Livre blanc signé Expert Insights

Comment réduire les primes de cyberassurance et améliorer la sécurité grâce à l'authentification multifacteur

Publié par
Janv 2023

Expert Insights

Sponsorisé par
HID

01 Introduction

Aujourd'hui, les entreprises sont confrontées à un volume sans précédent de menaces de cybersécurité, qui mettent en danger les données des clients et la réputation de l'entreprise. Les pertes financières subies par ces attaques peuvent être vertigineuses. Le coût moyen d'une fuite de données a atteint 4,35 millions de dollars en 2022, une somme existentielle pour de nombreuses PME.[1]

Il n'y a pas de réponse facile à ce problème. Les entreprises de toutes tailles ont besoin d'une stratégie de cybersécurité solide pour aider à minimiser les risques, en utilisant une gamme d'outils et de procédures garantissant la bonne protection.

Cela dit, il existe un dispositif fondamental que toutes les organisations devraient mettre en place : l'authentification multifacteur ou MFA (pour « Multi-Factor Authentication » en anglais). La MFA peut aider les organisations à lutter contre les cyberattaques en sécurisant l'accès et les comptes. C'est pourquoi elle est devenue une mesure de sécurité indispensable pour pouvoir obtenir une cyberassurance.

Dans cet article, nous verrons comment les organisations peuvent accéder plus facilement à la cyberassurance – tout en réduisant les primes d'assurance – grâce à l'utilisation d'une solution MFA robuste. Mais commençons par examiner en quoi consiste la cyberassurance, ce qu'elle couvre et comment faire pour en bénéficier.

02

Qu’est-ce que la cyberassurance et que couvre-t-elle ?

La cyberassurance, ou cyberassurance responsabilité, comprend un certain nombre de polices d’assurance conçues pour aider votre organisation en cas de violations causées par un incident de cybersécurité. À l’échelle mondiale, des centaines de cyberassureurs et de polices sont disponibles, couvrant un large éventail de scénarios différents. Ces politiques incluent généralement :

- Les coûts des dépenses directes engendrées par une attaque sur le réseau. Cela peut englober les coûts de conseils d’experts, d’investigation, de restauration ou de réparation des données, de notification de la violation aux clients, de frais juridiques et même de relations publiques

- Les frais juridiques si une cyberattaque entraîne la violation de la législation sur la protection de la vie privée ou des accords contractuels, ou dans le cas d’une action collective

- Les coûts portant sur les profits et paiements de défense en justice si votre organisation n’est pas en mesure de remplir ses obligations contractuelles en raison de cyberattaques

- La technologie devenue inutilisable et les profits perdus en raison d’attaques telles que les ransomwares, et le coût même des rançons pour pouvoir restaurer l’accès à la technologie

- La fraude au virement causée par l’ingénierie sociale, comme les attaques de phishing et les escroqueries par usurpation d’identité

- Les pertes de profits causées par l’atteinte à la réputation et à l’image de marque souvent constatés après la violation (bien que souvent limitées dans le temps)

Tous les fournisseurs, cependant, ne couvriront pas l’ensemble de ces polices. Nombre d’entre eux ne couvriront pas les pertes futures potentielles de bénéfices ni les dommages résultant de toute perte de votre propriété intellectuelle – ceux qui le font ont souvent des primes très chères.

C’est pourquoi la cyberassurance ne peut remplacer un cadre solide de sécurité capable de neutraliser la cybercriminalité en amont. Son rôle est plutôt d’encourager les entreprises à appliquer les meilleures pratiques de sécurité et d’offrir une assistance en cas d’attaque.

Qui a besoin d’une cyberassurance ?

Toute organisation qui stocke et gère des informations sensibles en ligne, utilise des systèmes numériques ou est hautement réglementée par des agences gouvernementales et internationales, est exposée au risque de cybercriminalité et doit donc envisager la souscription d’une cyberassurance. Si votre entreprise a recours à l’informatique et traite des informations personnelles sur Internet – comme le commerce électronique, la fabrication, les soins de santé, les infrastructures critiques – souscrire une cyberassurance doit faire partie de votre liste de priorités.

Pour les petites entreprises, la cyberassurance est essentielle. En effet, les PME sont une cible privilégiée pour les cybercriminels qui savent qu’il est peu probable qu’elles disposent d’une infrastructure de sécurité complète (et coûteuse) pour prévenir les attaques ou les escroqueries sur les réseaux. En cas d’attaque, les PME sont également plus vulnérables : elles ne peuvent pas se permettre les dépenses énormes qui découlent de l’absence d’une cyberassurance, telles que les frais juridiques, les paiements de rançons ou les pertes de profits.

