yubico

LIVRE BLANC SUR LE ZERO TRUST | JUIN 2021

Accélérez votre stratégie Zero trust avec l'authentification forte

Sept bonnes pratiques pour démarrer votre voyage

Introduction

La semaine dernière, j'ai reçu un e-mail dont l'objet méritait d'être lu deux fois : « Le zen du Zero trust ». Il s'agissait d'une invitation à un webinaire présenté comme « un échange animé de perspectives, d'opinions et de bonnes pratiques sur la voie de la sécurité des données ».

Cet e-mail est un bon exemple du buzz marketing autour du Zero trust. Le fait est qu'il n'y a rien de zen dans le Zero trust et encore moins d'éclaircissements. Où qu'ils aillent, les RSSI s'entendent dire qu'ils doivent absolument mettre en œuvre le Zero trust. Tous vos amis et concurrents ont déjà des stratégies. Et si vous n'en avez pas, vous pourriez avoir l'impression d'être en retard sur le sujet.

Le principe du Zero trust pourrait donc être applicable maintenant, sachant que le monde de la sécurité se dirige dans cette direction. Mais il est normal d'avoir quelques doutes sur le pragmatisme du Zero trust. C'est encore plus compréhensible si vous avez du mal à passer à un cadre ou une infrastructure Zero trust. Le fait est qu'il n'est pas facile de s'engager dans la voie du Zero trust et de continuer à le développer, quel que soit le nombre de RSSI qui prétendent le faire.

Si vous êtes un RSSI et que vous essayez de vous familiariser avec les aspects d'authentification du Zero trust, ce livre blanc est fait pour vous. Il se concentre sur les considérations clés et les mesures pratiques que vous pouvez prendre pour faire du Zero trust une stratégie viable et réalisable, en commençant par des éléments de base essentiels qui vous permettront de remporter des victoires rapides dans votre voyage vers le Zero trust.

Démystifier le Zero trust

Bien que le concept de Zero trust existe depuis un certain temps et que, dans de nombreuses entreprises, les initiatives Zero trust soient bien engagées dans le but de protéger leurs actifs les plus importants, il signifie encore différentes choses pour différentes personnes. Il peut y avoir de nombreux chemins vers le Zero trust qui traversent le réseau, l'identité et le contrôle des accès, et l'éventail des définitions ou des moyens d'y parvenir est vertigineux.

Pour faire court, le cadre du Zero trust implique simplement qu'une entreprise ne doit faire confiance à aucun individu ou objet à moins qu'il ne soit correctement vérifié avant de pouvoir accéder au réseau et aux données. Pouvez-vous imaginer aller faire des courses et penser que toutes les personnes qui entrent dans le magasin ne sont pas dignes de confiance et vont vous attaquer, voire compromettre votre bien-être ? Une pensée qui donne à réfléchir, et maintenant que nous avons vécu la pandémie, il s'agit d'un sentiment que nous connaissons tous trop bien.

Mais c'est exactement comme ça que fonctionne un système Zero trust. Votre réseau croit que tout ce qui vient de l'extérieur ou de l'intérieur du système est hostile. Le Zero trust signifie que vous ne pouvez faire confiance à rien, ni à l'utilisateur, ni à l'ordinateur, ni à la communication.

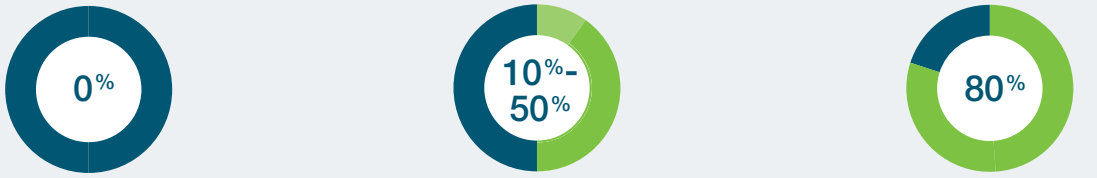
Vous devez valider et authentifier chaque utilisateur qui entre sur le réseau. Vous devez installer des agents de surveillance sur chaque terminal. Ils doivent valider que le dispositif est digne de confiance et fournir une attestation. Vous devez faire expirer la session d'un utilisateur et l'obliger à se réauthentifier fréquemment. Cela ne ressemble-t-il pas à une expérience utilisateur horrible ? Elle peut l'être si elle n'est pas abordée en tenant compte non seulement de la sécurité de l'entreprise, mais aussi de l'expérience de l'utilisateur.

