



Meilleures pratiques de l'authentification: mettre le contrôle à sa place

LIVRE BLANC

Avantages d'un environnement d'authentification totalement fiable :

- Permet au client de créer son propre token de données et de conserver une maîtrise totale sur ses données et politiques de sécurité
- Procure des niveaux supplémentaires de protection par le biais du chiffrement du token de données et grâce à sa capacité à stocker et à gérer les clés dans le matériel
- Permet de faire face à différents niveaux de danger du côté utilisateur et de répondre aux besoins de l'utilisateur grâce à un choix d'authentification tel que : l'authentification par certificat, l'authentification par mot de passe à usage unique (OTP), l'authentification mobile et l'accès sécurisé aux applications SaaS
- Amélioration de la gestion et la visibilité grâce à la centralisation et à la simplification de l'administration, du déploiement et de la gestion
- Reconnu sur le marché, utilisant des algorithmes standards et sans technologie propriétaire

Récemment, de nombreuses organisations victimes de nombreuses failles de sécurité très sérieuses ont fait les grands titres de la presse spécialisée. Ces événements ont eu un impact négatif sur l'image publique de ces entreprises, et peuvent également avoir un effet nocif sur leur activité. Ces incidents ont poussé les directeurs des systèmes d'information de nombreuses entreprises à revoir toute leur stratégie de sécurité de l'information tout en se concentrant particulièrement sur l'authentification de leurs utilisateurs et sur les conditions requises de sécurité des transactions.

Ces violations de la sécurité sont là pour nous rappeler que toute entreprise peut devenir la cible d'une attaque visant à dérober ses données client, financières et autres données confidentielles, ainsi que ses actifs de propriété intellectuelle. En réponse à ces menaces, l'adoption d'une approche globale et multi-niveaux de la sécurité et de l'authentification est essentielle pour garantir la protection des informations sensibles et des systèmes d'une entreprise. Ce livre blanc propose un ensemble des meilleures pratiques de l'authentification des utilisateurs.

Un "garde-barrière" pour une solution robuste de sécurité de l'information

Les solutions de sécurité doivent être gérées selon une approche multi-niveaux combinant le chiffrement, les politiques d'accès, la gestion des clés, la sécurité du contenu, et, bien sûr, l'authentification, comme n'importe quel autre composant dans le data center. Ces différents niveaux doivent être intégrés dans une structure souple permettant à l'entreprise de s'adapter aux risques auxquels elle est confrontée. Chacun de ces éléments peut être décomposé en vue de développer les meilleures pratiques lors de l'évaluation, du déploiement et de la maintenance de ces éléments au cours du cycle de vie de protection de l'information (ILP).

Une solution d'authentification qui vérifie l'identité des utilisateurs et des périphériques informatiques qui accèdent à des zones privées du réseau de l'entreprise est la première étape dans l'élaboration d'un système solide de protection de l'information. Le manque de mécanismes d'authentification appropriés peut provoquer une réaction en chaîne qui pourrait entraver l'aptitude d'une entreprise à assurer la protection de l'information pendant son cycle de vie.

Les récentes violations de sécurité ont mis en lumière les failles du processus de déploiement des solutions d'authentification. Le déploiement d'une solution d'authentification solide permet de garantir que les identités des utilisateurs dans le système sont validées à l'entrée et donc de créer un premier niveau de protection au sein d'une architecture de sécurité de l'information multi-niveaux.

Meilleures pratiques de l'authentification

Suite à ces récentes violations de sécurité, les entreprises ont entrepris un examen minutieux de leurs solutions d'authentification. Afin de mieux comprendre les risques auxquels elles sont confrontées, les entreprises sont invitées à analyser une série de facteurs liés à la stratégie informatique, aux règlements et aux normes en vigueur, au comportement des employés et au stockage des données. Une fois que les entreprises ont mis leur modèle de risque en place et qu'elles sont plus conscientes de leur vulnérabilité, elles se retrouvent dans une meilleure position pour réduire les risques de violations de leur sécurité et pour élaborer une stratégie d'authentification adaptée à leurs besoins. Cette stratégie doit être définie en fonction de leur activité et des utilisateurs qui devront s'authentifier pour accéder au système. En prenant en compte ces facteurs, le directeur des systèmes d'information peut définir une approche multi-niveaux de l'authentification qui comprend le système d'authentification de base, le cycle de vie des composants d'authentification et des solutions complémentaires.

