnérable face aux techniques toujours plus sophistiquées des fraudeurs. Pour aller plus loin dans la sécurisation de l'authentification, les entreprises ont tout intérêt à considérer l'identité numérique.

Elles pourront dès lors tirer le meilleur parti de la fonction première de la biométrie : une technologie efficace qui intervient dans le cadre d'une méthode sophistiquée d'authentification, et contribue à la fois à générer une croissance rentable pour les entreprises et à offrir une expérience digitale de qualité pour les utilisateurs.