Image: D3Damon / iStock

Dossier

Cloud Access Security Broker

en collaboration avec **BOLL**

Cybersécurité dans le cloud

osc. C'est l'une des promesses publicitaires les plus fréquemment entendues de la part des hyperscalers. Les grands fournisseurs de cloud public comme Amazon Web Services, Microsoft ou Google ne se lassent pas de souligner à quel point leurs plateformes sont sécurisées. Et à première vue, cela semble vrai. Les entreprises américaines emploient des légions d'informaticiens pour assurer la cybersécurité d'Azure, GCP, etc. Une petite entreprise ne peut pas rivaliser avec un tel dispositif.

Mais un regard plus attentif révèle que la sécurité dans les environnements cloud n'est pas du tout une évidence. Si les plateformes et l'infrastructure peuvent être sécurisées par le fournisseur, les dangers se cachent dans les détails. Aujourd'hui, de nombreuses applications cloud fonctionnent en parallèle dans l'entreprise, parfois sans que le département IT ne soit au courant. Les applications sont exploitées en mode as-a-Service, et les employés accèdent aux données de l'organisation sur le chemin du travail ou en home office. Tout cela doit être sécurisé et conforme aux règles de protection des données. Les fournisseurs de services cloud ne fournissent que la base, ce qui s'y passe relève de la responsabilité du client.

Comment garantir dès lors la sécurité au niveau de l'utilisateur? Dans les pages qui suivent, Joachim Walter, directeur général de BOLL, présente une approche prévue à cet effet: le «Cloud Access Security Broker» (CASB). Ces solutions opèrent entre les terminaux d'une organisation et le cloud, et assument en quelque sorte une fonction de gardien des applications et des données. Joachim Walter explique les fonctionnalités du CASB, la manière dont l'utilisateur peut les mettre en œuvre, et en donne un exemple en interview.

Comment sécuriser l'utilisation du cloud

Tous les utilisateurs des applications cloud doivent être particulièrement attentifs aux données transmises. Après tout, la sécurité des données demeure la responsabilité de l'entreprise. Les solutions CASB (Cloud Access Security Broker) aident à protéger les données et à utiliser les applications cloud sans hésitation.

L'AUTEUR

Joachim Walter
Directeur Général de
BOLL Europe

De plus en plus d'entreprises utilisent des applications cloud. Le leader en Europe est Office 365 – Microsoft fait la promotion de ses services de bureautique sur le cloud depuis des années et connaît un succès considérable. D'autres applications SaaS sont également très populaires, telles que Salesforce et ServiceNow. Les grandes entreprises utilisent également des centaines d'applications cloud. Certaines d'entre elles n'ont pas été introduites par le service informatique, mais sont utilisées par les employés sous la forme de «shadow IT».

De même que pour l'exploitation d'applications qui étaient auparavant hostées sur site ou développées en interne, les entreprises progressistes utilisent de plus en plus les plateformes IaaS telles que AWS, Azure ou Google Cloud.

Toute stratégie multi-cloud se heurte à un défi fondamental: bien que les plateformes cloud soient hautement sécurisées, le traitement des applications et surtout des données gérées avec elles reste la responsabilité de chaque organisation utilisant des applications cloud. Cela de manière officielle: le règlement général sur la protection des données (RGPD) de l'UE et les exigences de conformité spécifiques à l'entreprise stipulent qu'il doit être possible de vérifier à tout moment quelles données sont traitées, quand, par qui, à quel endroit et où elles sont stockées.

La sécurité au-delà du réseau d'entreprise

Les systèmes de sécurité traditionnels tels que les pare-feu ne résolvent pas ce problème. Pour ce faire, il faut faire appel à des solutions Cloud Access Security Broker (CASB). En tant qu'interface entre les applications cloud et les terminaux, les solutions CASB fournissent une visibilité complète et une protection des données globale dans toutes les applications cloud – y compris les développements internes et les applications tierces exploitées sur un cloud IaaS. Les solutions CASB sont souvent mises en œuvre en tant que service cloud et peuvent ensuite être utilisées de manière productive en très peu de temps. Même dans les environnements les plus vastes, le déploiement ne prend généralement que quelques jours.