Il est conseillé aux entreprises qui réévaluent leurs stratégies afin d'atténuer les risques pour la sécurité de l'information de passer minutieusement en revue les conseils des meilleures pratiques d'utilisation qui suivent :

Système d'authentification de base

Adaptez votre solution d'authentification à votre activité, vos utilisateurs et aux dangers

Une approche tout en souplesse permettant à une entreprise de mettre en œuvre différentes méthodes d'authentification selon différents niveaux de risque garantit l'utilisation d'un système solide dont le déploiement s'effectue de manière efficace et à moindre coût.

Les technologies d'authentification multi-facteurs comprennent :

- **Mots de passe à usage unique (OTP):** La technologie OTP est basée sur un secret partagé ou "seed" stocké sur le périphérique d'authentification et sur le système backend d'authentification. Cette méthode garantit l'authentification en générant un mot de passe à usage unique en fonction du secret du token.
- **Authentification par certificat:** Cette méthode garantit l'authentification en utilisant une clé de chiffrement publique et privée qui est exclusive au périphérique d'authentification et à la personne qui la possède. Les tokens d'authentification par certificat peuvent également être utilisés pour signer numériquement les transactions et éviter la non-répudiation.
- **Authentification selon le contexte:** L'authentification selon le contexte utilise des informations contextuelles pour vérifier si l'identité d'un utilisateur est authentique ou non. Son utilisation est conseillée en tant que supplément à d'autres technologies d'authentification forte.

Afin de développer une solide solution d'authentification, les entreprises doivent en premier lieu tenir compte de leur activité, de leurs utilisateurs et des risques potentiels puis choisir une solution qui leur offre la souplesse d'adaptation nécessaire. Par exemple, les entreprises intéressées par la mise en œuvre de solutions de sécurité supplémentaires s'appuyant sur la technologie PKI, qui offre par exemple le chiffrement intégral du disque, la connexion au réseau et les signatures numériques ou qui pense ajouter de telles solutions à l'avenir, devraient envisager l'authentification selon le contexte car celle-ci permet d'activer ces applications.

Renforcez vos solutions par mot de passe à usage unique (OTP) à l'aide d'un secret partagé de l'utilisateur

Pour l'authentification par mot de passe à usage unique, un niveau de sécurité supplémentaire peut être mis en œuvre en ajoutant un code PIN de 4 à 8 chiffres pour le mot de passe à usage unique qui est créé par le token. Le principe fondamental pour l'authentification à deux facteurs est que le code PIN du mot de passe à usage unique est «connu uniquement par vous-même». Ceci garantit que même s'il a réussi à percer le mécanisme d'authentification par token, le pirate informatique a encore besoin de connaître le code PIN de l'utilisateur pour pouvoir accéder au système.

Favorisez l'utilisation de solutions conformes aux normes et certifications de sécurité

Il est préférable d'utiliser des produits fondés sur des algorithmes de chiffrement et sur des protocoles d'authentification standards. Contrairement aux algorithmes propriétaires, les algorithmes standards ont été soumis à un examen public minutieux de la part des professionnels du secteur et de la sécurité afin de réduire toute présence potentielle de failles ou de vulnérabilités. En outre, ils bénéficient d'un soutien massif de la part du secteur.

L'utilisation de produits certifiés par un organisme tiers accrédité, comme FIPS (Federal Information Processing Standard) ou la certification Common Criteria, est une garantie qu'ils sont conformes à la norme industrielle.

Prenez en compte tous les points d'accès

Les entreprises doivent s'assurer que l'accès à toutes les informations sensibles est authentifié, que l'information se trouve sur site ou dans le Cloud. Les entreprises doivent mettre en œuvre les mêmes mécanismes de sécurité pour les ressources dans le Cloud que ceux qu'elles utilisent pour accéder à distance au réseau d'entreprise.

En outre, les entreprises doivent déployer des mécanismes de sécurité afin de s'assurer que les utilisateurs accédant aux ressources réseau à partir de leurs appareils mobiles grand public (par exemple, les tablettes ou les smartphones) sont bien authentifiés.

