Microsoft Relents, offre une journalisation critique gratuite à tous les clients 365

Le recul de l'industrie incite Microsoft à abandonner les prix premium pour l'accès aux données de journalisation dans le cloud.

Becky Bracken :

Note : Une version antérieure de l'histoire utilisait « clé » dans le titre comme synonyme de « critique ».
Le résultat a été lu comme une référence possible à l'« enregistrement de frappe », ce qui n'était pas l'intention.
Le mot a été changé pour plus de clarté.

Microsoft a supprimé les frais associés à l'accès élargi à la journalisation pour tous les niveaux des détenteurs de licences 365, après des plaintes selon lesquelles le fournisseur de services cloud percevait effectivement une taxe d'exploitation pour la gestion des logs* sur les clients.

**Définition de logging*

Le logging est un terme signifiant la gestion des logs.
Les logs sont des journaux d'évènements où sont collectés les évènements relatifs à l'état d'un système.
Il existe une multitude de logs en fonction des différents systèmes.

Prenons l'exemple d'une application web : les logs peuvent être toute action effectuée sur le service web, comme la connexion d'un utilisateur à la plateforme, une génération d'erreur HTTP ou encore un accès à une ressource sur le serveur.

Une grande quantité de données est rapidement collectée, ce qui implique un coût matériel et humain important.
De plus, pour que les logs soient utiles, ils nécessitent les actions suivantes :

Sélectionner les informations utiles à stocker et archiver

Garantir la sécurité et la confidentialité des journaux stockés

Contrôler la qualité des données des journaux en analysant et en ajoutant aux journaux les informations manquantes

Analyser les logs (souvent confondu avec le monitoring d'une application)

Contextualiser les évènements (enrichissement des logs)

Adresse IP ayant générée les logs

Utilisateur concerné

Fonctionnalité concernée

Détail de l'erreur

La contextualisation des logs est la partie qui requiert le plus d'expérience et de connaissances du système surveillé, afin de savoir quelles informations doivent être retenues et lesquelles sont inutiles.
Cette tâche demande également beaucoup de temps humain.

Une fois toutes ces actions réalisées, les logs vont permettre d'investiguer sur un dysfonctionnement de l'application pour qu'il ne se reproduise plus.
Dans le cadre d'une attaque, cela permettra notamment de connaître les acteurs à l'origine de celle-ci.
De plus, il sera possible de savoir quelle fonctionnalité a été abusée, afin de corriger la faille qui a permis l'attaque.

Parallèlement, une récente mise à jour de la Cybersecand Infrastructure Security Agency (CISA) sur une campagne d'espionnage menée contre Microsoft 365 par le groupe chinois APT Storm-0558 a encore souligné la nécessité pour les organisations d'avoir accès à une journalisation détaillée pour recueillir des preuves de compromission.

Microsoft a reconnu la nécessité de rendre l'accès aux données de journalisation plus économique.
« Ces étapes sont le résultat d'une coordination étroite avec les clients commerciaux et gouvernementaux, et avec CISA sur les types de données de journal de sécurité que Microsoft fournit aux clients du cloud pour obtenir des informations et des analyses à mesure que le paysage des menaces continue d'évoluer », a déclaré la société dans une déclaration à Dark Reading.

À l'avenir, les clients de Microsoft Purview Audit Standard bénéficieront d'une meilleure visibilité sur les données de sécurité, y compris les journaux détaillés de l'accès aux e-mails et plus de 30 autres types de données de journal auparavant réservés aux abonnés premium de Purview.
« Les journaux d'audit Purview permettent à une entreprise de visualiser les données des journaux dans le cloud, aidant ainsi les clients à répondre efficacement aux évènements de sécurité et à enquêter sur les données consultées lors d'une violation », a ajouté Microsoft.

En outre, Microsoft prolongera la durée de conservation des journaux de 90 jours à 180 jours.

Le directeur adjoint exécutif de la CISA pour la cybersécurité, Eric Goldstein, a applaudi la décision de Microsoft.

"Nous pensons que chaque organisation mérite d'avoir des produits sécurisés par conception et livrés avec les données de sécurité nécessaires « prêtes à l'emploi », a déclaré Goldstein, dans une déclaration de soutien.
« L'annonce de Microsoft aujourd'hui est une étape importante dans l'amélioration de la sécurité de nos communautés, de nos entreprises et de notre pays, reconnaissant notre travail commun à venir. »

Tenez-vous au courant des dernières menaces de cybersécurité, des vulnérabilités récemment découvertes, des informations sur les violations de données et des tendances émergentes.
Livré quotidiennement ou hebdomadairement directement dans votre boîte de réception.

S'inscrire

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230720
"C'est ensemble qu'on avance"