Comment faire pour bénéficier d’une cyberassurance ?

Comme pour tout type d’assurance, certaines conditions doivent être remplies pour obtenir une couverture. Ces conditions peuvent déterminer si vous êtes éligible et, surtout, quel sera le coût des primes de cyberassurance.

Si les conditions spécifiques varient d’un fournisseur à l’autre, un certain nombre d’entre elles, fondamentales, sont couramment observées dans les diverses politiques de sécurité. Voici les principales :

- Mettre en place une formation à la sécurité, qui comprend une simulation de phishing et des campagnes de sensibilisation

- S’assurer que les données sensibles et précieuses sont régulièrement sauvegardées pour être restaurées en cas d’attaque par ransomware

- Auditer et examiner régulièrement les procédures et politiques de sécurité

- S’assurer que les données clés sont chiffrées pour les protéger contre la violation et le vol de données

- S’assurer que les appareils sont protégés contre les malwares et maintenus à jour grâce à la sécurité et à la gestion des terminaux

- Respecter les cadres et procédures de protection des données tels que le RGPD

- Mettre en œuvre des contrôles d’identité et d’accès avec un approvisionnement sécurisé et, surtout, une authentification multifacteur

De plus en plus, l’authentification multifacteur devient un outil non optionnel pour obtenir une assurance. Sans elle, vous pourriez être confronté à un refus de couverture ou à des primes d’assurance beaucoup plus élevées.

03

Qu’est-ce que l’authentification multifacteur et comment fonctionne-t-elle ?

L’authentification multifacteur impose l’utilisation de plusieurs méthodes de vérification différentes lorsque les utilisateurs se connectent à leurs comptes et applications. Cela permet d’éviter les attaques par prise de contrôle de compte et s’avère très efficace pour arrêter les violations de données liées à l’identité. La MFA est souvent imposée par de nombreux cyberassureurs – et les solutions MFA les plus sécurisées peuvent aider à maintenir le coûts des primes à un faible niveau.

Un « facteur » est un moyen de confirmer l’identité lorsqu’un utilisateur demande l’accès à un compte numérique. Les trois facteurs d’authentification les plus courants sont :

- Quelque chose que vous connaissez : un mot de passe ou code PIN

- Quelque chose que vous avez : un appareil sécurisé, comme un smartphone, une carte à puce ou une clé USB

- Quelque chose que vous êtes : un être contrôlable biométriquement, notamment par l’empreinte digitale ou la reconnaissance faciale

Avant, l’authentification de l’identité ne reposait que sur un seul facteur : un mot de passe. Mais face à la prolifération des arnaques liées aux mots de passe, les facteurs de sécurité supplémentaires sont désormais courants, en particulier pour les comptes des particuliers, mais de plus en plus aussi dans la sphère professionnelle.

Par exemple, lorsque vous vous connectez à un compte avec la MFA, il peut vous être demandé un mot de passe, puis un code de vérification envoyé par SMS ou une application d’authentification. Vous pouvez également utiliser un code PIN et une empreinte digitale ou un scan facial à l’aide d’un smartphone de confiance.

Pour les particuliers, la MFA est souvent gérée par compte. Pour l’entreprise, il existe une gamme de solutions MFA sur le marché qui fournissent des contrôles d’authentification centralisés pour tous les systèmes et applications. La mise en œuvre de la MFA est une étape importante, non seulement pour obtenir une cyberassurance, mais aussi pour créer une posture de cybersécurité solide dans le paysage actuel des menaces.

04

Pourquoi les cyberassureurs demandent-ils la MFA ?

L’explosion des applications cloud et SaaS a entraîné une augmentation de 307 % des attaques par prise de contrôle de comptes entre 2019 et 2021[2], engendrant une hausse des pertes financières de 90 % rien qu’en 2021. Souvent, ces attaques ne sont pas si high-tech ni sophistiquées ; elles fonctionnent à l’aide de méthodes simples, moyennant un coût faible, mais hautes en récompenses.[3]

Par exemple, les attaquants peuvent envoyer des e-mails de phishing déguisés en e-mails légitimes pour récupérer des mots de passe ; plus de 80 % des violations de données[4] commencent par un mot de passe compromis. Ils peuvent également acheter des malwares prêts à l’emploi pour compromettre les adresses électroniques et les mots de passe. Ces attaques sont faciles à exécuter à grande échelle et des millions d’entreprises dans le monde entier se retrouvent ainsi exposées à des risques.