Mettez en œuvre des politiques efficaces de gestion des mots de passe

À chaque fois qu'il est nécessaire d'utiliser des mots de passe, par exemple pour garantir l'authenticité de l'utilisateur ou lors de la définition de mots de passe pour les jetons de l'authentification selon le contexte, SafeNet vous conseille de suivre les pratiques de gestion de mots de passe ci-dessous :

- Les entreprises ne doivent pas autoriser l'utilisation de mots de passe par défaut.
- Les entreprises doivent mettre en vigueur des mots de passe comprenant un mélange de lettres majuscules et minuscules et des chiffres.
- Le mot de passe doit contenir au moins 8 caractères.
- Les entreprises ne doivent pas autoriser l'utilisation de mots de passe semblables au nom de l'utilisateur.
- Les entreprises doivent mettre en vigueur une politique de remplacement régulier du mot de passe. La fréquence de remplacement du mot de passe doit être basée sur le profil de risque, mais doit être effectuée au moins une fois tous les trois mois

Déploiement robuste de l'authentification par mot de passe à usage unique (OTP)

Utilisez une gestion de clés solide en complément de la solution d'authentification

Les systèmes d'authentification par mot de passe à usage unique (OTP ou One-Time Password) reposent sur l'utilisation d'un secret partagé, généralement appelé la graine ou "seed" OTP (ou valeur de la graine du token). Cette graine est utilisée pour générer le code d'accès à usage unique. La graine OTP est stockée sur le token et sur le système de gestion de l'authentification.

L'efficacité du mécanisme d'authentification OTP repose sur le secret de la graine OTP, ainsi que sur l'indice de chiffrement de l'algorithme utilisé pour générer le mot de passe à usage unique. Si un de ces éléments est compromis, c'est la solution d'authentification toute entière qui se voit fragilisée.

Dans la majorité des cas, le fournisseur du système d'authentification programme les graines dans le token et fournit les informations du token au client. Lorsque le token est attribué à un utilisateur, le lien est établi entre l'utilisateur et le mécanisme d'authentification. Ces graines du token attribué, associées à des profils d'authentification de l'utilisateur, sont utilisées par le gestionnaire d'authentification pour contrôler l'accès de l'utilisateur à l'information.

La gestion des clés contribue à prévenir le vol interne et les logiciels malveillants en stockant les données de sécurité sur un système de fichiers chiffrés ou dans une base de données chiffrées. Les systèmes d'authentification étant tous constitués d'un certain type d'informations sensibles, la protection des données confidentielles est primordiale. Par conséquent, il est conseillé de chiffrer la base de données, par exemple, d'un système d'authentification OTP qui stocke les graines des tokens et des informations qui relient les graines aux tokens et aux utilisateurs. La gestion des clés de chiffrement permettant de déverrouiller ces données est devenue indispensable à une approche globale de la sécurité. Pour obtenir une gestion de clés solide, les clients peuvent stocker les clés de chiffrement dans un module de sécurité matériel (HSM : Hardware Security Module).

Contrôlez la sécurité des données sur votre site de travail

Les entreprises qui pensent avoir un profil de risque élevé peuvent créer un autre niveau de sécurité en programmant les graines du token dans leur data center. Les tokens programmables permettent aux entreprises de générer les données de sécurité du token et de le programmer en toute sécurité dans leurs locaux. Les entreprises considérées comme étant particulièrement à risque qui voudraient se reposer sur la sécurité d'un fournisseur s'exposeraient à une autre variable qui échappe à leur contrôle, quelles que soient les mesures de sécurité prises par le vendeur. Ce conseil est surtout valable pour les secteurs où les problèmes de sécurité sont beaucoup plus saillants, tels que les services financiers, la santé, et les organismes gouvernementaux.

Solutions complémentaires

Utilisez l'authentification avant le démarrage pour protéger votre main-d'œuvre itinérante et vos appareils portables

Pour les composants vitaux du système, les entreprises devraient examiner la nécessité d'une authentification avant le démarrage. De cette manière, elles s'assurent que seuls les employés sélectionnés sont en mesure de démarrer le système et d'effectuer des tâches administratives.

