VARONIS

ÉQUIPE DE RECHERCHE CLOUD

RAPPORT 2021 SUR LES RISQUES DU SAAS

Ce rapport traite des tendances et défis clés liés aux identités non supervisées et aux privilèges du Shadow IT, qui sont susceptibles de mettre en danger les données sur les environnements fragmentés SaaS et IaaS.

À PROPOS DU RAPPORT

Les données ont été recueillies à partir des SaaS/IaaS suivants, pris en charge par Varonis **DatAdvantage Cloud :**

Google box GitHub okta

zoom slack salesforce

Jira Software aws amazon S3

200 000
identités

Des centaines de millions
d'actifs cloud

DES IDENTITÉS CLOUD À FORT IMPACT

43 %

de toutes les identités cloud sont abandonnées, inutilisées… et vulnérables

IMPACT

Les identités inutilisées, abandonnées par des utilisateurs qui ne recourent plus à un service cloud, sont des cibles faciles lors des prises de contrôle de comptes, et augmentent donc considérablement la surface exposée aux attaques d'une organisation.

RECOMMANDATION

Les identités inutilisées, qui se multiplient rapidement, doivent être surveillées et identifiées en permanence afin d'être immédiatement supprimées de l'ensemble des applications SaaS et des services cloud critiques pour l'exploitation.

75 %

des identités cloud appartenant à des prestataires externes restent actives après leur départ

IMPACT

La plupart des anciens prestataires ne voient pas tous leurs accès résiliés lorsqu'ils quittent l'entreprise ; ils conservent souvent l'accès aux services cloud de l'organisation, à partir desquels ils peuvent continuer à accéder à l'adresse IP et aux données et potentiellement les voler.

RECOMMANDATION

Lorsqu'un prestataire quitte l'entreprise, ses identités, droits et accès doivent être entièrement répertoriés en vue d'une suppression complète. En outre, leurs activités au cours des 60 jours précédant leur départ devraient être auditées pour détecter les vols de données potentiels ou autres compromissions.

25 %

des identités dans les applications SaaS et **la moitié** des identités dans les services IaaS ne sont pas humaines

IMPACT

Les identités non humaines comprennent les API, les applications sans serveur, les machines virtuelles, etc. Contrairement aux identités humaines, elles sont menacées de compromission 24 h/24 et 7 j/7, car elles sont toujours connectées et généralement négligées par les équipes de sécurité, puisqu'elles fonctionnent en arrière-plan.

RECOMMANDATION

Tout comme les identités humaines, les identités non humaines doivent être étroitement contrôlées pour s'assurer qu'elles n'ont pas été compromises et que leurs autorisations ne sont pas excessives au vu des tâches requises.

PRIVILÈGES CLOUD MAL CONFIGURÉS

44 %

des privilèges des utilisateurs cloud ne sont pas configurés correctement

IMPACT

Les utilisateurs disposent souvent de privilèges excessifs et mal attribués en raison d'une négligence de l'équipe de sécurité ou d'une activité malveillante. Cela peut exposer une organisation au piratage de comptes et à l'exfiltration de données.

RECOMMANDATION

Les privilèges des utilisateurs doivent être surveillés en permanence pour détecter les erreurs de configuration et les modifications non autorisées, en vue d'ajuster correctement les privilèges excessifs et d'appliquer véritablement un modèle de moindre privilège.

60 %

des utilisateurs cloud dotés de privilèges sont des administrateurs du Shadow IT

IMPACT

Les administrateurs du Shadow IT sont des utilisateurs privilégiés qui disposent d'un accès privilégié non autorisé acquis en dehors du champ d'action de l'équipe de sécurité. Ils sont en mesure d'effectuer des modifications de niveau administrateur pouvant causer des dommages dans un service cloud.

RECOMMANDATION

Les administrateurs du Shadow IT doivent être surveillés tout comme vos administrateurs réguliers ; dans la plupart des cas, il est nécessaire d'adapter leurs droits à leur rôle et de les aligner sur les droits du groupe d'utilisateurs non privilégiés auquel ils sont affectés.