La MFA protège l’accès aux applications, aux systèmes et aux données sensibles en empêchant les attaquants de compromettre les comptes, même s’ils ont réussi à voler des noms d’utilisateur et des mots de passe. En fait, une étude de Microsoft a révélé que la simple mesure consistant à implémenter la MFA peut empêcher 99,9 % des attaques sur les comptes.[5]

Certains assureurs ne couvriront pas les violations dues à des erreurs humaines au sein des entreprises.[6] C’est le cas des escroqueries par phishing, où un employé donne accidentellement accès à un compte à un attaquant. La MFA aide les entreprises à éviter ce scénario en appliquant des politiques d’authentification sur les réseaux, les applications et les périphériques afin d’empêcher tout accès non autorisé, quel que soit l’emplacement.

La MFA est donc une mesure de sécurité essentielle à mettre en place, même si vous n’envisagez pas de cyberassurance. En mai 2021, le Décret américain sur l'amélioration de la cybersécurité nationale[7] signé par le président Biden a imposé l’utilisation de la MFA pour toutes les agences fédérales et, en Europe, l’utilisation de la MFA est recommandée par les directives de l’ENISA.[8]

05

Comment choisir la bonne solution d’authentification multifacteur

La mise en œuvre d’une solution MFA peut aider à satisafire aux conditions fixées par de nombreux assureurs. Mais toutes les solutions MFA ne se valent pas et, si l’on est à la recherche d’une solution, trois domaines clés sont à prendre en compte pour garantir le plus haut niveau de protection et réduire davantage le risque de violation des données (ce qui permet également de diminuer les primes de cyberassurance).

Examinons chacun de ces domaines en détail :

Authentification multifacteur résistante au phishing

Comme nous l’avons vu, la mise en œuvre de la MFA permet de prévenir la grande majorité des attaques de compromission de comptes. Mais les cybercriminels continuent d’innover avec de nouvelles méthodes d’attaque conçues pour contourner les contrôles d’authentification. Parmi les attaques les plus courantes figurent le phishing, le spam par notification push, le vol de cookies système et les attaques par échange de cartes SIM. C’est pourquoi il est important de rechercher des solutions d’authentification multifacteur avec des méthodes et des politiques d’authentification robustes capables de résister à ces attaques.

Aux États-Unis, la CISA (Cybersecurity and Infrastructure Security Agency) a publié des directives sur l’authentification résistante au phishing. Ils recommandent de mettre en œuvre l’authentification basée sur FIDO2/WebAuthn, une méthode d’authentification largement prise en charge qui permet une authentification sécurisée et sans mot de passe à l’aide d’appareils fiables.[9]

Avec FIDO, une clé privée est stockée localement sur l’appareil client, tandis que la clé publique est enregistrée auprès du service en ligne. Lors d’une tentative de connexion, l’appareil de l’utilisateur prouve la possession de la clé privée par une vérification d’authentification multifacteur, telle qu’un scan d’empreinte digitale. Cela permet un accès sécurisé aux comptes et résistant au phishing, sans utiliser de mot de passe. Nous recommandons donc de rechercher une solution qui fournit une authentification basée sur FIDO.

Prise en charge de différentes préférences utilisateur et exigences d'accès

Les meilleurs fournisseurs d'authentification offrent une large gamme de méthodes d'authentification flexibles pour répondre aux besoins uniques de votre organisation et prendre en charge les préférences des utilisateurs. Il existe différentes méthodes d'authentification (OTP, PIN, FIDO, biométrie, notifications push, etc.) et formats (mobile, carte à puce, clé de sécurité) disponibles, il est donc important de tenir compte des besoins uniques de vos utilisateurs lors du choix d'une solution.

Par exemple, certains utilisateurs utiliseront la biométrie sur leurs appareils mobiles personnels pour s'authentifier, tandis que d'autres voudront peut-être garder les appareils privés séparés du travail et utiliser un jeton de sécurité fourni par l'entreprise à la place. Certains secteurs ne peuvent pas du tout utiliser de smartphones : par exemple, les salariés travaillant dans les plateformes pétrolières, où ils présentent un risque d'incendie, ou dans les zones géographiques ayant une mauvaise couverture réseau. Dans ces cas, les entreprises doivent pouvoir proposer des cartes ou des clés d'authentification à leurs utilisateurs.