Pour les utilisateurs qui stockent des informations sensibles sur des appareils mobiles et ordinateurs portables, le chiffrement intégral du disque avec l'authentification avant le démarrage (par certificat) permet de s'assurer que les données se trouvant sur un appareil perdu ou volé ne seront pas exposées.

Développez vos capacités d'audit et de vérifications judiciaires

Les pistes d'audit et les vérifications judiciaires facilitent une détection précoce en cas de violation de la sécurité du système de l'entreprise. Les pistes d'audit sont efficaces car elles fournissent des informations sur les tentatives d'authentification réussies ou non au système. L'indicateur le plus évident d'une attaque se traduit par une forte augmentation du nombre de tentatives ratées de connexion et de verrouillage du compte. Généralement, ceci est l'œuvre d'un pirate informatique maladroit et pas très doué. En général, les stratégies de verrouillage limitent ce type d'attaque. Un pirate informatique plus expérimenté va patiemment effectuer un petit nombre de tentatives de connexion ou aura recours à des méthodes d'ingénierie sociale telle qu'un appel au service d'assistance pour demander une réinitialisation du code PIN / mot de passe. Sans outils d'audit efficaces, ce type d'attaque pourrait passer inaperçu.

L'authentification selon le contexte est un complément à une approche multi-niveaux

L'authentification selon le contexte utilise des informations contextuelles pour vérifier si l'identité d'un utilisateur est authentique ou non. Grâce aux profils de risque, les entreprises ont les moyens de restreindre l'accès à des systèmes spécifiques ou à des éléments de contenu selon les critères d'un utilisateur. Ces moyens sont valables même si l'utilisateur s'authentifie sur le réseau local ou à distance, même si l'utilisateur accède à des informations à partir d'un ordinateur d'entreprise, ou même si l'heure d'accès semble raisonnable (par exemple aux heures de bureau correspondant au pays où se trouve l'utilisateur détecté en fonction de l'adresse IP de son ordinateur). La plupart des informations utilisées par l'authentification selon le contexte sont accessibles au public. Elles sont donc également

facilement accessibles aux pirates informatiques. Aussi, il est conseillé d'utiliser cette méthode en tant que complément à d'autres méthodes d'authentification plus fortes ou en tant que premier niveau d'authentification dans le cadre d'une approche multi-niveaux.

Authentification polyvalente pour une structure de sécurité complète

SafeNet, tout en reconnaissant à quel point il devient de plus en plus compliqué de maintenir les contrôles de sécurité dans un paysage aussi diversifié, offre aux entreprises des suites de produits intégrés leur permettant de s'assurer un accès autorisé et de gérer toutes les opérations d'authentification multi-facteurs pour les employés qui ont besoin d'un accès sécurisé aux applications sur site et dans le Cloud ainsi que pour les clients et partenaires qui travaillent en ligne.

Les solutions de SafeNet, maintes fois récompensées, offrent une base adaptable et complète répondant aux besoins de l'entreprise pour une solution solide d'authentification et de vérification des transactions.

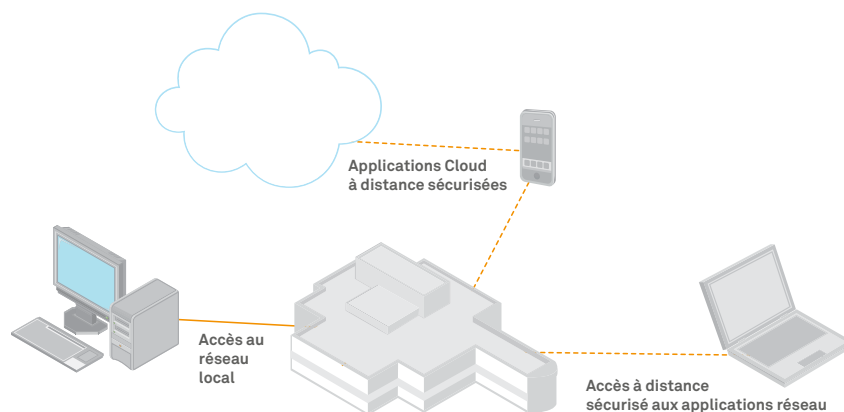
Environnement d'authentification totalement fiable de SafeNet