ACTIVITÉS CLOUD À HAUT RISQUE

15 %

des employés transfèrent des données professionnelles stratégiques sur des comptes cloud personnels

IMPACT

Les données stratégiques de l'entreprise ne demeurent pas toujours dans les services cloud autorisés. Les employés transfèrent souvent des données vers des services cloud non contrôlés, y compris des comptes personnels. Au mieux, cela signifie que les données résident hors du contrôle de votre équipe de sécurité ; au pire, cela indique que les données ont été volées.

RECOMMANDATION

Les équipes de sécurité doivent appliquer des politiques d'utilisation qui empêchent le transfert de documents depuis des applications autorisées vers des comptes privés.

16 %

de tous les utilisateurs cloud effectuent des actions privilégiées et **20 %** d'entre eux ont accès à des données sensibles de l'entreprise

IMPACT

Les actions privilégiées, généralement réservées aux administrateurs, mais souvent effectuées par des administrateurs du Shadow IT, devraient être l'un des principaux sujets d'inquiétude des organisations, surtout si les auteurs ont également accès à de grandes quantités de données. Ces actions peuvent avoir un impact négatif sur l'ensemble du service cloud ou sur une grande partie de l'expérience du personnel tout entier, et pas seulement sur un utilisateur ou un ensemble de données unique.

RECOMMANDATION

Les équipes de sécurité doivent constamment examiner tous les privilèges d'identité pour repérer les administrateurs du Shadow IT et réduire leurs autorisations au strict minimum nécessaire pour faire leur travail, voire supprimer leur accès s'il est établi que leurs privilèges ont été augmentés à des fins malveillantes.

LISTE DE CONTRÔLE DE LA SÉCURITÉ DANS LE CLOUD

Réduisez votre rayon d'exposition dans le cloud en veillant à ce que les employés disposent de l'accès minimal nécessaire pour faire leur travail. Cela nécessite de mapper en permanence les listes de contrôle d'accès dans vos services cloud disparates, en vue d'identifier et de révoquer les privilèges excessifs.

Surveillez l'activité des utilisateurs pour détecter les anomalies ou les cas de non-respect des politiques. Guettez les utilisateurs privilégiés qui abusent de leurs droits d'administrateur pour des activités non pertinentes pouvant mettre en danger votre organisation.

Éliminez les identités fantômes en surveillant l'activité (ou l'absence d'activité) du compte. Supprimez ou désactivez les identités humaines et non humaines, telles que les jetons d'accès aux applications inactifs, afin de limiter votre surface exposée aux attaque et d'éviter la prise de contrôle de comptes.

Examinez régulièrement les droits existants afin que les responsables d'unités métier puissent voir qui a accès à leurs données et applications, et révoquer les autorisations qui ne sont plus nécessaires.

Utilisez la détection des menaces sur tous les services cloud pour repérer les activités malveillantes qui couvrent plusieurs applications cloud. Certains fournisseurs SaaS ont intégré à leurs logiciels des journaux et des alertes, mais ne peuvent voir qu'une partie d'une attaque. La surveillance SaaS unifiée vous offre une modélisation des menaces plus robuste et accélère les enquêtes.

Vérifiez les paramètres de configuration du partage de fichiers dans le cloud. Cela permettra d'éviter un partage accidentel ou la fuite de données stratégiques. Le transfert imprudent d'un fichier vers un dossier doté de nombreux droits de partage peut entraîner une fuite de données.

Instaurez des processus pour le départ des employés et prestataires externes. Cela peut être compliqué lorsque les services cloud sont gérés hors SSO. Adoptez une solution IAM unifiée et inter-services qui vous permet de révoquer les autorisations lorsque les employés ou les prestataires quittent l'entreprise.

Essayez Varonis gratuitement !

Varonis DatAdvantage Cloud vous permet de surveiller et de protéger vos applications cloud stratégiques à partir d'une seule et même interface.

OBTENEZ UNE DÉMO