Parmi les fonctions de base d'un CASB figurent la reconnaissance de toutes les applications en ligne utilisées et le contrôle de celles qui sont autorisées et de celles qui ne le sont pas. Le CASB bloque l'accès à une application non autorisée, permet l'approbation individuelle par l'administrateur si nécessaire ou suggère des alternatives autorisées. En outre, le CASB devrait identifier les applications cloud problématiques sur la base des informations de menaces et de Machine Learning, comme celles qui présentent des failles de sécurité ou un comportement malveillant, afin de les bloquer automatiquement.

La protection des données est essentielle

Toutefois, le travail d'un CASB n'est pas uniquement le contrôle d'accès spécifique à une application. Une autre fonction importante est la protection contre la perte de données – et celle-ci doit couvrir tous les emplacements ainsi que tous les dispositifs, ce qui n'est pas le cas des solutions de prévention des pertes de données basées sur la localisation: Celles-ci sont impuissantes une fois que les données ont quitté le réseau de l'entreprise. Lorsqu'il est intégré au CASB, le mécanisme DLP peut surveiller et contrôler tout le trafic vers le cloud en fonction des directives données – soit automatiquement, basé sur un ensemble de règles pour des types de données spécifiques, soit individuellement, jusqu'à l'autorisation ou l'interdiction du trafic en fonction de mots clés. Par exemple, un numéro de carte de crédit contenu dans un document est automatiquement reconnu et numériquement «masqué».

Les données sont mieux protégées si elles sont cryptées avec des certificats spécifiques à l'entreprise avant d'être transférées sur le cloud, si possible même deux fois avec les algorithmes d'encryption les plus sûrs tels que AES256. C'est à partir de ces conditions-là que nous pouvons garantir que l'exploitant de la plateforme cloud ne pourra pas accéder aux données. Idéalement, la fonction de cryptage est intégrée dans le CASB et permet de saisir à la fois des données structurées, comme dans Salesforce, et des fichiers de tout type.

Gestion intégrée des identités et des accès

La méthode la plus simple et la plus sûre d'utiliser le cloud est que le CASB agisse simultanément en tant que fournisseur d'identité

(Identity-as-a-Service), non seulement pour les services SaaS du cloud public, mais aussi pour vos propres applications et services fonctionnant sur un cloud IaaS. La sécurité du cloud est alors regroupée sur une seule plateforme. Les fonctionnalités d'IaaS comprennent l'authentification unique (Single-Sign-on) pour toutes les applications cloud, la synchronisation avec Active Directory, la prise en charge des systèmes de gestion d'identité inter-domaines (SCIM), l'intégration avec d'autres systèmes de gestion d'identité et l'authentification multi facteurs.

Le CASB comme base pour le BYOD et le Home Office

Avec toutes ces fonctions, un CASB est parfaitement adapté aux scénarios de home office qui sont particulièrement d'actualité aujourd'hui: L'entreprise conserve le contrôle du flux de données et des applications cloud, qu'il s'agisse d'appareils d'entreprise ou privés. Dès que des appareils privés sont intégrés au réseau de l'entreprise, une solution CASB est indispensable. La raison est la suivante: certains projets BYOD échouent parce que les employés ne veulent pas permettre l'installation d'une solution de gestion des appareils mobiles sur leurs appareils. Selon une enquête réalisée par un prestataire CASB, 57 % des employés des entreprises interrogées rejettent cette idée.

Par conséquent, l'objectif d'une stratégie de BYOD ou de home office ne doit pas être le contrôle total des appareils, mais plutôt la sécurisation des données et des applications professionnelles qui y sont utilisées, ce qui relève à son tour de la compétence des solutions CASB. Plus important encore, le CASB devrait également être en mesure de le faire sans installer d'agent sur les dispositifs. Seule une approche sans agent ne porte pas atteinte à la vie privée de l'utilisateur et ne charge pas l'appareil en termes d'utilisation du processeur et de durée de vie de la batterie.

Les utilisateurs peuvent continuer à utiliser leurs applications préférées tout en restant conformes, car seules les données dont l'utilisation est approuvée peuvent accéder à l'appareil – et uniquement sous forme cryptée et sécurisée par l'authentification de chaque application, qui est configurée pour communiquer avec le CASB. Idéalement, le CASB offre également la possibilité de bloquer sélectivement l'accès aux données d'entreprise si un appareil est perdu ou si un employé quitte l'entreprise. En conclusion: qu'il s'agisse de home office ou de collaborateurs mobile, les organisations qui utilisent des applications cloud auront besoin d'une solution CASB dont les fonctionnalités sont aussi complètes que possible. C'est la seule façon de garantir que les données ne tombent pas entre de mauvaises mains. Une solution CASB de nouvelle génération est un élément essentiel de la stratégie de sécurité moderne Secure Access Service Edge (SASE), qui consolide et intègre les solutions de sécurité cloud sur une plateforme flexible de type «cloud-first».

