Les 7 vérités cachées sur la sécurité du cloud

WITH secure

Sommaire

Introduction

Il y a près de vingt ans, le cloud computing a fait d'un rêve utopique une réalité. Désormais, des entreprises aux ressources limitées peuvent faire concurrence à des organisations d'envergure, mieux équipées et mieux financées. Quant à ces mastodontes, ils bénéficient eux aussi de la liberté et de la flexibilité du cloud.

Le rêve du cloud est devenu réalité, mais ce rêve a un prix. Il existe de fortes implications sur le plan de la sécurité organisationnelle, et les entreprises doivent veiller à bien les comprendre.

Bien entendu, le « cloud » renvoie à de nombreux concepts. Il y a, par exemple, les infrastructures-as-a-service (IaaS) et les plateformes-as-a-service (PaaS) : nous en dépendons tous mais les utilisateurs finaux ignorent jusqu'à leur existence. Il y a aussi les outils SaaS (Software-as-a-Service) tels que Microsoft 365 et Salesforce, que beaucoup de professionnels utilisent au quotidien.

Toutes ces variantes du cloud ont un point commun : elles impliquent une responsabilité partagée du point de vue de la sécurité. Les clients sont responsables des aspects de sécurité que les fournisseurs cloud excluent de leurs contrôles de sécurité intégrés.

Le cloud pose de nombreux défis en termes de sécurité, et souvent, les entreprises n'en prennent la mesure que lorsqu'une violation de données se produit. En réalité, très peu d'entreprises peuvent se permettre d'assurer seules leur cyberprotection sur le cloud.

Voici sept vérités cachées sur la sécurité du cloud en 2022. Nous souhaitons vous montrer ici comment les entreprises se réorganisent pour exploiter, sans entraves, tout le potentiel du cloud. Les avantages du cloud computing doivent être supérieurs aux risques[1]. Et dans cette optique, les entreprises doivent adopter une approche axée sur les résultats.

« Je ne serais en mesure de citer qu'une ou deux entreprises capables de détecter elles-mêmes les attaques cloud. Un tel travail exige de mobiliser des ressources significatives en interne. C'est parfait pour une banque d'envergure internationale, moins pour 99,5 % des entreprises possédant des ressources plus limitées. »

Nick Jones,
Principal Security Consultant, WithSecure™

1. https://www.f-secure.com/gb-en/consulting/our-thinking/cloud-security-striking-the-balance

Vérité cachée n°1

Il est impossible de protéger quelque chose qu'on ne voit pas

W / T H
secure

Vérité cachée n°1

Il est impossible de protéger quelque chose qu'on ne voit pas

Ishan Singh-Levett
Director, Product Management

Il est impossible de protéger quelque chose qu'on ne voit pas. Et dans le cloud, les équipes informatiques font face à un défi de taille : le shadow IT.

Le succès du cloud est lié à sa grande flexibilité : cette technologie facilite grandement l'acquisition d'espace de stockage, de performances et d'applications. Résultat : le BYOC (Bring Your Own Cloud) est venu rejoindre le BYOD (Bring Your Own Device). Ce phénomène complique la tâche des services informatiques et des équipes de sécurité, qui peinent à déterminer quelles ressources cloud sont utilisées, et à quels endroits.

Même sans prendre en compte les applications SaaS, il est très difficile d'identifier les ressources cloud déployées au sein d'un environnement professionnel. N'importe quelle équipe peut créer, avec une simple carte de crédit, des instances cloud contenant des données et des systèmes sensibles. Certaines de ces instances cloud - mais pas toutes - peuvent être difficiles à identifier et à monitorer. Des dépendances peuvent alors survenir entre le BYOC connu, le cloud approuvé par l'entreprise et le BYOC invisible et dangereux.

Les équivalents on-premise peuvent être repérés plus facilement, par le biais d'agents et de scans. Ce problème de visibilité du cloud est particulièrement palpable en environnement de développement, où il est fréquent de lancer des instances cloud, de déployer des données de production et de créer des liens vers des systèmes internes, avec un minimum de contrôle et de procédures de sécurité. Sans parler du fait qu'outre ces problèmes de sécurité et de confidentialité, de nombreuses entreprises paient leurs services cloud à des tarifs déraisonnables.

Affronter la vérité

Du fait de l'adoption massive et non structurée du cloud, des services ou employés isolés peuvent détenir des clouds individuels. Ces clouds peuvent manquer d'une configuration cohérente.