Accélérez le Zero trust avec l'authentification forte

Le modèle Zero trust implique un niveau de confiance élevé dans les mécanismes d'authentification de chaque utilisateur de chaque appareil qui tente d'accéder aux ressources de l'entreprise, que ce soit à l'intérieur ou à l'extérieur du périmètre du réseau. L'adoption de l'authentification forte en tant qu'élément de base de votre stratégie Zero trust permettra de renforcer la sécurité de l'entreprise grâce à une gestion des identités et une authentification fortes. En revanche, pour une entreprise qui commence par l'accès au réseau, la ré-architecture des éléments du réseau peut être un processus beaucoup plus complexe et prendre beaucoup plus de temps. La ré-architecture de votre réseau selon les principes du Zero trust est importante, mais, avec une authentification forte et un cadre de contrôle d'accès en place, vous disposerez d'un composant fondamental du Zero trust qui peut être exploité tout au long du parcours. En outre, avec un cadre d'identité en place, vous pouvez savoir qui sont les utilisateurs, la force de leur authentification et comment ils sont connectés afin de détecter tout comportement inhabituel.

Quelle que soit la façon dont on aborde ce cadre général, il est important de commencer par créer une identité de confiance avec une authentification forte pour l'utilisateur comme base de référence, car elle offre des avantages immédiats à travers l'entreprise sur lesquels on peut s'appuyer à mesure que l'on développe des politiques d'accès Zero trust. Une partie essentielle de ce processus consiste à examiner comment les utilisateurs établissent leur identité et quel niveau de confiance peut être attribué à ce mécanisme. Si les utilisateurs n'utilisent que des mots de passe pour vérifier leur identité, l'entreprise n'a aucune garantie de sécurité, même si le reste de la stratégie du Zero trust est très nuancé et bien pensé. Les mots de passe sont connus pour être très vulnérables aux attaques à distance et aux attaques de l'homme du milieu (MiTM), et les mots de passe volés sont responsables de 80 % des violations de comptes. L'authentification par SMS, e-mails et mobile offre plus de sécurité pour les identités des utilisateurs que les mots de passe, mais toujours très vulnérables aux attaques à distance et à celles par hameçonnage.

Figure 1 : Taux de pénétration variable pour différentes vérifications d'utilisateur



Authentification/ MFA forte

2FA basiques : SMS, e-mail, mobile

Nom d'utilisateur et mot de passe

Les mots de passe sont responsables de 80 % des violations de sécurité

Dans une approche Zero trust, l'atténuation des vulnérabilités connues qui exposent des données sensibles est essentielle. L'accès des utilisateurs étant un risque fondamental pour la protection des données sensibles, il est essentiel de mettre en œuvre des mesures d'authentification forte.

Malheureusement, l'un des pièges les plus courants dans lequel les entreprises peuvent tomber est de considérer les initiatives Zero trust comme une initiative, et de considérer l'authentification forte comme une toute autre initiative, dans le cadre peut-être d'un mandat réglementaire ou d'un flux de travail connexe. Un exemple concret pourrait être d'avoir des moteurs de stratégie Zero trust et la gouvernance/ les politiques d'autorisation d'identité comme des systèmes séparés. Un moyen plus rapide et plus efficace de mettre les choses en place dès le départ est de considérer l'authentification forte comme un aspect fondamental du Zero trust et de lier l'authentification forte à l'initiative plus large du Zero trust.

Établir des identités d'utilisateur de confiance à l'aide d'une MFA moderne

L'authentification multifacteurs (MFA) moderne, dans le cadre de l'authentification forte, peut empêcher l'accès au réseau avec des mots de passe volés. L'authentification forte utilisant la MFA moderne permet une authentification de l'utilisateur résistant au hameçonnage avant que l'accès ne soit fourni. Les anciennes méthodes d'authentification multifacteurs (MFA), telles que les SMS, les applications d'authentification et autres, se sont avérées être hautement hameçonnables. L'authentification dans ces modèles n'est pas vraiment liée entre ce que l'utilisateur possède et le service, ce qui permet d'intercepter et de rejouer les codes d'accès. Si un utilisateur utilise ces méthodes pour vérifier son identité et entrer dans le réseau, le compte peut être compromis, ce qui permet à l'attaquant de prendre pied et d'effectuer un mouvement latéral qui peut être difficile à repérer. Par conséquent, le marché s'éloigne des secrets basés sur la symétrie (mots de passe, OTP) pour se tourner vers des solutions asymétriques plus avancées qui sont liées à des appareils physiques.

Pour qu'il s'agisse d'un cadre Zero trust sécurisé, les comptes d'utilisateur doivent être établis à l'aide d'une 2FA ou d'une MFA moderne, en utilisant des clés de sécurité matérielles spécialement conçues qui offrent les niveaux les plus élevés de défense contre le hameçonnage et d'accès sécurisé aux utilisateurs. Avec des clés de sécurité matérielles utilisant des protocoles d'authentification modernes, les utilisateurs peuvent enregistrer une seule clé de sécurité pour des centaines de services avec une paire de clés publique/privée unique générée pour chaque service, et les secrets ne sont jamais partagés entre les services. La clé privée stockée dans l'élément sécurisé de la clé matérielle ne peut être exfiltrée. De cette manière, les clés de sécurité matérielles empêchent les attaques à distance, de l'homme du milieu et par hameçonnage, car seul le service enregistré est autorisé à lancer la procédure d'authentification, contrairement à l'authentification par SMS ou avec toute autre application mobile.

Figure 2 : authentification forte activée avec les 2FA/MFA modernes

Quelque chose que vous connaissez (PIN) que vous êtes (biométrie) déverrouille l'appareil

Procédure de la paire de clés privée/publique pour valider l'accréditation

Un utilisateur peut enregistrer une clé de sécurité matérielle sur des centaines de services avec une paire de clés publiques/privées pour des services avec des secrets jamais partagés.

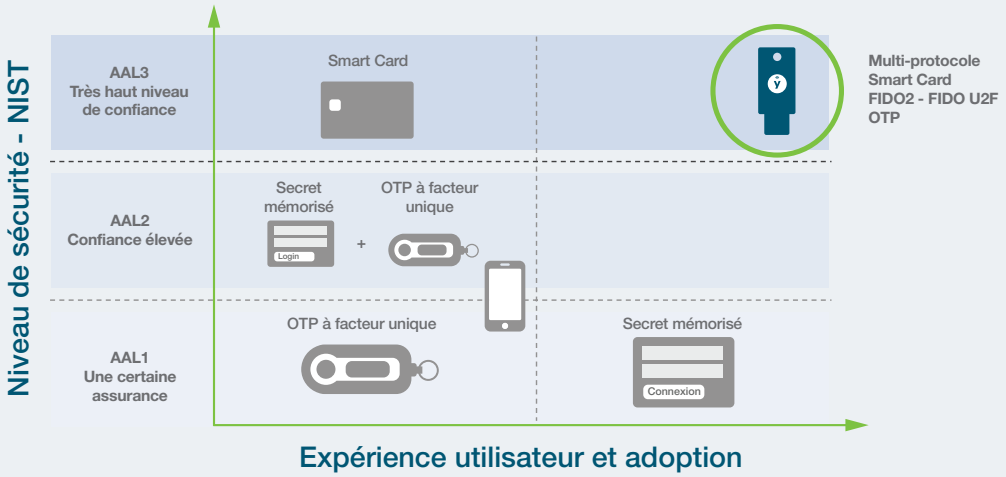
Les 7 bonnes pratiques d'authentification forte pour soutenir le Zero trust

Le Zero trust est un parcours, dont la première étape consiste à établir un cadre de confiance pour les utilisateurs. Les sept bonnes pratiques suivantes vous permettront de protéger l'accès d'un utilisateur en tant qu'élément fondamental de la construction de votre architecture Zero trust.

1. Déployez une authentification forte résistant au hameçonnage

Alors que toutes les études convergent pour constater que la cybercriminalité a augmenté de 300 % depuis la COVID-19 et que les utilisateurs continuent de travailler à domicile, les entreprises reconnaissent la nécessité de renforcer la sécurité de l'authentification des utilisateurs grâce à l'authentification multifacteurs (MFA). Comme nous l'avons mentionné précédemment, toutes les formes de MFA ne se valent pas et nous vous présentons ci-dessous quelques éléments à prendre en compte lors du choix des authentificateurs qui établissent l'identité des utilisateurs.

Figure 3 : toutes les formes de MFA ne sont pas créées de manière égale



Les clés de sécurité matérielle offrent une sécurité élevée et une grande facilité pour l'utilisateur

Lors de l'examen des capacités d'authentification, une entreprise doit prendre en compte les éléments suivants :

- **La sécurité :** s'agit-il d'un dispositif matériel spécialement conçu pour la sécurité ou d'un dispositif conçu principalement pour la communication (comme un téléphone) ? L'authentificateur ajoute-t-il d'autres complexités, comme le fait que l'utilisateur doive télécharger des applications ou des logiciels supplémentaires ? Et assure-t-il une protection à 100 % contre les attaques par hameçonnage ? Dans une perspective Zero trust, permettre une sécurité forte tout en réduisant la complexité devrait être un objectif clé de la conception. Un dispositif dédié à la sécurité permet une surveillance plus facile et plus cohérente.

- **Accès normalisé :** L'authentificateur est-il basé sur des normes ouvertes ? Si oui, il s'authentifiera de manière cohérente et sécurisée sur toute une gamme de plateformes et de services. L'utilisation de normes ouvertes permet des centaines d'intégrations prêtes à l'emploi et ne nécessite qu'une configuration limitée, ce qui réduit au minimum les solutions propriétaires. En outre, les normes ouvertes incitent le marché à suivre des modèles de déploiement standard, ce qui signifie que les fournisseurs déploieront les solutions d'une manière commune, réduisant ainsi la complexité pour les entreprises. Les normes FIDO et les cartes à puce (PIV) sont les normes d'authentification forte par défaut autour desquelles le marché se développe.
- **Déployabilité :** L'authentificateur peut-il assurer la sécurité sur plusieurs dispositifs et peut-il fonctionner hors ligne dans des zones restreintes aux mobiles ou autres, dans des lieux complètement éloignés ou sur des postes de travail partagés ? Nous savons que toutes les applications ou tous les environnements ne peuvent pas accueillir des protocoles d'authentification forte comme FIDO ou les cartes à puce (PIV). Un authentificateur, et votre système IAM, doit être capable de faire le lien entre les solutions basées sur l'OTP et les solutions plus sécurisées. Lorsqu'un système est prêt à utiliser une authentification plus forte, il n'est pas nécessaire de remplacer tous vos authentificateurs sur les terminaux. Sera-t-il en mesure de résister aux abus quotidiens dans divers environnements hostiles et de continuer à fonctionner ? Et enfin, s'agit-il d'une solution facile à gérer pour l'entreprise et l'utilisateur, avec une livraison clé en main à l'utilisateur où qu'il soit et des options simples de libre-service lui permettant d'être opérationnel en quelques minutes ?

La bonne solution d'authentification forte doit pouvoir répondre à toutes ces considérations pour obtenir les meilleurs résultats pour l'entreprise et ses utilisateurs.

2. L'attestation est importante pour le Zero trust

Dans un modèle du Zero trust, vous ne pouvez pas avoir une confiance implicite dans l'authentificateur. Dans un état d'esprit Zero trust, l'authentification forte est très importante mais vous devez toujours valider le dispositif matériel lui-même pour vous assurer qu'il provient d'une source connue et qu'il n'est pas compromis. La gestion des terminaux est un élément important d'un cadre du Zero trust, car les téléphones et les ordinateurs sont vulnérables aux logiciels malveillants. L'attestation permet de valider que le matériel d'authentification provient d'un fabricant de confiance et que les informations d'identification générées sur ce dispositif n'ont pas été clonées.

Il existe deux types d'authentificateurs : les authentificateurs de plateforme qui sont intégrés aux appareils modernes tels que les ordinateurs portables et les smartphones. Et puis les authentificateurs portables qui sont externes à l'ordinateur et aux téléphones et qui peuvent être transportés avec l'utilisateur, soit sur un porte-clés, soit sur une version miniaturisée qui peut être branchée sur l'ordinateur.

Le processus d'attestation d'un authentificateur particulier y est lié. L'attestation consiste en une paire de clés qui est gravée dans l'appareil pendant la fabrication et qui fournit des détails importants tels que le fabricant et le modèle de l'appareil. Il faut que le service connaisse l'origine de l'authentificateur et permette de vérifier, sur le plan du chiffrement, que la « signature de l'attestation » sur la clé publique nouvellement créée provient bien du dispositif de confiance. Les concepts d'attestation sont intégrés dans la norme FIDO et certains fournisseurs, comme Yubico, incluent également des capacités d'attestation pour les déploiements de cartes à puce. De plus, l'attestation est disponible dans des ordinateurs qui ont un élément sécurisé comme un TPM ou un Secure Enclave. Tous les appareils informatiques ne disposent pas d'un élément sécurisé par défaut. En outre, les systèmes informatiques qui comportent des composants OEM auront des éléments sécurisés provenant de nombreux tiers que vous devrez pister.

Il faut noter que si un authentificateur de plateforme (intégré au dispositif) est utilisé pour l'attestation du terminal, vous devrez pister et valider un certain nombre de fabricants OEM pour vous assurer qu'ils répondent à vos critères de sécurité. En outre, si le dispositif est compromis, l'authentificateur lui-même a un risque plus élevé d'être compromis car le code malveillant a plus de possibilités de trouver et d'en exploiter les vulnérabilités. Il s'agit essentiellement d'un point de défaillance unique. En revanche, l'utilisation d'un authentificateur portable sur lequel aucun logiciel tiers ne peut être chargé offre un niveau de garantie plus élevé que le dispositif de sécurisation des clés privées est connu et authentique, ce qui est conforme aux principes du Zero trust. À la fin, tout se résume à ce simple fait : si vous ne pouvez pas faire confiance à l'authentificateur ou si vous n'avez aucune visibilité sur celui-ci, vous ne pouvez pas non plus faire confiance à l'authentification.

3. Authentification forte pour tous les points d'accès

La plupart des entreprises utilisent des plateformes de gestion des identités et des accès (IAM) comme composants essentiels de leur cadre Zero trust. L'IAM est essentiel pour sécuriser l'entreprise hybride multi-cloud. Correctement mises en œuvre, les solutions modernes d'IAM peuvent offrir une expérience sans friction et sécurisée pour chaque utilisateur, actif et interaction de données, ce qui constitue la base d'une stratégie Zero trust. Ces solutions peuvent accorder des droits d'accès, fournir une authentification unique à partir de n'importe quel appareil, renforcer la sécurité avec la MFA, permettre la gestion du cycle de vie des utilisateurs, protéger les comptes privilégiés, etc... Lorsque l'on envisage la MFA dans le cadre du Zero trust, une approche architecturale prudente consiste à découpler l'authentificateur depuis la plateforme d'IAM. Cela permet d'avoir un authentificateur qui peut fonctionner avec un large éventail de solutions d'IAM. Le choix de produits qui exploitent des normes ouvertes permet au même authentificateur de fonctionner avec diverses solutions IAM, ce qui réduit considérablement l'impact du déploiement sur les utilisateurs finaux. Un utilisateur doit pouvoir être productif sur un nouveau système IAM, ou un point d'accès non fédéré, en utilisant le même authentificateur en quelques minutes et non en quelques semaines.

