Communiqués de presse

Rapport X-Force : Aucune pénurie de ressources pour pirater les environnements Cloud

Par Charles DeBeck, le 16 septembre 2021 : Alors que les cybercriminels continuent de chercher des moyens d'infiltrer les entreprises d'aujourd'hui sans qu'elles se méfient, un nouveau rapport d'IBM Security X-Force met en lumière les principales tactiques des cybercriminels, les portes ouvertes que les utilisateurs leur laissent et le marché florissant des ressources Cloud volées sur le dark web. Ce que l'on peut retenir de ces données, c'est que les entreprises contrôlent toujours leur propre destin en matière de sécurité du Cloud. Une bonne configuration des applications, des bases de données et des politiques aurait pu empêcher deux tiers des violations d'environnements Cloud observées par IBM dans le rapport de cette année.

Le rapport X-Force 2021 d'IBM sur le paysage des menaces de sécurité dans le Cloud a été étendu par rapport à 2020 avec de nouvelles données plus complètes, couvrant du deuxième trimestre 2020 jusqu'au deuxième trimestre 2021. Les ensembles de données que nous avons utilisés comprennent l'analyse du dark web, les données des tests de pénétration IBM Security X-Force Red, les indicateurs d'IBM Security Services, l'analyse des données de l'équipe X-Force de réponse aux incidents et les données de recherche de l'équipe X-Force Threat Intelligence. Cet ensemble de données élargi nous a donné une vue sans précédent sur la totalité du secteur technologique afin d'établir des liens pour améliorer la sécurité. Voici quelques faits saillants :

- **L'importance d'une bonne configuration** – Pour deux des trois environnements Clouds étudiés ayant subi une violation, cette dernière était due à une interface de programmation d'applications (API) mal configurée. Les intervenants de l'équipe X-Force de réponse aux incidents ont également observé des machines virtuelles dont les paramètres de sécurité par défaut étaient exposés par erreur à Internet, notamment des plateformes mal configurées et des contrôles réseau insuffisamment appliqués.
- **Le non-respect des règles conduit à la compromission** – L'équipe X-Force Red a constaté des violations des mots de passe et des politiques dans la grande majorité des tests de pénétration du Cloud réalisés au cours de l'année écoulée. L'équipe a également observé une augmentation significative de la gravité des vulnérabilités dans les applications déployées dans le Cloud, tandis que le nombre de vulnérabilités décelées dans les applications déployées dans le Cloud a bondi de 150 % au cours des cinq dernières années.
- **Accès automatisé pour les cybercriminels** - Avec près de 30 000 comptes Cloud compromis en vente à prix cassés sur les places de marché du dark web et le protocole Remote Desktop (protocole de bureau à distance) représentant 70 % des ressources Cloud en vente, les cybercriminels disposent d'options clés en main pour automatiser davantage leur accès aux environnements Cloud.
- **Tous les regards se tournent vers les ransomwares et le minage de cryptomonnaies** - Les mineurs de cryptomonnaies et les ransomwares restent les logiciels malveillants les plus répandus dans les environnements Cloud, représentant plus de 50 % des compromissions de systèmes détectées, selon les données analysées.

Télécharger le rapport

La modernisation est le nouveau pare-feu

De plus en plus d'entreprises reconnaissent la valeur métier du Cloud hybride et distribuent leurs données sur

une infrastructure diversifiée. En fait, le rapport 2021 sur le coût d'une violation de données a révélé que les organisations victimes d'une violation mettant en œuvre une approche principalement axée sur le Cloud public ou privé ont subi des coûts de violation supérieurs d'environ 1 million de dollars à ceux des organisations ayant adopté une approche de Cloud hybride.

Les entreprises recherchant des environnements hétérogènes pour répartir leurs applications et mieux contrôler où sont stockées leurs données les plus critiques, la modernisation de ces applications devient un point de contrôle pour la sécurité. Le rapport met en lumière les politiques de sécurité qui n'englobent pas le Cloud, ce qui augmente les risques de sécurité auxquels les entreprises sont confrontées dans des environnements déconnectés. En voici quelques exemples :

- **Le pivot parfait** - Les entreprises peinent à surveiller les environnements Cloud aujourd'hui et à détecter les menaces liées à ces derniers. Cela a contribué à faire pivoter les acteurs de la menace des environnements en local vers les environnements Cloud, ce qui en fait l'un des vecteurs d'infection ciblant les environnements Cloud les plus fréquemment observés - représentant 23 % des incidents auxquels IBM a répondu en 2020.
- **Exposition des APIs** - Les actifs mal configurés constituent un autre vecteur d'infection important que nous avons identifié. Deux tiers des incidents étudiés concernaient des APIs mal configurées. Les APIs dépourvues de contrôles d'authentification peuvent permettre à quiconque, y compris les acteurs malveillants, d'accéder à des informations potentiellement sensibles. D'un autre côté, les APIs auxquelles on accorde l'accès à trop de données peuvent également entraîner des divulgations involontaires.