Un CASB (Cloud Access Security Broker) permet de savoir qui accède à quels services cloud, et depuis quel endroit. Les entreprises utilisent le CASB comme proxy d'interception, de manière à obtenir un niveau de compréhension supplémentaire. Le CASB est un outil polyvalent et très utile, mais des solutions mono-cloud telles que Cloud Protection for Salesforce de WithSecure™ peuvent offrir, sur un mode plus simple, le même type de protection. Le CASB nécessite par ailleurs un accès aux endpoints pour installer des agents, tout comme les solutions EDR (Endpoint Detection and Response) et MDR (Managed Detection and Response).

Vérité cachée n°2

Les erreurs de configuration cloud sont partout

WITH secure

Vérité cachée n°2

Les erreurs de configuration cloud sont partout

Nick Jones
Principal Security Consultant

Du fait de sa flexibilité et de son accès public, le cloud doit impérativement être bien configuré pour rester sécurisé. Face à un cloud mal configuré, même les hackers les moins compétents peuvent devenir dangereux.

Les fournisseurs cloud ont simplifié le processus de sécurisation des environnements qu'ils proposent. N'importe quel service informatique est désormais en mesure d'obtenir une configuration parfaite pour un compte individuel à charge de travail unique. Et grâce à plusieurs années d'expérience, les grands fournisseurs cloud disposent tous d'une excellente documentation et d'outils permettant d'identifier les problèmes de base.

La tâche se complique lorsqu'il s'agit de sécuriser plusieurs comptes, des centaines de charges de travail et plusieurs fournisseurs cloud. Les entreprises utilisent généralement trois à cinq fournisseurs cloud[2] : le problème est donc plus que courant.

Il existe des outils et des services permettant de sécuriser des environnements multiples, mais pour satisfaire à une stratégie de sécurité donnée et s'adapter aux charges de travail en constante évolution, ces outils et services doivent, eux aussi, être bien configurés. Ils doivent également pouvoir être utilisés par les professionnels chargés de détecter les intrusions. Même si les entreprises sont capables de définir une stratégie en ce sens, elles n'ont souvent pas les moyens de la mettre en œuvre[3].

De rares organisations, comme les grandes institutions financières mondiales, disposent des ressources et de l'expertise nécessaires pour développer d'importantes capacités en interne. Mais celles-ci ne représentent qu'un infime pourcentage des entreprises qui utilisent le cloud.

De nombreuses équipes parviennent toutefois à établir des configurations adaptées, soit en appliquant des politiques de sécurité standard à un petit nombre de fournisseurs, soit en consacrant beaucoup de temps à des configurations complexes.[4]

2. https://www.cio.com/article/228677/it-governance-critical-as-cloud-adoption-soars-to-96-percent-in-2018.html

3. https://www.withsecure.com/en/expertise/campaigns/detect-to-respond

4. https://www.f-secure.com/en/business/resources/webinar-replay-cisos-step-up-on-cloud-and-cyber-priorities-for-2022

En tout état de cause, définir des configurations cloud à grande échelle tient du défi : ce travail nécessite une collaboration étroite entre les responsables de la sécurité et les ingénieurs qui créent les charges de travail.

Les fournisseurs proposent certes des outils et des conseils, mais face à un nombre de clients considérable, ils ne peuvent fournir qu'un accompagnement d'ordre général. Pour des entreprises qui possèdent chacune un environnement unique, composé de plusieurs clouds et configurations, cette aide ne constitue pas une réponse à elle seule.

La licence créative que les fournisseurs cloud proposent aux utilisateurs participe au succès du cloud, mais elle constitue aussi un défi du point de vue de la sécurité. Une mauvaise configuration dans un environnement donné peut s'avérer tout à fait correcte dans un autre : les mauvaises configurations sont de ce fait particulièrement difficiles à repérer avec des outils automatisés. Il n'existe d’ailleurs pas d'outil de diagnostic unique capable de combler toutes les lacunes de sécurité d'un environnement. Le problème exige une approche plus humaine : il est ainsi préférable de disposer de quelques professionnels compétents plutôt que d'un éventail d'outils de diagnostic rigides.

Affronter la vérité

Si la solution à ce problème vous semble familière, c'est peut-être parce que les entreprises de conseil spécialisées, les fournisseurs de réponse aux incidents et les fournisseurs de services MDR ont résolu ce problème depuis très longtemps pour l'informatique on-premise.