Outre les solutions centrées sur l'identité, il existe des solutions axées sur l'accès au réseau et la virtualisation qui jouent un rôle important dans la mise en place d'une architecture Zero trust. Une authentification idéale et forte et une solution MFA moderne devraient également fonctionner avec ces types de solutions pour aider à lancer une posture Zero trust. L'authentification forte par carte à puce est disponible depuis des années sur les réseaux et des solutions basées sur FIDO arrivent maintenant sur le marché. Il n'existe pas de « taille unique » dans le domaine du Zero trust. Quel que soit le point de départ de l'entreprise, il est possible d'obtenir une solution d'authentification forte à l'épreuve du temps et de la mettre en œuvre rapidement. Comme nous l'avons mentionné précédemment, certains systèmes existants peuvent présenter des limitations qui rendent la MFA impossible sans efforts supplémentaires. Une approche architecturale de transition consiste à exploiter un authentificateur physique capable de prendre en charge l'authentification forte OTP existante ainsi que l'approche d'authentification forte de votre état cible. Un utilisateur peut utiliser le même authentificateur physique et portable, ce qui minimise les complexités de déploiement et les perturbations pour l'utilisateur.

4. Authentification forte pour les comptes de non-utilisateurs

Les comptes qui sont utilisés pour exécuter des services sont vulnérables à la compromission. Tout comme pour les comptes d'utilisateurs, les comptes de services doivent être fortement protégés, surveillés et correctement circonscrits. Trop souvent, ces types de comptes ont été protégés par des mots de passe statiques. Malheureusement, un certain nombre de systèmes informatiques et télématiques présentent des limitations quant aux options d'authentification. Il est cependant courant que nombre de ces systèmes puissent tirer parti de l'authentification par chiffrement asymétrique intégrée aux environnements d'infrastructure à clé publique (PKI) couramment utilisés. Une authentification basée sur un certificat de chiffrement fournit une authentification forte car aucun mot de passe ne peut être volé. Il est cependant essentiel que la clé privée soit stockée dans du

matériel physique afin de s'assurer qu'elle ne puisse pas être volée. Une bonne pratique du marché consiste à stocker les clés privées dans des modules de sécurité matérielle (HSM), à savoir des matériels de sécurité de différentes tailles prévus à cet effet, allant des gros appareils physiques aux petits périphériques USB. Les HSM génèrent les paires de clés privée/publique utilisées pour l'authentification, et la clé privée ne quitte pas le HSM. La création de l'architecture d'un système HSM doit être abordée dès le début car les modèles de déploiement peuvent être centralisés ou décentralisés en fonction des cas d'utilisation. Il n'est pas rare que les entreprises disposent de différents HSM pour répondre à différents scénarios.

5. Authentifiez-vous pour prouver qu'il s'agit bien de vous au fil du temps

L'authentification forte est essentielle à une approche Zero trust. Mais comment savoir qu'une personne authentifiée a effectué le travail, et que ce travail peut être attesté dans le temps ? Dans le monde physique, une personne apposerait sa signature sur un document pour approuver un contrat ou tout autre document juridique. Dans le monde numérique, il est possible depuis un certain temps de signer numériquement des courriers électroniques et des documents électroniques. Ce processus était quelque peu lourd par le passé, mais aujourd'hui, avec les authentificateurs personnels et les HSM bon marché, la signature électronique est devenue beaucoup plus facile et plus fiable. Les procédures de signature basées sur le chiffrement, soutenues par du matériel, garantissent que le contenu a bien été créé par le signataire. Les processus de signature sont bien définis mais ceux-ci doivent être intégrés dans les différents systèmes de création de contenu. Les systèmes de gestion du développement logiciel sont probablement les systèmes les plus matures pour permettre des procédures de signature et sont un très bon endroit pour commencer. Pour une entreprise, le code qui fait fonctionner votre activité est essentiel et est une cible privilégiée de vos adversaires. En ces temps modernes, il est difficile de trouver une entreprise, quelle que soit sa taille, qui ne développe pas de logiciels à un certain niveau. Ce code doit donc être protégé par des processus d'authentification et de signature forts.