Autre point à prendre en compte : toutes les méthodes d'authentification ne sont pas aussi sûres. L'envoi d'un mot de passe à usage unique par e-mail ou SMS est moins sécurisé que la biométrie ou une notification push. Choisir une solution qui offre ces méthodes plus sûres peut aider à réduire les primes de cyberassurance.

Enfin, les administrateurs doivent pouvoir gérer facilement les identifiants d'authentification et les appareils. Dans les grandes entreprises, gérer les identifiants pour des centaines d'utilisateurs peut être extrêmement complexe et chronophage. Nous recommandons de choisir une solution qui offre une gestion centralisée des identifiants PKI et qui provisionne/révoque automatiquement l'accès lorsqu'un employé rejoint ou quitte l'organisation.

Souplesse des politiques de contrôle d'accès

Quelle que soit la solution MFA que vous choisissez, vous devez inclure des options de déploiement flexibles pour garantir la convivialité et l'évolutivité, tout en répondant aux besoins et aux exigences de votre propre posture de sécurité. Cela suppose la prise en charge d'un large éventail de méthodes d'authentification, mais aussi de politiques de contrôle d'accès pouvant être configurées et ajustées.

Par exemple, la question de savoir combien de fois une tentative d'authentification est autorisée avant que le système ne soit verrouillé dépend en fin de compte du niveau de risque que votre organisation souhaite prendre. Cela doit être évalué en fonction des besoins des utilisateurs qui doivent se connecter rapidement à leurs comptes professionnels. Les entreprises doivent pouvoir personnaliser ce type de politique de contrôle d'accès pour s'assurer que des règles de sécurité cohérentes sont définies et maintenues, empêchant ainsi tout accès non autorisé aux comptes.

Une autre politique d’accès importante concerne les utilisateurs à privilèges. Dans certaines entreprises, les utilisateurs à privilèges, tels que les administrateurs informatiques ayant accès à des ressources et des données sensibles, doivent respecter des politiques de sécurité supplémentaires. Ces politiques peuvent rajouter d’autres facteurs d’authentification, tels que la vérification biométrique ou la notification push avec clé.

Ces utilisateurs peuvent également avoir besoin de s’authentifier plus régulièrement que les utilisateurs ayant accès à des données moins sensibles. Les meilleures solutions d’authentification prendront en charge la configuration et la mise en œuvre des politiques pour faciliter ce cas d’utilisation.

Nous recommandons donc de rechercher une solution offrant cette souplesse, avec des politiques de contrôle d’accès qui peuvent être déployées dans toute l’entreprise au niveau des utilisateurs et des rôles. Cela garantit que les meilleures pratiques de sécurité de la MFA peuvent être respectées et équilibrées par rapport aux besoins globaux de l’entreprise, en gérant la sécurité et le confort des utilisateurs, tout en améliorant la sécurité des utilisateurs à privilèges.

« Nous recommandons donc de rechercher une solution offrant cette souplesse, avec des politiques de contrôle d’accès qui peuvent être déployées dans toute l’entreprise au niveau des utilisateurs et des rôles. »

06

Trouver la bonne solution d’authentification avec HID

Comme nous l’avons vu, la première étape pour respecter les exigences en matière de cyberassurance et minimiser le montant des primes consiste à mettre en œuvre une solution d’authentification multifacteur efficace, sécurisée et fiable. La MFA n’est pas une solution unique et universelle. Elle est proposée dans un large éventail de solutions, avec de nombreux cas d’utilisation et de scénarios à prendre en compte. Il est donc crucial de choisir les bonnes méthodes et les bons formats, qui répondront aux besoins de votre organisation, seuls ou combinés les uns avec les autres.

Aujourd’hui, les entreprises doivent prendre en charge un large éventail de cas d’utilisation pour l’authentification et sécuriser l’accès aux systèmes cloud et hérités, sur différents appareils, postes de travail, réseaux, applications web et cloud, tout en respectant les normes et réglementations de sécurité en constante évolution. En outre, cela doit se faire avec peu ou pas d’interruption des flux de travail actuels et des comportements utilisateurs.

Dans des secteurs tels que la santé, l’industrie, la vente, les centres d’appels et les forces de l’ordre, plusieurs utilisateurs doivent souvent s’authentifier sur les mêmes appareils rapidement et facilement plusieurs fois par jour.