La sécurité cloud s'accompagne certes de ses propres défis, mais de nombreuses techniques existantes peuvent être adaptées pour surmonter ces difficultés.

Les conseils d'experts indépendants (tels que les consultants en sécurité du cloud de WithSecure™) associés à des services MDR dotés de capacités de gestion de sécurité cloud (comme F-Secure Countercept) apportent une solution efficace : ils permettent de combler le vide existant entre les mesures de sécurité prises par les fournisseurs cloud et celles prises par les entreprises.

Vérité cachée n°3

Le cloud a changé la donne

W / T H
secure

Vérité cachée n°3

Le cloud a changé la donne

Jennifer Howarth
Product Manager - Cloud

À mesure que les entreprises passent au cloud et aux applications as-a-service, les attaques d'identifiants augmentent. Pourquoi ? Parce que dans le cloud, la surface d'attaque est fondamentalement différente de celle des environnements traditionnels on-premise, dans lesquels les endpoints[5] constituent la cible d'attaque la plus évidente et le principal objet des mesures de protection.

À l'exception de l'IaaS, où le cloud est essentiellement utilisé comme data center hors-site pour héberger des instances virtuelles, les charges de travail du cloud n'exposent pas les systèmes d'exploitation aux potentielles attaques. Résultat : les exploits et les exécutions de code deviennent sans effet ; et les mesures défensives affinées au fil des ans pour les contrer perdent en pertinence. Pour attaquer, les hackers procèdent donc en appelant l'API du cloud avec des identifiants légitimes. D'un point de vue défensif, il n'y a rien d'intrinsèquement malveillant dans chacun de ces appels API, mais une séquence d'appels qui ne correspond pas au fonctionnement normal pour un utilisateur ou pour une charge de travail particulière peut éveiller des soupçons. C'est là qu'intervient l'analyse du comportement des utilisateurs et des entités (UEBA).

L'UEBA permet de décrire le fonctionnement normal pour une charge de travail donnée, un environnement particulier, et éventuellement un utilisateur spécifique. En environnement on-premise, définir les comportements normaux et anormaux permet d'aider aux détections. Dans le cloud, ce procédé est la base-même d'un monitoring efficace. Et cette détection basée sur les identifiants ne concerne pas seulement les identifications humaines. Les utilisateurs sont un excellent point de départ pour le monitoring des SaaS, mais pour les services cloud bruts, les identifications de système à système sont tout aussi importantes. Des incidents récemment traités par l'équipe de réponse aux incidents de WithSecure™ ont révélé que, pour causer des ravages, les hackers recherchaient les identifiants-machine plutôt que les comptes des utilisateurs finaux.

Le cloud apporte avec lui de nouvelles technologies et de nouvelles méthodes. Et les entreprises ont dû apprendre à se défendre autrement[6].

5. https://www.f-secure.com/gb-en/consulting/our-thinking/detecting-attacks-in-the-cloud

6. https://www.f-secure.com/gb-en/consulting/our-thinking/how-the-cloud-has-changed-response

Certaines nouvelles attaques affectant la couche de gestion cloud ne nécessitent d'interaction avec aucune infrastructure traditionnelle on-premise. Les entreprises doivent donc impérativement mettre en place des mécanismes de détection et de réponse spécifiques au cloud. L'équipe de réponse aux incidents de WithSecure™ traite de plus en plus d'enquêtes portant uniquement sur le cloud, et d'après nous, cette tendance devrait s'accentuer.

Affronter la vérité

La sécurisation du cloud représente actuellement un défi. Les renseignements sur les menaces sont rares ou inexistants ; les données sont difficiles à collecter ; le volume et l'ampleur des attaques connues sont encore faibles ; et les entreprises qui ont été durement touchées par ces attaques sont réticentes à s'exprimer. Il existe toutefois plusieurs raisons de rester optimiste.

La détection des menaces s'adapte. Grâce à l’ajustement minutieux des fonctionnalités existantes aux plateformes cloud, les experts forensiques et les spécialistes de la réponse aux incidents (DFIR) peuvent intervenir dans le cadre d'incidents cloud.

MITRE[8] travaille activement à intégrer davantage de renseignements sur les menaces cloud dans son cadre d'attaque (même si, pour le moment, les fournisseurs et experts en cybersécurité sont contraints d'adopter une approche expérimentale).