6. Mettez en place une authentification basée sur le risque

Le cadre Zero trust implique la mise en œuvre en temps réel de stratégies d'accès basées sur le risque, en fonction des signaux et des scores de risque. Ce cadre doit permettre aux contrôles automatisés et aux décideurs d'accéder facilement aux informations sur les applications, de savoir d'où viennent les utilisateurs, ce qui permet de différencier facilement les types de comptes et les empreintes digitales des appareils. Une solution d'authentification forte basée sur le matériel et hautement fiable peut obtenir un score de confiance élevé, permettant ainsi un accès privilégié plus important. Une fois vérifié, cet utilisateur hautement qualifié et approuvé peut effectuer des transactions plus sensibles telles qu'un important virement bancaire dans le cadre d'une transaction financière ou une ordonnance, et plein d'autres opérations sensibles de ce type. Une approche d'authentification forte de confiance permet une authentification progressive basée sur le risque, protégeant ainsi l'utilisateur et l'entreprise tout en augmentant la productivité.

7. Planifiez un avenir sans mot de passe

Ces dernières années, le terme « sans mot de passe » a pris de l'ampleur et il est désormais utilisé par de nombreux fournisseurs de solutions de sécurité, d'authentification et d'identité - chacun avec sa propre nuance. Pour plus de clarté, il est préférable d'utiliser une définition plus large.

Chez Yubico, nous avons adopté la suivante :

> « L'authentification sans mot de passe consiste en toute forme d'authentification qui ne demande pas à l'utilisateur de fournir un mot de passe lors de la connexion ».

Obtenir une connexion sécurisée sans mot de passe sur un ordinateur de bureau et un mobile et dans un large éventail de services nécessite un écosystème riche et un cadre cohérent pour l'authentification. Plus précisément, il faut un riche écosystème de normes ouvertes construit pour assurer la sécurité et la convivialité, tout en répondant aux besoins de portabilité, de compatibilité et d'interopérabilité pour s'adapter aux masses. Depuis sa création, Yubico a plaidé en faveur de normes de sécurité ouvertes pour atteindre ces objectifs. Yubico a ouvert la voie en lançant les normes ouvertes WebAuthn et FIDO, et a travaillé avec des géants de la technologie comme Google, Microsoft et Apple pour intégrer ces normes dans les systèmes d'exploitation et les logiciels de navigation que nous utilisons tous les jours. Ces normes, associées à une YubiKey, permettent une authentification forte sur les appareils, les applications et les services, sans logiciel propriétaire supplémentaire. Cela fonctionne, tout simplement.

Solutions de gestion des identités et des accès (IAM) (par ex. Azure Active Directory, Okta, Duo, Ping, ILEX et bien d'autres) ont également adopté des normes ouvertes en se superposant aux géants de plateforme pour offrir les fonctionnalités et l'échelle dont les entreprises ont besoin pour adopter l'authentification forte sans mot de passe pour leurs applications et services critiques.

Les entreprises peuvent emprunter toutes les voies vers l'authentification sans mot de passe en adoptant une approche sans mot de passe par carte à puce, sans mot de passe FIDO2/WebAuthn ou une approche hybride sans mot de passe qui utilise une combinaison de carte à puce et de mot de passe FIDO2. La solution dépendra de leurs scénarios commerciaux et de leur environnement d'infrastructure interne. Les entreprises qui disposent d'un grand nombre de systèmes existants et d'une infrastructure sur site seraient sages de poursuivre une stratégie sans mot de passe par carte à puce, tandis que les entreprises qui privilégient le cloud computing peuvent en toute confiance explorer le sans mot de passe FIDO2. Ou, dans un troisième scénario, les entreprises peuvent choisir d'employer une double approche. Par exemple, les clients peuvent opter pour une approche sans mot de passe FIDO2/WebAuthn pour la connexion aux ordinateurs et les applications Web fédérées, tout en choisissant une approche sans mot de passe par carte à puce pour l'accès sécurisé au réseau sur site (RDP, VPN, VDI). De cette manière, les entreprises peuvent adopter une stratégie sans mot de passe pour s'adapter à des cas d'utilisation spécifiques, compte tenu de leurs environnements et de leurs segments d'utilisateurs. Yubico peut soutenir les initiatives Zero trust et aider les entreprises dans leur voyage sans mot de passe sur tous ces scénarios.

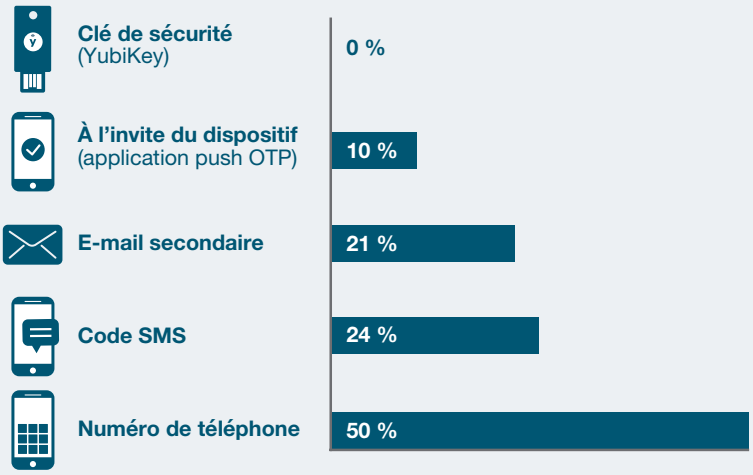
Pour en savoir plus sur la manière de poursuivre une stratégie sécurisée sans mot de passe afin de soutenir votre initiative Zero trust, consultez notre série Sans mot de passe, partie 1 et partie 2.

YubiKeys et le YubiHSM créent une solide base de confiance dans un monde Zero trust.

Dans le monde Zero trust dans lequel nous vivons aujourd'hui, et, en particulier pendant et après la crise sanitaire de la Covid-19 où le travail à domicile et les politiques de travail hybride sont devenus la norme pour de nombreuses entreprises dans de nombreux secteurs, les RSSI doivent trouver un moyen d'activer une architecture Zero trust sans entraver la productivité des utilisateurs qui adoptent le travail à distance et utilisent les applications dans le cloud.

La solution de sécurité matérielle résistant au hameçonnage de Yubico - les clés YubiKey - prend en charge l'approche Zero trust, à savoir « N'ayez confiance en rien, vérifiez tout » avec une identité forte de l'utilisateur et une authentification du dispositif. Les clés YubiKey ont été conçues pour la sécurité et pour stopper le hameçonnage et d'autres formes de prise de contrôle de comptes, en fournissant une authentification forte à grande échelle.

Figure 4 : Risque de piratage de compte avec les YubiKey



Sur la base d'une étude Google réalisée sur 350 000 tentatives de piratage dans le monde réel[1]

1 Blog de sécurité Google - « Quelle est l'efficacité de l'hygiène de base des comptes pour prévenir les piratages ? », 17 mai 2019. Recherche basée sur 350 000 tentatives de piratages dans le monde réel. Les résultats affichés concernent les attaques ciblées.

S'appuyant sur les normes d'authentification modernes FIDO2/WebAuthn, les clés YubiKey fonctionnent de manière transparente dans les environnements sur site ou dans le cloud, ne repose pas sur des secrets partagés entre les services enregistrés, ne stocke aucune donnée et ne nécessite aucune connectivité mobile. En d'autres termes, les YubiKey peuvent fonctionner hors ligne, à tout moment et en tout lieu, en offrant une sécurité permanente à l'utilisateur et à son identité. Les clés YubiKey peuvent être remises facilement aux utilisateurs, qu'il s'agisse d'adresses professionnelles ou privées, pour une sécurisation efficace des collaborateurs travaillant à distance ou à distance et sur site. Et avec des clés de sécurité qui offrent un auto-enregistrement facile des utilisateurs et s'intègrent à votre infrastructure de sécurité existante, aux plateformes de gestion des identités et des accès et à des centaines d'autres services, les identités des utilisateurs peuvent être protégées en quelques minutes seulement. Avec les clés YubiKey, une entreprise peut bénéficier d'une sécurité forte, d'une expérience utilisateur simple et rapide, et d'un coût total de possession réduit.

La clé USB YubiHSM 2 est disponible et assureune sécurité matérielle de chiffrement sans compromis pour les applications, les serveurs et les dispositifs informatiques, à une fraction du coût et de la taille des HSM traditionnels.

Principales idées reçues sur le Zero trust

« Le Zero trust est un produit »

- Le Zero trust n'est pas un produit, mais une approche de conception et un cadre dans lequel plusieurs solutions peuvent jouer un rôle en travaillant ensemble pour garantir que l'accès aux données sensibles soit limité aux besoins et aux scores de risque.

« Il n'existe qu'une seule façon d'atteindre le Zero trust »

- Il existe de nombreux chemins pour mettre en œuvre un cadre Zero trust, et de nombreuses initiatives spécifiques peuvent exister dans le cadre général ou l'architecture Zero trust. En outre, le Zero trust est une approche de conception, de sorte que chaque projet à venir devrait être abordé sous cet angle.
- Cependant, une excellente façon de commencer le voyage vers le Zero trust est de s'assurer que tous les utilisateurs accédant au réseau sont fortement vérifiés et que le mécanisme d'authentification qu'ils utilisent est fiable.
- Attention, à ne pas oublier ! Malgré tous les autres contrôles mis en place pour soutenir le Zero trust, si l'utilisateur accédant au réseau ou aux données n'est pas digne de confiance, l'ensemble du modèle s'effondre.