De nombreuses entreprises n'ont pas le même niveau de confiance et d'expertise lors de la configuration des contrôles de sécurité dans les environnements de Cloud computing que dans les environnements en local, ce qui conduit à un environnement de sécurité fragmenté, plus complexe et difficile à gérer. Les entreprises doivent gérer leur infrastructure distribuée comme un seul et même environnement pour éliminer la complexité et obtenir une meilleure visibilité du réseau, du Cloud à la périphérie (au edge) et inversement. En modernisant leurs applications critiques, les équipes de sécurité pourront non seulement récupérer plus rapidement les données, mais elles disposeront également d'une vision beaucoup plus globale des menaces qui pèsent sur leur organisation, ce qui leur permettra de réagir plus rapidement.

Croyez bien que les attaquants vont réussir et garder le cap

Il est de plus en plus évident que la notion de périmètre s’efface et les conclusions du rapport ne font qu'ajouter à ce corpus de données. C'est pourquoi l'adoption d'une approche « zero trust » gagne en popularité et en urgence. Elle supprime l'élément de surprise et permet aux équipes de sécurité d’anticiper tout manque de préparation à la réponse. En appliquant ce cadre, les organisations peuvent mieux protéger leur infrastructure de Cloud hybride, en leur permettant de contrôler tous les accès à leurs environnements et de surveiller l'activité liée au Cloud et les configurations appropriées. De cette façon, les organisations peuvent passer à l'offensive avec leur défense, en détectant les comportements à risque et en appliquant des contrôles liés à la réglementation en matière de confidentialité et des accès à privilège moindre. Voici quelques-unes des preuves tirées du rapport :

- **Politique impuissante** - Nos recherches suggèrent que deux tiers des violations étudiées dans les environnements Cloud auraient probablement été évitées par un renforcement important des systèmes, comme la mise en œuvre correcte des politiques de sécurité et des correctifs.

- **L'informatique de l'ombre** – Le «« Shadow IT », c'est-à-dire les instances ou ressources Cloud qui ne sont pas passées par les canaux officiels d'une organisation, indique que de nombreuses organisations ne respectent pas les normes de sécurité de base actuelles. En fait, X-Force estime que l'utilisation du shadow IT a contribué à plus de 50 % des expositions de données étudiées.
- **Le mot de passe est « admin 1 »** - Le rapport illustre les données de X-Force Red accumulées au cours de l'année dernière, révélant que la grande majorité des tests de pénétration de l'équipe dans divers environnements Cloud ont montré des problèmes liés aux mots de passe ou au respect des politiques.

Le recyclage de ces vecteurs d'attaque souligne le fait que les acteurs de la menace s'appuient de manière répétée sur l'erreur humaine pour s'introduire dans l'organisation. Il est impératif que les entreprises et les équipes de sécurité opèrent avec en tête l'hypothèse d'une compromission pour garder le cap.

Les marchés aux puces du Dark Web vendent des accès au Cloud

Les ressources Cloud offrent aux cyberacteurs de nombreux accès aux entreprises, attirant l'attention sur les dizaines de milliers de comptes Cloud disponibles à la vente sur des marchés illicites à prix cassés. Le rapport révèle que près de 30 000 comptes Cloud compromis sont exposés sur le dark web, avec des offres de vente allant de quelques dollars à plus de 15 000 dollars (en fonction de la géographie, du montant du crédit sur le compte et du niveau d'accès au compte) et des politiques de remboursement alléchantes pour influencer le pouvoir d'achat des clients.

Mais ce n'est pas le seul « outil » Cloud en vente sur les marchés du dark web. Notre analyse souligne que le protocole de bureau à distance (RDP : Remote Desktop Protocol) représente plus de 70 % des ressources Cloud à vendre - une méthode d'accès à distance qui dépasse largement tout autre vecteur commercialisé. Si les places de marché illicites constituent un terrain d'achat idéal pour les acteurs de la menace à la recherche de moyens pour pirater le Cloud, ce qui nous préoccupe le plus, c'est la persistance d'un modèle dans lequel les contrôles et protocoles de sécurité faibles - des formes de vulnérabilité évitables - sont exploités de manière répétée pour des accès illicites.

Pour lire nos conclusions complètes et en savoir plus sur les mesures détaillées que les entreprises peuvent prendre pour protéger leurs environnements Cloud, consultez le rapport X-Force 2021 d'IBM sur le paysage des menaces de sécurité dans le Cloud ici.

Contacts presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0) 6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Jennifer Tshidibi / Eric Chauvelot

Tél. : + 33 (0)6 13 94 26 58 / + 33 (0)6 21 64 28 68

ibmfrance@webershandwick.com