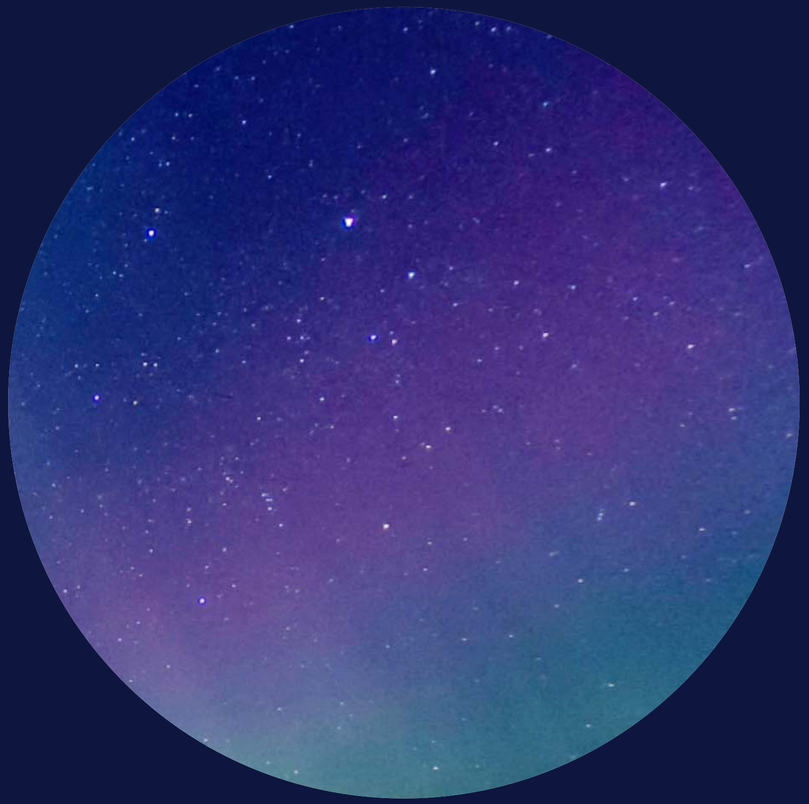
Découvrez comment l'équipe de réponse aux incidents de WithSecure™ travaille avec le cloud. Nous menons un travail de préparation stratégique et ajustons les fonctionnalités existantes aux plateformes cloud[9].

8. https://attackevals.mitre-engenuity.org/enterprise/participants/f-secure/?adversary=carbanak_fin7

9. https://www.f-secure.com/gb-en/consulting/our-thinking/how-the-cloud-has-changed-response

Vérité cachée n°4

Il reste essentiel de bien protéger les endpoints



WITH secure

Vérité cachée n°4

Il reste essentiel de bien protéger les endpoints

Harri Ruusinen
Director, Global Sales Engineering

Les services cloud se généralisent et la surface d'attaque augmente. Dans la mesure où les postes de travail et autres appareils constituent des points d'entrée vers le cloud, ils doivent impérativement rester protégés. Les systèmes EDR continuent donc là de jouer un rôle-clé.

Les services cloud sont généralement conçus avec différents niveaux de sécurité. Par exemple, l'authentification multifactorielle (MFA) empêche les hackers d'accéder aux systèmes via des identifiants volés. Pour autant, si l'appareil utilisant ce service est piraté à distance ou bien volé, la session peut rester active : le hacker pourra donc contourner ce contrôle de sécurité supplémentaire. Cette absence de MFA ou de chiffrement sur les endpoints est un problème : si le hacker a pu accéder aux ressources qu'il convoite, la responsabilité incombera à l'entreprise, et non au fournisseur cloud. L'EDR reste donc vital pour protéger les appareils utilisés pour accéder aux services cloud de l'entreprise.

Affronter la vérité

La protection des endpoints et les solutions EDR sont plus importantes que jamais pour améliorer la cyber-résilience globale des entreprises. Heureusement, de nombreuses entreprises disposent déjà ces outils.

L'EDR permet aux équipes de sécurité d'identifier les comportements malveillants et anormaux, et de conserver un enregistrement de toutes les actions menées depuis les endpoints. Cette approche reste essentielle mais elle doit s'adapter pour jouer également son rôle dans le processus de sécurisation du cloud. WithSecure™ étudie cette question avec attention, car le monitoring simultané de tous les environnements constitue un défi de plus en plus grand.

L'EDR doit être optimisé pour mieux détecter les vols d'identifiants cloud à partir des endpoints : une alerte doit pouvoir être déclenchée dès le premier point d'entrée. Celle-ci doit ensuite être corrélée avec les anomalies de l'UEBA du cloud, afin de détecter immédiatement les tentatives d'accès au cloud via un endpoint piraté.