Si votre organisation appartient à l’un de ces secteurs et que vous souhaitez mettre en œuvre une authentification sécurisée et flexible avec prise en charge de la biométrie, des appareils mobiles, des badges d’accès, des cartes à puce ou des clés de sécurité, vous pouvez envisager de déployer une solution MFA telle que HID DigitalPersona.

Si vous cherchez à exploiter les appareils mobiles des utilisateurs comme supports d’authentification, faciles à utiliser et toujours à portée de main, ou si vous cherchez à fournir à vos clients une solution sécurisée et rapide pour vous connecter ou vérifier les transactions, vous pouvez envisager HID Approve, une solution intelligente, évolutive et intuitive qui permet aux utilisateurs d’authentifier, d’accéder aux ressources ou de signer une transaction en quelques secondes.

Si vous cherchez à vous débarrasser des mots de passe, les cartes à puce et les clés de sécurité Crescendo HID compatibles FIDO et PKI fournissent une authentification résistante au phishing en permettant aux utilisateurs de se connecter et d’accéder en toute sécurité aux réseaux, postes de travail, applications et données, sans avoir besoin d’un mot de passe. Cela permet d’améliorer la sécurité et le confort de l’utilisateur, tout en réduisant les primes de cyberassurance.

Les solutions d’authentification multifacteur de HID sont utilisées par des organisations de toutes tailles dans de multiples secteurs, des services bancaires et financiers, aux gouvernements, universités et hôpitaux, en passant par les forces de l’ordre, les services publics et la vente/distribution – pour augmenter la sécurité et améliorer l’expérience utilisateur avec une authentification multifacteur facile à déployer, à gérer et à utiliser. De plus, HID permet également aux administrateurs informatiques de gérer de manière centralisée le cycle de vie des moyens d’identification numériques, de l’émission à la révocation, afin de s’assurer que l’accès est automatiquement révoqué lorsqu’un employé quitte l’entreprise.

Nous recommandons le portefeuille MFA de HID comme suite robuste, évolutive et hautement sécurisée de solutions d’authentification multifacteur qui garantissent la conformité et prennent en charge un large éventail de méthodes d’authentification et de facteurs de forme.

« Nous recommandons le portefeuille MFA de HID comme une suite robuste, évolutive et hautement sécurisée de solutions d’authentification multifacteur ».

07 Sponsor de ce livre blanc

HID est un fournisseur leader sur le marché de solutions de sécurité des identités pour l'authentification des actifs physiques et logiques (numériques). Marque indépendante du fournisseur suédois de portes et de contrôle d'accès ASSA ABLOY, HID fabrique et vend une variété de solutions de contrôle d'accès physique et logique, ainsi que des produits d'émission sécurisée pour accompagner ces solutions.

Il s'agit notamment de cartes à puce, de lecteurs de cartes, d'imprimantes et d'encodeurs de cartes, de services cloud, de technologies d'identification IoT et de logiciels de gestion des identités et des accès.

Depuis ses bureaux internationaux dans le monde entier, HID travaille avec des organisations dans plus de 100 pays à travers un certain nombre de secteurs, dont l'administration publique, l'éducation, la finance et l'aviation, les aidant à mettre en œuvre des environnements physiques et virtuels fiables basés sur un accès transparent et sécurisé.

www.hidglobal.com
Twitter: @HIDGlobal
LinkedIn: @hidglobal
customerservice@hidglobal.com
Tel: 800-872-5359

08 À propos d’Expert Insights

À propos d’Expert Insights

Expert Insights est une ressource mondiale et indépendante qui permet aux entreprises du monde entier d’effectuer des recherches et de comparer les solutions et services informatiques pou les entreprises. Notre objectif numéro un est d’aider les entreprises à rechercher et à trouver les bonnes solutions pour résoudre leurs problèmes de sécurité.

Textes de références

1. https://www.ibm.com/uk-en/security/data-breach

2. https://resources.sift.com/ebook/q3-2021-digital-trust-safety-index-battling-new-breed-account-takeover/

3. https://www.veriff.com/blog/account-takeover-fraud-statistics

4. https://www.idx.us/knowledge-center/how-compromised-passwords-lead-to-data-breaches

5. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

6. https://www.techtarget.com/searchsecurity/definition/cybersecurity-insurance-cybersecurity-liability-insurance

7. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

8. https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

9. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf