Communiqués de presse

IBM : La sécurité dans le Cloud reste challengée par la complexité et le Shadow IT

De nouvelles données identifient les principaux risques de sécurité auxquels les entreprises doivent faire face alors que la migration vers le Cloud s'accélère

CAMBRIDGE, MA, le 11 juin 2020 : IBM Security a publié aujourd'hui de nouvelles données relatives à l'analyse des principaux défis et menaces qui pèsent sur la sécurité du Cloud. Il en ressort que la facilité et la rapidité avec lesquelles les nouveaux outils dans le Cloud peuvent être déployés peuvent également rendre plus difficile le contrôle de leur utilisation par les équipes de sécurité. Selon les données de l'enquête d'IBM et l'analyse des études de cas, les questions fondamentales de surveillance de la sécurité, notamment la gouvernance, les vulnérabilités et les mauvaises configurations, restent les principaux facteurs de risque auxquels les organisations devraient faire face pour aider à sécuriser des opérations de plus en plus basées sur le Cloud. L'analyse de cas des incidents de sécurité survenus au cours de l'année écoulée met également en lumière la manière dont les cybercriminels ciblent les environnements Cloud avec des logiciels malveillants personnalisés, des ransomwares et autres.

Pour les entreprises migrant rapidement vers le Cloud afin de répondre aux besoins de leurs employés travaillant à distance, il est essentiel de comprendre les défis spécifiques que pose cette transition en matière de sécurité pour gérer les risques. Si le Cloud permet de nombreuses fonctionnalités commerciales et technologiques essentielles, l'adoption et la gestion ad hoc des ressources Cloud peut également créer une complexité pour les équipes informatiques et de cybersécurité. Selon IDC, plus d'un tiers des entreprises ont acheté plus de 30 types de services Cloud auprès de 16 fournisseurs différents rien qu'en 2019[1] . Ce paysage distribué peut conduire à une appropriation peu claire de la sécurité dans le Cloud, créant des "angles morts" en matière de politique de sécurité, amenant à du shadow IT et donc finalement à de potentielles vulnérabilités et mis-configurations.

Afin d'avoir une meilleure idée de la nouvelle réalité en matière de sécurité, alors que les entreprises s'adaptent rapidement aux environnements hybrides et multiclouds, l'IBM Institute for Business Value (IBV) et l'IBM X-Force Incident Response and Intelligence Services (IRIS) ont examiné les défis spécifiques qui ont un impact sur les opérations de sécurité dans le Cloud, ainsi que les principales menaces ciblant les environnements Cloud.

Les principales conclusions sont les suivantes :

• **Appropriation complexe** : 66 % des personnes interrogées disent compter sur les fournisseurs de Cloud pour la sécurité ; Cependant, leur perception de qui fait quoi en termes de sécurité dans le cloud varie considérablement selon les plateformes et les applications Cloud étudiées[2].

• **Les applications Cloud ouvrent la porte** : La voie la plus courante utilisée par les cybercriminels pour compromettre les environnements Cloud sont les applications Cloud qui représentent 45 % des incidents dans les études de cas d'IBM X-Force IRIS liées au Cloud . Dans ces études de cas, les cybercriminels ont profité d'erreurs de configuration ainsi que de vulnérabilités au sein de ces applications restées non détectées car les employés les ont mises en place sans passer par les processus standards de mise en production.

• **Amplification des attaques** : Alors que le vol de données était le principal impact des attaques Cloud

étudiées[3], les pirates ont également ciblé le Cloud pour des attaques de type cryptomining et ransomwares[4] - en utilisant les ressources Cloud pour amplifier l'effet de ces attaques.

« *Le cloud offre un énorme potentiel d'efficacité et d'innovation pour les entreprises, mais il peut aussi créer un "Far West"* d'environnements plus vastes et distribués que les entreprises doivent gérer et sécuriser », a déclaré **Abhijit Chakravorty**, **Cloud Security Competency Leader**, I**BM Security Services.** *« Lorsqu'il est bien utilisé et configuré, le Cloud peut rendre la sécurité plus évolutive et plus adaptable. Mais les organisations doivent se défaire de leurs anciens réflexes et s'orienter vers de nouvelles approches de sécurité conçues spécifiquement pour cette nouvelle frontière technologique, en tirant parti de l'automatisation dans la mesure du possible. Cela commence par une image claire des obligations réglementaires et du mandat de conformité, ainsi que des défis de sécurité uniques, techniques et politiques, et des menaces externes ciblant le Cloud".*

Qui est responsable de la sécurité dans le Cloud ?

Une enquête de l'IBM Institute for Business Value a révélé que les organisations interrogées comptaient fortement sur les fournisseurs de Cloud pour s'occuper de la sécurité dans le Cloud, bien que les problèmes de configuration - qui sont généralement la responsabilité des utilisateurs - étaient le plus souvent à l'origine des fuites de données (représentant plus de 85 % de toutes les violations en 2019 pour les organisations interrogées) .

En outre, la perception de la responsabilité de la sécurité dans le Cloud par les organisations interrogées varie considérablement selon les plateformes et applications. Par exemple, la majorité des personnes interrogées (73 %) pensent que les fournisseurs de Cloud public sont les principaux responsables de la sécurisation du Software-as-a-Service (SaaS), tandis que 42 % seulement pensent que les fournisseurs sont les principaux responsables de la sécurisation de l'infrastructure-as-a-Service (IaaS).

Si ce type de modèle de responsabilité partagée est nécessaire pour les environnements Cloud hybrides et multicloud, il peut également entraîner des politiques de sécurité changeantes et un manque de visibilité à travers les différents Cloud. Les organisations capables de rationaliser les opérations de sécurité et Cloud peuvent réduire ce risque grâce à des politiques clairement définies qui s'appliquent à l'ensemble de leur environnement informatique.

Les principales menaces dans le Cloud : Vol de données, cryptomining et ranswomware.

Afin d'avoir une meilleure idée de la manière dont les attaquants ciblent les environnements Cloud, les experts en réponse aux incidents de l'X-Force IRIS ont effectué une analyse approfondie des cas liés au Cloud auxquels l'équipe a répondu au cours de l'année dernière[5].

Voici ce que l'analyse a révélé :

• **La catégorie de cybercriminels en tête des attaques** : Les cybercriminels motivés par les gains financiers sont la catégorie de groupes de menace ciblant les environnements Cloud la plus fréquemment observée dans les cas de réponse aux incidents d'IBM X-Force, bien que les acteurs étatiques constituent également un risque persistant.

• **Les attaques à travers les applications Cloud** : Le point d'entrée le plus courant pour les attaquants sont les applications Cloud, attaquées par « brute-force », exploitation des vulnérabilités ou mis-configurations. Les vulnérabilités sont souvent passées inaperçues en raison du shadow IT, lorsqu'un employé sort des processus établis de mise en production et déploie une application Cloud vulnérable. La gestion des vulnérabilités dans le Cloud pouvait être difficile car les vulnérabilités des services dans le Cloud sont restées en dehors du champ d'application des CVE traditionnelles jusqu'en 2020.

• **Les ransomwares dans le Cloud** : Les ransomwares ont été déployés trois fois plus que tout autre type de logiciels malveillants dans les environnements Cloud dans les cas étudiés de réponse aux incidents d'IBM, suivis des cryptominers puis des logiciels malveillants de type botnet.

• **Le vol de données** : Après le déploiement de logiciels malveillants, le vol de données a été la menace la plus courante qu'IBM a observée dans les environnements Cloud compromis au cours de l'année dernière, allant des informations d'identification personnelle (IIP) aux emails liés aux clients.

• **Les retours exponentiels** : Les attaquants ont utilisé les ressources Cloud pour amplifier l'effet d'attaques telles que le cryptomining et DDoS. De plus, les groupes d'attaquants ont utilisé le Cloud pour héberger leurs infrastructures et opérations malveillantes, ajoutant ainsi un facteur d'échelle et une couche supplémentaire d'obscurcissement pour rester non détectés.

« D'après les tendances observées dans nos cas de réponse aux incidents, il est probable que les logiciels malveillants ciblant le Cloud continueront à se développer et à évoluer à mesure que l'adoption du Cloud augmentera", a déclaré Charles DeBeck, IBM X-Force IRIS. "Notre équipe a observé que les développeurs de logiciels malveillants ont déjà commencé à créer des logiciels malveillants qui désactivent les fonctions de sécurité courantes dans le Cloud, et à concevoir des logiciels malveillants qui tirent parti du facteur d'échelle et de l'agilité offertes par le Cloud".

Une sécurité du Cloud mature peut conduire à une réponse plus rapide en matière de sécurité .

Alors que la révolution du Cloud présente de nouveaux défis pour les équipes de sécurité, les organisations qui sont capables de pivoter vers un modèle de gouvernance plus mature et plus rationnel pour la sécurité du Cloud peuvent améliorer leur agilité en matière de sécurité et leurs capacités de réponse.

L'enquête de l'IBM Institute for Business Value a révélé que les organisations interrogées qui se sont classées à un niveau de maturité élevé dans l'évolution du Cloud et de la sécurité étaient capables d'identifier et de contenir les atteintes aux données plus rapidement que celles qui en étaient encore aux premières phases de leur parcours d'adoption du Cloud. En termes de temps de réponse aux atteintes aux données, les organisations interrogées les plus matures ont été capables de les identifier et de les contenir deux fois plus vite que les organisations les moins matures (cycle de vie moyen des menaces de 125 jours contre 250 jours).

Alors que le Cloud devient essentiel pour les opérations commerciales et pour les employés travaillant de plus en plus à distance, IBM Security recommande aux organisations de se concentrer sur les éléments suivants pour aider à améliorer la cybersécurité dans les environnements hybrides et multiclouds :

• **Établir une gouvernance et une culture de collaboration** : Adopter une stratégie unifiée qui combine les

opérations Cloud et de sécurité - entre les développeurs d'applications, les opérations informatiques et la sécurité. Désigner des politiques et des responsabilités claires pour les ressources Cloud existantes ainsi que pour l'acquisition de nouvelles ressources Cloud.

• **Adopter une vision basée sur le risque** : Évaluez les types de workloads et de données que vous prévoyez de migrer vers le Cloud et définissez des politiques de sécurité appropriées. Commencez par une évaluation basée sur les risques pour une visibilité de l'ensemble de votre environnement et créez une feuille de route pour l'adoption progressive du Cloud.

• **Appliquer une gestion rigoureuse des accès** : Exploiter les politiques et les outils de gestion des accès aux ressources Cloud, notamment l'authentification multifacteurs, pour empêcher l'infiltration au moyen d'identifiants volés. Restreindre les comptes privilégiés et définir tous les groupes d'utilisateurs avec les privilèges les moindres (least privileges) afin de minimiser les dommages causés par la compromission des comptes (modèle de zero trust).

• **Avoir les bons outils** : S'assurer que les outils de surveillance, de visibilité et de réponse en matière de sécurité sont efficaces pour toutes les ressources, Cloud et locales. Envisager de passer à des technologies et des normes ouvertes qui permettent une plus grande interopérabilité entre les outils.

• **Automatiser les processus de sécurité** : Mettre en œuvre une automatisation efficace de la sécurité dans votre système peut aider à améliorer vos capacités de détection et de réponse, plutôt que de se fier à une réaction manuelle aux événements.

• **Utiliser des simulations proactives** : S'entraîner à divers scénarios d'attaque ; Cela peut aider à identifier les angles morts et à résoudre les éventuelles questions qui pourraient survenir au cours de l'enquête sur l'attaque.

Vous pouvez télécharger le rapport complet X-Force IRIS sur le paysage de la sécurité du Cloud ici.

---

[1] IDC CloudPulse Summary Q119

[2] IBM Institute for Value Survey of 930 senior business and IT professionals

[3] IBM X-Force IRIS: "Cloud Security Landscape Report"

[4] IBM X-Force Threat Intelligence Index, 2020

[5] IBM X-Force IRIS "Cloud Landscape Report," based on client incident response cases taking place between June 2018 and March 2020

Contacts :

IBM
Gaëlle Dussutour

Tel. : + 33 (0)6 74 98 26 92
DUSGA@fr.ibm.com

Weber Shandwick pour IBM
Robin Legros / Morad Salehi
Tel. : + 33 (0)6 68 04 57 83
ibmfrance@webershandwick.com