Chez F-Secure, nous veillons à ce que notre EDR puisse rendre compte efficacement de la posture de sécurité de l'entreprise (notamment de l'utilisation des fonctions de sécurité matérielle). L'objectif est de rendre aussi difficile que possible les piratages et les propagations sur les endpoints de nos clients.

Le système EDR est loin d'être mort et enterré : il reste essentiel pour sécuriser les endpoints, et empêcher les hackers d'accéder au cloud.

Chez F-Secure, nous prédisons pour l'avenir une plus grande synergie entre l'EPP/EDR et la sécurité cloud. Cette synergie permettra à nos clients et partenaires d'adopter de nouvelles méthodes de travail tout en maintenant leur résilience.

Pour plus de conseils sur les aspects essentiels d'une configuration EDR adaptée au cloud, consultez notre guide : *Les 10 éléments à prendre compte au moment d'acquérir une solution EDR*[10].

10. https://www.f-secure.com/en/business/resources/10-things-to-consider-before-buying-an-edr-solution

Vérité cachée n°5

Une protection fractionnée perd en efficacité

W / T H
secure

Vérité cachée n°5

Une protection fracturée perd en efficacité

Domenico Gargano
Director, Technical Operations

Difficile d'imaginer une entreprise n'existant que sur le cloud : un point d'accès physique semble le minimum. Les entreprises sont donc vouées à être présentes à la fois physiquement et sur le cloud. Pour autant, il existe une fracture de sécurité entre le cloud et les applications locales, et cette fracture engendre une augmentation de la surface d'attaque. Ajoutez plusieurs clouds, et les problèmes se multiplient.

Combler cette faille de sécurité semble essentiel. Il est d'ailleurs fort probable que votre entreprise, consciemment ou non, prenne des mesures actives en ce sens.

L'approche « shift left » consiste à transférer la responsabilité de la sécurité aux développeurs[11]. Parallèlement, les RSSI deviennent des leaders au carrefour des différents services. Ces tendances témoignent du rapprochement entre services cloud et applications.

Dans ce cas, d'où vient initialement cette fracture ? Les fournisseurs cloud disposent de ressources colossales en matière de sécurité et possèdent les moyens de doter leurs clients de connaissances et d'outils décisifs. Mais le service s'arrête là.

Ils ne proposent à leurs clients aucun moyen de mettre sur pied une sécurité personnalisée sans augmenter le coût du cloud à un niveau prohibitif. Les fournisseurs cloud, qu'ils proposent des infrastructures ou des applications, opèrent à très grande échelle et doivent gérer de très nombreux utilisateurs. Des outils impressionnants et des configurateurs sont là pour aider les utilisateurs à sécuriser leur cloud, mais cela ne suffit pas.

11. https://www.f-secure.com/gb-en/consulting/our-thinking/tech-not-culture-is-key-to-devsecops

Défenses séparées, équipes séparées ?

Les consultants de WithSecure™ ont constaté qu'un nombre important d'entreprises gèrent un centre d'opérations de sécurité (SOC) distinct pour leur parc informatique cloud. Cette pratique, au succès mitigé, semble souvent aller de pair avec une autre difficulté : celle du recrutement et de la fidélisation des experts en sécurité cloud. Cette pénurie n'est pas nouvelle et s'inscrit dans un contexte de pénurie de compétences informatiques qui dure depuis déjà des dizaines d'années.

Les équipes cloud tendent à mettre en place leur propre sécurité, parfois en parallèle de la sécurité on-premise. Les consultants en sécurité cloud de WithSecure™ finissent même souvent par échanger davantage avec ces équipes car, bien souvent, elles comprennent mieux la sécurité cloud que les équipes de sécurité informatique traditionnelles. L'organigramme de la sécurité est ainsi plus fragmenté que par le passé.

Sans une bonne visibilité sur leur environnement, les entreprises peinent à identifier les anomalies ou à faire des recoupements… Et les hackers peuvent en tirer profit. Il est essentiel de pouvoir corréler les points de données de l'infrastructure on-premise et de l'infrastructure cloud afin d'obtenir une image complète des éventuelles activités de piratage. Ces corrélations augmentent les chances de détecter les menaces et d'y répondre.

L'enquête de WithSecure™ sur les activités de piratage de NOBELIUM a montré comment ce groupe était capable d'opérer des intrusions via un vecteur on-premise, puis de passer de ce vecteur au cloud, tout en maintenant sa présence et en collectant les informations qu'il recherchait.

Les chercheurs de Microsoft ont par ailleurs révélé en détail les approches utilisées par NOBELIUM pour voler des identifiants donnant accès aux services ADFS (Active Directory Federation Service). Grâce à ces identifiants, les hackers accédaient au cloud et pouvaient s'y maintenir[12].

WithSecure™ a reproduit cette approche dans le cadre d'exercices de red teaming et a constaté que, même si les entreprises supprimaient les implants on-premise, la Red team pouvaient maintenir sa présence dans les environnements cloud du client jusqu'à la fin de sa mission.

Sygnia a décrit comment, une fois les droits administrateurs ADFS obtenus, NOBELIUM piratait ensuite le certificat SAML (Security Assertion Markup Language) de la victime[13].

Cette attaque, baptisée « SAML doré », accorde aux hackers un accès sans réserve aux services reconnaissant les tokens SAML, et leur offre une persistance sur les services cloud et XaaS. Dans une alerte, le CISA a apporté des précisions[14] sur les techniques, tactiques et procédures (TTP) de NOBELIUM. Sans la possibilité de corréler les logs d'authentification ADFS avec les logs d'activité du cloud, les entreprises sont dans l'impossibilité de repérer quels utilisateurs ont accédé au cloud, si ces derniers n'ont pas eu à s'authentifier au préalable via le serveur ADFS des systèmes on-premise.

12. https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

13. https://www.sygnia.co/golden-saml-advisory

14. https://www.cisa.gov/uscert/ncas/alerts/aa21-008a

Sécuriser le pipeline de conception

Les équipes chargées de l'infrastructure et de la sécurité ne savent pas toujours comment interpréter des logs d'activités. À l'inverse, les équipes chargées des pipelines et autres outils de développement disposent de cette expertise essentielle. Dans les enquêtes réalisées au cours des deux dernières années par l'équipe de réponse aux incidents de WithSecure™, les erreurs de configuration liées à un DevOps décentralisé[15] ont constitué la cause principale d'intrusions cloud.

La solution consiste à intégrer très tôt la sécurité dans le cycle de développement. Pour y parvenir, les entreprises peuvent décentraliser les dépenses de sécurité en responsabilisant les fonctions commerciales. Par ailleurs, il leur faut bâtir de solides liens de communication entre l'équipe de sécurité et l'ingénierie cloud.

Une fois encore, notre équipe de réponse aux incidents a constaté que les RSSI opéraient souvent indépendamment du département informatique, et répartissaient les opérations de sécurité entre les différentes unités commerciales. Il ne s'agit alors plus de silos indépendants et mal connectés, mais d'équipes décentralisées et hautement connectées.

Tous les services engagés dans cette décentralisation doivent adopter une approche similaire du risque : une entité intermédiaire doit donc faire le lien entre les différentes unités.

Des maillons faibles inattendus

Les missions de conseil et de réponse aux incidents réalisées par WithSecure™ ont révélé que, mis à part dans des erreurs de configuration triviales, les actifs cloud tournés vers internet constituent rarement des maillons faibles. Ce sont plutôt les services, les applications et les outils que les entreprises utilisent pour mettre en place des clouds qui s'avèrent problématiques. Il peut s'agir de fournisseurs d'identifiants, des dépôts de code source, du code d'infrastructure, ou encore des outils de déploiement de services en production.

Les outils d'intégration et de livraison continues (CICD) tels que Jenkins offrent notamment des droits d'administration très importants : si un hacker parvient à y accéder, la bataille est perdue d'avance.

Affronter la vérité

Le changement de culture d'entreprise est ici la clé, et dans de nombreuses entreprises, ce changement est déjà en cours. Certains ajustements mineurs peuvent alors suffire pour orienter davantage la sécurité vers le cloud.

Il peut s'agir, par exemple, de décentraliser certaines tâches et dépenses de sécurité, pour responsabiliser les équipes commerciales, sous la houlette d'un RSSI indépendant de l'équipe informatique.

15. https://www.f-secure.com/gb-en/consulting/our-thinking/security-team-of-the-future

Vérité cachée n°6

Personne ne sait qui est responsable de la sécurité des données cloud

W / T H
secure

Vérité cachée n°6

Personne ne sait qui est responsable de la sécurité des données cloud

Dmitriy Viktorov
Head of Product and Technology, Cloud Solutions

« Les données sont le nouveau pétrole » : voilà une expression désormais bien connue. Les données constituent en effet un actif extrêmement précieux pour les entreprises. Le transfert de vos données dans le cloud nécessite donc une réflexion approfondie : vous devez veiller à conserver une visibilité et un contrôle adéquat. Et de nombreux détails doivent être pris en compte.

Lorsque vous achetez des services cloud, vous reportez une partie de la responsabilité de la sécurité des données sur le fournisseur. C'est justement l'un des intérêts du cloud. Mais vous devez vous rappeler qu'il est toujours de votre responsabilité de maintenir un certain niveau de sécurité. C'est ce que l'on appelle le modèle de responsabilité partagée.

Une fois encore, c'est une question de visibilité, et plus précisément, de visibilité des données. Vous devez savoir quel type de données vous possédez, comment elles sont classées, d'où elles proviennent, qui peut y accéder et où elles vont.

Si les données proviennent de sources externes et non fiables (comme les e-mails), vous devez bloquer les contenus malveillants et non-autorisés avant qu'ils n'atteignent les utilisateurs internes ou externes.

En cas d'exigences réglementaires, monitorez l'accès à vos données sensibles, soyez en mesure de savoir qui accède aux données, et disposez d'une piste d'audit.

Ne négligez pas les menaces d'initiés malveillants et les accès non-autorisés aux données. Comme l'explique la deuxième vérité cachée de ce livre blanc, les services cloud SaaS peuvent vite devenir très complexes, donnant lieu à de mauvaises configurations ou à des contrôles d'accès insuffisants. Et à leur tour, ces mauvaises configurations peuvent entraîner des violations de données.

Pensez également aux accès illégitimes aux données, via d'autres applications et services connectés au cloud SaaS, par le biais d'API. Si ces services sont mal configurés ou donnent plus d'autorisations qu'ils ne le devraient, ils peuvent aussi engendrer une violation. Quant aux API elles-mêmes, elles peuvent aussi être compromises, même si elles sont configurées correctement : les récentes attaques de la supply chain sont là pour en témoigner.

Affronter la vérité

Les services cloud SaaS tels que Salesforce, Microsoft 365, Google Workspace, etc. sont de plus en plus populaires. Ils deviennent de ce fait des cibles lucratives pour les hackers. D'après nos prévisions, les attaques n'auront pas toujours, à l'avenir, comme objectif de voler des données stratégiques stockées dans le cloud. Les pirates informatiques tenteront plutôt d'utiliser les services cloud comme tremplins, pour s'introduire sur le réseau des entreprises et attaquer d'autres systèmes internes et externes. Nous avons déjà observé des attaques de phishing et de ransomware menées via des services cloud. À mesure que les cybermenaces évoluent, WithSecure™ continue d'améliorer ses solutions et d'étendre ses capacités de détection et de réponse pour couvrir à la fois les endpoints et les plateformes cloud IaaS, PaaS et SaaS.

L'une de nos solutions existantes, WithSecure™ Cloud Protection for Salesforce[16], offre une protection en temps réel contre les virus, les chevaux de Troie et les ransomwares. Cette solution unique analyse l'ensemble des contenus partagés via le cloud Salesforce. Elle comble les failles de sécurité liées au partage des responsabilités dans le cloud. WithSecure™ Cloud Protection for Salesforce aide les clients utilisant Salesforce Sales, Service ou Experience Cloud, à prévenir ou stopper les attaques menées via des fichiers malveillants ou des URL de phishing[17]. Cette solution offre également une visibilité accrue et des analyses complètes des contenus consultés par des utilisateurs internes ou externes.

WithSecure™ Cloud Protection for Salesforce s'appuie sur une plateforme cloud de réputation des contenus et d'analyse des menaces appelée WithSecure™ Security Cloud. Le Security Cloud s'appuie sur plusieurs niveaux de technologies de pointe et sur un répertoire en constante évolution. Ce répertoire recueille des cyber-renseignements et des informations relatives aux menaces recueillies en temps réel, par des dizaines de millions de capteurs de sécurité situés dans le monde entier. Le Security Cloud constitue la pierre angulaire de nos produits primés de protection des endpoints, et d'autres solutions de protection de la collaboration cloud, telles que WithSecure™ Elements Collaboration Protection.