« Le Zero trust est seulement pour les utilisateurs privilégiés »

- Dans toute entreprise qui a des données à protéger contre des menaces internes ou externes, chaque utilisateur doit être considéré comme un utilisateur privilégié, et pas seulement les quelques rares personnes qui occupent des rôles importants ou visibles.
- Dans les entreprises hyper connectées et flexibles d'aujourd'hui, les données sensibles peuvent se trouver à plusieurs endroits et être accessibles à plusieurs niveaux de l'entreprise.
- Par conséquent, une entreprise devrait vérifier chaque utilisateur, et pas seulement ceux qui sont considérés comme « privilégiés » en utilisant une définition étroite.

« Le Zero trust est seulement pour les grandes entreprises »

- Le Zero trust est applicable aux entreprises de toutes tailles.
- Il est certainement pertinent pour les grandes entreprises où différents types d'utilisateurs accèdent à différents systèmes depuis n'importe où, mais ce cadre et cette approche de conception ne sont pas relégués aux seules grandes entreprises.
- En effet, le concept du Zero trust peut être encore plus pertinent pour les PME, compte tenu de leurs environnements lourds d'applications dans le cloud.

« Le Zero trust est seulement pour les entreprises dans les secteurs réglementés ou à haut risque »

- Le Zero trust n'est pas seulement destiné aux entreprises qui ont des mandats de conformité spécifiques pour assurer la sécurité des données ou du réseau.
- Toute entreprise qui a des données sensibles ou une propriété intellectuelle à protéger devrait envisager d'adopter un modèle Zero trust, étant donné l'évolution constante du paysage des menaces avec des vecteurs de risque plus importants.

« Le Zero trust deviendra moins pertinent à mesure que les utilisateurs retourneront au bureau »

- On peut affirmer sans risque de se tromper que ce ne sera pas le cas.
- Alors que la crise sanitaire due à la Covid-19 s'atténue, que le retour au bureau peut se faire en toute sécurité et que les entreprises adoptent un modèle de travail hybride, le Zero trust restera tout aussi pertinent car les utilisateurs seront amenés, dans un avenir prévisible, à travailler de n'importe où.

Conclusion

La mise en œuvre d'une architecture Zero trust peut être un processus long et complexe. Déployez l'authentification forte dès le départ comme une base solide lors de l'élaboration de votre stratégie Zero trust et pendant que vous vous lancez dans l'aventure. Les solutions d'authentification forte ont fait leurs preuves depuis des années et peuvent renforcer votre posture de sécurité rapidement et facilement. De nombreux défis de déploiement liés à la sécurité matérielle ont été considérablement améliorés avec FIDO. De plus, Yubico a révolutionné et boosté l'utilisation des cartes à puce grâce à sa technologie facile à utiliser. De cette manière, l'authentification forte peut vous donner une victoire précoce alors que vous déployez votre initiative plus large du Zero trust. Bien que la mise en place d'un cadre plus large du Zero trust puisse prendre un certain temps, les entreprises peuvent rapidement établir une authentification des utilisateurs de confiance qui est fondamentale pour un cadre Zero trust. Concentrez-vous sur le déploiement d'une MFA moderne et pas seulement d'une MFA « suffisante », car le paysage des menaces ne fait que devenir plus sophistiqué et envisager une solution à l'épreuve du temps est l'approche architecturale appropriée. Avec les MFA modernes utilisant des clés de sécurité matérielles, l'attestation de l'authentificateur renforce la confiance dans la protection des clés privées, et offre une sécurité contre les menaces malveillantes externes et les attaques internes. Enfin, associer une authentification forte à une facilité d'utilisation pour l'utilisateur est une combinaison puissante. Une MFA moderne peut offrir aux utilisateurs une expérience de connexion sans mot de passe, en réduisant les frictions des utilisateurs, avec moins d'appels au service d'assistance et des économies significatives pour l'entreprise. En somme, le Zero trust est sans aucun doute un parcours complexe. Facilitez-vous la tâche en pensant d'abord à l'authentification forte et en ajoutant la puissance de la MFA moderne et du sans mot de passe à votre liste de présélection de la stratégie Zero trust.

yubico

About Yubico

Yubico établit de nouvelles normes mondiales pour un accès simple et sécurisé aux ordinateurs, aux appareils mobiles, aux serveurs et aux comptes Internet.

L'invention principale de l'entreprise, la YubiKey, offre une protection matérielle solide, d'une simple pression, sur un grand nombre de systèmes informatiques et de services en ligne. Le YubiHSM, le module de sécurité matériel ultra-portable de Yubico, protège les données sensibles stockées dans les serveurs.

Yubico est l'un des principaux contributeurs aux normes d'authentification ouverte FIDO2, WebAuthn et FIDO Universal 2nd Factor. La technologie de la société est déployée et appréciée par 9 des 10 premières marques Internet et par des millions d'utilisateurs dans 160 pays.

Fondée en 2007, Yubico est une société privée, avec des bureaux en France, en Suède, au Royaume-Uni, en Allemagne, aux États-Unis, en Australie et à Singapour. Pour plus d'informations : www.yubico.com.