Lutter efficacement contre le **Phishing** : L'insuffisance de **l'authentification** multifacteur

Ces dernières années, le phishing a évolué d'emails grossiers à des attaques sophistiquées combinant intelligence artificielle et automatisation pour créer des messages crédibles et personnalisés. Une réalité qui exige non seulement des mesures de sécurité plus avancées mais également une approche plus globale de la problématique, à l'instar des solutions proposées par Eviden

Courriels, SMS, réseaux sociaux… « *En 2023 l'hameçonnage représentait plus de 21% des cyberattaques en France selon le Rapport annuel de Cybermalveillance.gouv.fr* », rappelle **Yann Vincent, Vice President, Global Head of Cybersecurity Products business line d'Eviden**. Les entreprises sont ciblées mais les individus aussi : vous avez certainement reçu un jour ou l'autre des messages vous demandant de saisir vos coordonnées bancaires pour un second passage du livreur qui vous aurait raté la première fois ou qui vous invitent à corriger votre profil sur le site prétendument d'Ameli, voire à payer une contravention en retard sur de prétendues pages du gouvernement.

Menace persistante ayant atteint un niveau record en 2023, le phishing est malheureusement là pour rester avec des attaques toujours plus sophistiquées et dangereuses que même un œil averti risque d'avoir du mal à détecter.

Phishing : une menace persistante et sophistiquée

Véritable fléau du monde numérique, le phishing se limitait à ses débuts à des emails grossièrement imités. Aujourd'hui, il se décline sous de multiples formes : courriels, SMS, messages sur les réseaux sociaux, tous conçus pour tromper les utilisateurs.

YANN VINCENT

Vice President, Global Head of Cybersecurity Products business line, Eviden

SIMON ULMER

Global VP Digital Identity, Eviden

L'objectif reste le même : vous inciter à révéler vos identifiants (personnels et plus encore professionnels), mots de passe ou données bancaires. Ainsi, 90% des attaques contre les entreprises débutent par un email de phishing. Et, depuis l'arrivée de ChatGPT, le phishing aurait connu une progression de 1 265%, les cyberattaquants utilisant cette IA pour varier et parfaire leurs messages dans une multitude de langues.

De fait, les attaques sont de plus en plus sophistiquées. Les pirates ont élaboré de nouvelles techniques pour contrer les protections, y compris celles 2FA (double authentification) pourtant censées renforcer la sécurité de vos comptes. Ainsi, l'évolution la plus inquiétante exploite la technique de « l'attaquant du milieu » (ou AiTM pour Attacker in the Middle). En piratant un réseau Wi-Fi, un serveur de messagerie ou des équipements réseau, les cybercriminels peuvent intercepter les échanges et usurper les protocoles de sécurité, rendant inefficients bien des systèmes d'authentification.

La nécessité de technologies résilientes by design plutôt que la MFA

Face à ces menaces de plus en plus élaborées, la vigilance de chacun est plus que jamais cruciale d'autant que les anciennes méthodes de protection s'avèrent insuffisantes.

Même l'authentification multifacteur (MFA), ne présente plus un rempart fiable contre des attaques d'un niveau bien plus élevé que dans le passé

La lutte contre le phishing nécessite désormais une approche globale qui combine une sensibilisation accrue des utilisateurs à des systèmes de sécurité plus intelligents.

« *Aujourd'hui, aidé par l'IA et l'automatisation des attaques, le phishing atteint un niveau quasi industriel. Une technologie résistante by design est donc nécessaire pour protéger l'employé et son environnement professionnel. L'authentification par certificat (Certificate Based Authentication) est le moyen parfait pour se prémunir efficacement contre ce type d'attaques* », confirme **Simon Ulmer**, **Global VP Digital Identity d'Eviden**.

En 2023 l'hameçonnage représentait plus de 21% des cyberattaques en France. Conscients des risques encourus par les entreprises, nos solutions de cybersécurité adressent particulièrement cette menace.

Les deux méthodes d'authentification forte les plus robustes s'appuient sur le principe des signatures numériques et sont d'un côté FIDO (Fast IDentity Online) et de l'autre la PKI (Public Key Infrastructure).

FIDO se concentre sur la simplification de l'authentification de l'utilisateur avec un niveau de sécurité élevé, alors que la PKI garantit sans effort supplémentaire en outre la confidentialité et l'intégrité des informations sensibles (voir encadré).

Authentification par certificat

Méthode qui utilise des certificats numériques pour vérifier l'identité d'un utilisateur ou d'un appareil, l'authentification par certificat s'appuie sur une clé publique et des informations d'identité, signées par une autorité de certification (AC) de confiance. Lors de la connexion, le système vérifie la validité du certificat et utilise la cryptographie à clé publique pour authentifier le détenteur du certificat, offrant ainsi un niveau de sécurité supérieur aux méthodes basées uniquement sur les mots de passe.

Reposant sur cette technologie éprouvée qui assure une protection robuste contre le phishing, l'offre d'Eviden va au-delà comme l'explique **Yann Vincent** : « *Nous proposons une offre globale allant de la génération de clés cryptographiques dans des boitiers sécurisés, de la gestion des identités numériques de confiance avec nos solutions PKI (sur site ou en SaaS) et jusqu'à leur utilisation à travers nos applications d'IAM (Identity and Access Management)* ».