16. https://www.f-secure.com/en/business/resources/salesforce-data-security

17. https://withsecure.com/en/expertise/campaigns/disrupting-the-kill-chain-with-withsecure-cloud-protection-for-salesforce

Vérité cachée n°7

Les plateformes de collaboration sont vouées à gagner du terrain

W / T H
secure

Vérité cachée n°7

Les plateformes de collaboration sont vouées à gagner du terrain

Juha Högmander
Director, Technical Offering

Depuis deux ans, le télétravail est devenu la norme, et il est probable que ce mode de travail s'impose durablement pour certains.

Dans de telles conditions, les outils de collaboration jouent un rôle crucial. Les entreprises doivent pouvoir partager des documents, organiser des ateliers et des réunions en direct, et faire des présentations en toute sécurité. Malheureusement, les exercices de Red teaming de WithSecure™ ont toujours prouvé que les plateformes de collaboration et de communication en temps réel constituaient de vraies mines d'or pour les pirates informatiques qui tentent d'infiltrer l'environnement d'une entreprise. Ces outils collaboratifs doivent donc être sécurisés.

Parallèlement, la messagerie reste le plus grand vecteur d'attaque. Plus de la moitié des PME - 51 %[18] - ont subi une attaque au cours des deux dernières années. Ce chiffre témoigne d'un changement d'approche des cybercriminels : ils recherchent désormais des proies faciles, et ne prêtent que peu d'attention à la taille ou au secteur d'activité des entreprises visées. Les attaques automatisées par e-mails permettent des envois en masse. Elles sont peu coûteuses pour le pirate informatique, et lui garantissent un bon retour sur investissement.

Il est important que vos employés soient sensibilisés au phishing pour qu'ils sachent rester vigilants et éviter les clics dangereux. Pour autant, nous le savons tous : cette solution n'est pas infaillible. Et le phishing a grandement bénéficié de la quarantaine : sa fréquence a augmenté et on le retrouve dans 36% des intrusions informatiques, contre 25 % en 2020[19]. Les liens électroniques sont le principal vecteur de malwares dans les violations de données, et environ 46 % des malwares sont transmis par e-mail[20].

Loin de nous l'idée de restreindre les utilisateurs légitimes dans leur accès aux données… même s'il s'agirait d'un moyen efficace de sécurisation. Nous voulons plutôt empêcher les utilisateurs d'entreprendre des actions non autorisées, comme le partage de données confidentielles depuis des endroits inappropriés. Et nous voulons disposer de la visibilité nécessaire pour retracer les activités inhabituelles.

18. Ponemon. IBM. 2020. *Rapport Cost of a Data Breach*. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

19. Verizon. 2021. *Rapport Data Breach Investigations 2021*. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

20. Verizon. 2020. *Rapport Data Breach Investigations 2020* https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

Affronter la vérité

Microsoft 365 permet de prendre ces précautions et constitue de loin la plateforme la plus importante. C'est pourquoi WithSecure™ a donné la priorité au développement de sa solution WithSecure™ Elements Collaboration Protection[21], même si d'autres développements sont en cours, et si WithSecure™ Cloud Protection for Salesforce offre déjà une protection collaborative pour les utilisateurs de cet environnement.

Nous avons travaillé à l'amélioration de notre solution de protection de la messagerie pour protéger Sharepoint et Teams, et ainsi proposer une protection complète pour cette plateforme. Nous avons également intégré la détection des comptes piratés, qui joue un rôle essentiel dans la protection du service.

Dans le monde d'aujourd'hui, nous ne souhaitons pas devenir des agents de sécurité en lutte contre un monde enclin à l'ouverture. La transition technologique s'est étendue à l'ensemble de l'économie, et celle-ci doit donner aux êtres humains le pouvoir de prendre des décisions sur une base individuelle.

21. https://www.youtube.com/watch?v=rvzXvtXoyF8&t=1s

Conclusion

Les nouveaux outils et procédures de sécurité cloud n'ont qu'un intérêt limité, tant pour les fournisseurs de services cloud que pour les fournisseurs de sécurité et leurs clients.

En pratique, un changement de culture professionnelle s'avère bien plus efficace. Une approche de la sécurité adaptée, axée sur les résultats, peut démultiplier l'apport d'un bon outil ou d'une bonne technique.

En investissant pour créer une approche solide et décentralisée de la sécurisation cloud, vous réduirez les frais généraux cachés que le cloud peut engendrer.

À Propos de WithSecure™

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnement cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

WITH secure