«La plupart des entreprises savent qu'elles doivent agir en matière de sécurité cloud»

Les applications cloud sont de plus en plus souvent utilisées. Les solutions Cloud Access Security Broker sont utilisées pour assurer la sécurité des données. M. Joachim Walter, directeur général de BOLL Europe, présente une solution CASB particulièrement réussie. Interview: Oliver Schneider

Les applications cloud sont-elles par principe peu sûres?
Le cloud n'est pas nuisible en soi, mais il faut l'utiliser de manière judicieuse. Les utilisateurs d'applications cloud doivent être très prudents avec les applications et les données pour éviter les problèmes de sécurité. Si vous avez des utilisateurs répartis dans tout le pays, vous devez réfléchir à qui peut utiliser quelles données sur quel appareil. Un Cloud Access Security Broker (CASB) peut vous aider à cet égard.

BOLL a décidé de distribuer les solutions CASB de Bitglass. Quel a été le facteur décisif?
Bitglass possède plusieurs caractéristiques qu'aucun autre CASB ne propose actuellement. Dans l'ensemble, il s'agit du CASB le plus complet et le plus exhaustif. Gartner l'a reconnu et a nommé Bitglass leader du «Magic Quadrant for Cloud Access Security Brokers 2018». De plus, les solutions Bitglass sont adaptées pour servir de base à une stratégie SASE (Secure Access Service Edge) orientée vers l'avenir et le cloud.

Quelle est la particularité de la solution Bitglass?
Cela commence par le concept de base. Alors que d'autres CASB se concentrent sur la détection et l'activation ou le blocage d'applications cloud, Bitglass accorde une grande importance à l'identification, la classification automatique et la protection des données confidentielles.

Comment cela fonctionne?
La solution comprend des fonctionnalités telles que le filigrane des documents pour une surveillance granulaire du contenu transmis, un cryptage fort avant le transfert des données sur le cloud – avec possibilité d'encryption des champs et des fichiers, la prévention des pertes de données, ainsi que des services d'identité intégrés et, en option, la détection et la prévention avancées des menaces (Advanced Threat Prevention).

Bitglass couvre également les appareils qui ne sont pas gérés par l'entreprise …
Correct. La couche d'abstraction de la machine virtuelle AJAX, que seul Bitglass propose, permet de protéger les données sur les appareils mobiles sans avoir à installer un agent comme cela serait nécessaire avec les solutions de GDR classiques – idéal pour BYOD, qui ne fonctionne vraiment que si elle peut être mise en œuvre sans agents.

«Des pare-feu seront toujours nécessaires, mais moins qu'auparavant.»

Joachim Walter, directeur général de BOLL Europe

À qui s'adresse Bitglass?
En bref, pour toutes les organisations à partir d'une centaine d'utilisateurs. Mais aussi les très grands environnements: Pour le plus gros client, une université américaine comptant 200 000 utilisateurs. Les coûts sont gérables. L'édition standard pour trois applications, par exemple Office 365, Salesforce et ServiceNow, coûte environ 100 CHF par utilisateur et par an.

Qui sont les concurrents?
Les principaux concurrents sont Netskope, McAfee et Symantec. Ils sont tous issus de la sécurité IT et savent donc tous comment identifier les applications cloud qui sont utilisées mais ils sont moins forts pour résoudre le problème de la sécurité des données. Microsoft a récemment ajouté MCAS comme nouvelle solution.

Comment se développe le marché de BOLL et Bitglass?
C'est une solution très prometteuse. Si nous participons à une évaluation, nous avons de bonnes chances de remporter le projet. De plus, nous avons de nombreuses demandes de clients – y compris de grandes entreprises avec des dizaines de milliers d'utilisateurs.

Le CASB remplacera-t-il les systèmes de sécurité traditionnels?
Partiellement seulement. Des pare-feu seront toujours nécessaires, mais moins qu'auparavant. Pour les distributeurs et les revendeurs, le CASB peut même devenir une extension de leur activité: La plupart des entreprises savent qu'elles doivent agir en matière de sécurité cloud.