En pratique, l'offre d'Eviden se caractérise par quatre principaux atouts qui en font à la fois une solution efficace, économique, flexible et simple à mettre en œuvre :

1. **L'authentification par certificats électroniques**, en utilisant l'authentification basée sur des signatures numériques. Une clé privée, protégée par un facteur supplémentaire comme un PIN ou une biométrie, est utilisée pour créer une signature numérique. Cette méthode garantit qu'aucune information secrète n'est transmise sur le réseau, rendant les attaques de phishing inefficaces.
2. **Une infrastructure à clés publiques** (ou PKI, Public Key Infrastructure) disponible en mode licence ou en mode « as a service » à base d'un cloud souverain et accessible sous forme d'abonnement. Cette formule présente l'avantage de réduire les coûts initiaux et opérationnels, tout en offrant une gestion simplifiée et automatisée des certificats, de leur émission à leur renouvellement. De plus, elle affranchit l'entreprise d'une mise en œuvre en interne parfois complexe qui freine beaucoup d'organisations, surtout quand elles ne disposent pas des compétences nécessaires.
3. **Des cartes à puce physiques et virtuelles :** Les cartes à puce d'Eviden permettent non seulement de gérer des clés cryptographiques et les certificats associés, mais peuvent également embarquer des applications FIDO pour un maximum de flexibilité.

CERTIFICATE BASED AUTHENTICATION	FIDO
Sans mot de passe	Sans mot de passe
Nécessite une infrastructure à clé publique	Nécessite de générer et de stocker des paires de clés distinctes pour chaque partie se fiant au système.
Les certificats garantissent l'authenticité, la confidentialité, l'intégrité et la non-répudiation	Gère uniquement l'authentification
Pris en charge par les systèmes d'exploitation, les navigateurs et les applications.	Pris en charge par les systèmes d'exploitation, les navigateurs et les applications.
Peuvent être gérés de manière centralisée (émission, renouvellement, révocation)	Ne peut être géré de manière centralisée
Peuvent être stockés dans des dispositifs cryptographiques divers	Existe sous différents facteurs de forme
Gestion des clés, y compris séquestre et recouvrement	Pas de gestion des clés

Afin d'offrir une solution flexible et économique en évitant aux entreprises l'investissement dans des cartes à puce physiques, Eviden supporte également les cartes à puce virtuelles s'appuyant sur ce standard du marché pour stocker les clés privées de manière sécurisée dans un module TPM (Trusted Platform Module). Intégré à de nombreux ordinateurs et appareils modernes, le TPM se concrétise par une puce cryptographique capable de générer et stocker des clés cryptographiques, de chiffrer et déchiffrer des données, de créer et de vérifier des signatures numériques et, enfin, d'attester de l'intégrité du système. Dès lors, il joue un rôle crucial dans la protection contre certaines formes d'attaques.

4. **Signature S/MIME pour les emails :** standard pour le chiffrement et la signature des emails, S/MIME assure l'authentification de l'expéditeur, garantit l'intégrité du message ainsi que la non-répudiation. Largement supporté par les clients de messagerie modernes et couramment utilisé dans les environnements professionnels nécessitant un haut niveau de sécurité, S/MIME permet de prouver que les messages proviennent bien de l'expéditeur déclaré et qu'ils n'ont pas été altérés en transit, deux facteurs essentiels pour lutter efficacement contre les formes les plus évoluées de phishing. L'offre Eviden inclut également des solutions de chiffrement « bout-en-bout » hautement sécurisées.

Les avantages d'une Infrastructure à Clé Publique (PKI) vis-à-vis de la MFA

Au-delà des technologies de protection, les entreprises ont désormais besoin de s'appuyer sur des plateformes qui englobent plus largement les multiples défis cyber liés à l'authentification des personnes et des machines.

Centrée sur son infrastructure à clé publique (PKI), l'offre d'Eviden va bien au-delà de la simple protection contre le phishing. Elle constitue une plateforme de sécurité complète et évolutive, offrant des avantages considérables pour les entreprises modernes :

1. **Sécurité renforcée :** La PKI fournit une base solide pour l'authentification forte, le chiffrement des données et la signature électronique, protégeant contre un large éventail de cybermenaces.
2. **Gestion centralisée des identités :** Elle permet une administration simplifiée des certificats numériques non seulement pour tous les utilisateurs mais également pour tous les appareils et services de l'entreprise.
3. **Conformité réglementaire :** L'utilisation de certificats numériques aide à répondre aux exigences de nombreuses réglementations en matière de protection des données et de confidentialité.
4. **Flexibilité et évolutivité :** La solution s'adapte facilement à la croissance de l'entreprise et à l'évolution des besoins en sécurité.

Une technologie résistante by design au Phishing est nécessaire pour protéger l'employé et son environnement professionnel. L'authentification par certificat est le moyen parfait pour se prémunir efficacement contre ce type d'attaques.

5. **Interopérabilité :** Les standards ouverts utilisés par la PKI assurent une compatibilité avec une large gamme de systèmes, clouds et applications.
6. **Sécurisation des communications :** Elle permet de mettre en place des connexions sécurisées pour le travail à distance et les échanges avec les partenaires commerciaux.
7. **Protection des objets connectés :** La PKI peut sécuriser l'Internet des Objets (IoT) en authentifiant et chiffrant les communications des appareils.
8. **Signature électronique :** Elle facilite la mise en place de processus de signature électronique légalement valides, accélérant les transactions commerciales.

Dit autrement, en choisissant l'offre d'Eviden, les entreprises acquièrent non seulement une protection robuste contre les menaces actuelles, mais aussi une infrastructure de sécurité flexible et pérenne, capable de s'adapter aux défis futurs du monde numérique.