Suite aux récents événements, SafeNet a été le premier à offrir une structure d'authentification qui fournit aux entreprises une sécurité, une flexibilité et un contrôle sans précédent de leur environnement d'authentification. Cette structure inclut:

- **Tokens programmables:** permet aux clients de générer les données de sécurité du token et de le programmer sur le lieu de travail. SafeNet est l'un des seuls fournisseurs du marché à permettre la programmation sur le site de travail de tokens à mot de passe à usage unique. Les tokens d'authentification selon le contexte peuvent être reprogrammés automatiquement.
- **Niveaux supplémentaires de protection:** chiffre les données du token et stocke / gère les clés à l'aide d'un module de sécurité matériel (HSM)
- **Amélioration de la gestion et de la visibilité:** centralisation et simplification de l'administration, du déploiement et de la gestion
- **Reconnu sur le marché:** algorithmes standards et pas de technologie propriétaire

Gamme de solutions d'authentification de SafeNet pour une plus grande sécurité de l'accès à distance, local et au Cloud

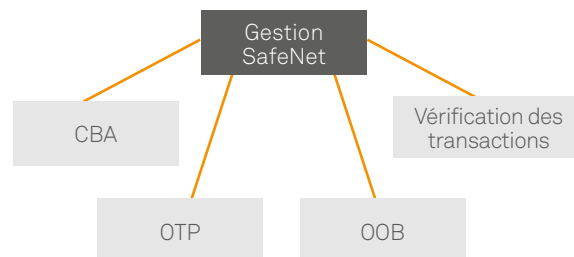
Les solutions d'entreprise de SafeNet permettent aux entreprises de satisfaire aux exigences en matière de sécurité et de prévoir les dépenses éventuelles sans avoir à modifier leur infrastructure sous-jacente. En proposant des plates-formes de gestion d'une grande souplesse, la plus large gamme de méthodes d'authentification forte et de facteurs de forme, et des fonctions de vérification des transactions, ainsi que la fédération d'identité et l'identification unique (SSO), les solutions SafeNet posent les fondations de l'avenir de la sécurité qui permettent aux entreprises d'adopter une stratégie de gestion des identités modulaire et tournée vers l'avenir afin de s'assurer que leurs besoins en matière de sécurité sont satisfaits au fur et à mesure de l'émergence de nouvelles menaces et de l'évolution des appareils et des besoins des utilisateurs.



Toutes les solutions d'authentification de SafeNet sont gérées par une plate-forme d'authentification unique, qui permet de bénéficier de:

- L'accès distant sécurisé pour les employés et les partenaires
- La sécurité des transactions pour les services bancaires en ligne
- La prise en charge du Cloud embarqué pour l'accès sécurisé aux applications SaaS
- L'accès sécurisé aux ressources de l'entreprise à partir des appareils mobiles
- Un serveur d'authentification unique pour une gestion centralisée et simplifiée
- Un environnement d'authentification totalement fiable permettant au client de garder le contrôle de ses propres données

Pour en savoir plus à propos de la gamme complète de solutions d'authentification de SafeNet, veuillez-vous rendre sur www.safenet-inc.com/authentication.



À propos de SafeNet

Fondé en 1983, SafeNet est l'un des leaders mondiaux de la sécurité des informations. SafeNet protège les biens qui ont la plus grande valeur de ses clients et, entre autres, les identités, transactions, communications, données et licences logicielles tout au long du cycle de vie de ces informations. Plus de 25 000 clients, des entreprises commerciales aux organismes gouvernementaux, répartis dans plus de 100 pays du monde entier, font confiance à SafeNet pour assurer la sécurité de leurs informations.

Nous contacter: Pour retrouver les coordonnées de toutes nos filiales, rendez-vous sur www.safenet-inc.com

Nous suivre: www.safenet-inc.com/connected

©2011 SafeNet, Inc. Tous droits réservés. SafeNet et le logo SafeNet sont des marques déposées de SafeNet.

Tous les autres noms de produits sont des marques déposées de leurs propriétaires respectifs. WP (FR) A4-28.6.11