ORACLE

Vos logiciels sont-ils vulnérables face à la cybercriminalité?

Le support tiers et la maintenance réalisée par soi-même ne peuvent pas vous protéger — la vraie solution se situe à la source

La cybercriminalité est une réalité

23 000 milliards de dollars

C'est le coût annuel estimé des dommages causés par la cybercriminalité dans le monde d'ici 2027[1]

Les cyberattaques et les violations de données progressent de manière exponentielle[2]

Le coût moyen d'une violation de données est de **4,88 millions de dollars** en 2024[3]

Les attaques par ransomware représentent une menace persistante touchant tous les secteurs d'activite[4]

De nombreuses entreprises ne se relèvent jamais des conséquences

- Atteinte aux informations sensibles et propriétaires
- Perturbation de l'activité
- Restauration des systèmes et des fichiers
- Amendes et litiges
- Atteinte à la réputation et à la marque
- Confiance des clients et des employés

Ne vous laissez pas tromper par les méthodes de sécurité des fournisseurs de support tiers et de la maintenance réalisée par soi-même

1 Il n'y a pas d'application de correctif dans le "patching virtuel"

Le patching virtuel est une solution de contournement qui en réalité ne corrige pas ou ne met pas à jour votre logiciel.

- Est une solution temporaire
- Qui néglige la cause profonde du problème
- Qui ignore toute l'étendue des vulnérabilités

Département américain de la sécurité intérieure

"Toutes les organisations doivent mettre en place un processus solide et durable de gestion des correctifs pour s'assurer que les mesures préventives appropriées sont prises pour faire face aux menaces potentielles".

https://www.cisa.gov/

2 Les pare-feux ont des limites

Les stratégies de sécurité basées sur la protection du périmètre laissent vos logiciels exposés à des attaques.

- Risques de brèches internes
- Visibilité minimale des menaces sur les réseaux
- La sécuritée intégrée au logiciel est ignorée

Règlement général sur la protection des données de l'UE

Un cadre unifié de règles visant à renforcer la confidentialité des données et à garantir la sécurité des données à caractère personnel et du traitement des données.

- ✓ S'applique à tout organisme traitant des données relatives aux citoyens de l'UE
- ✓ Applicable depuis le 25 mai 2018
- ✓ Le non-respect ou la violation peut entraîner des amendes conséquentes

https://commission.europa.eu/law/law-topic/data-protection_en?prefLang=fr&etrans=fr

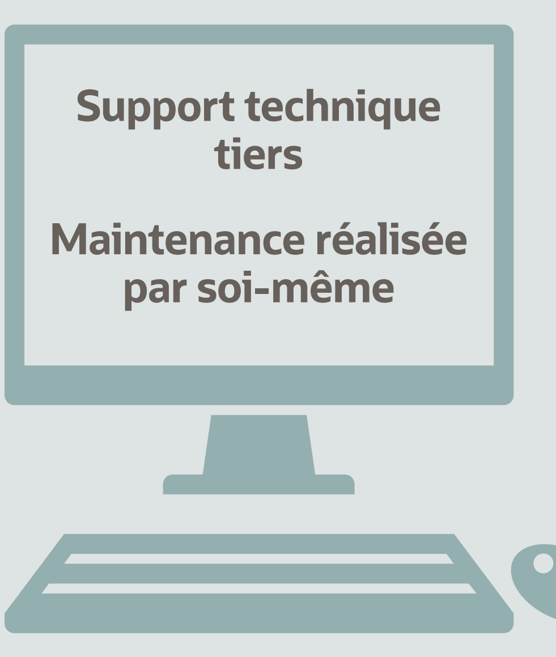
3 Maintenance réalisée par soi-même = responsabilité potentielle

En le gérant vous-même, vos logiciels sont privés des mises à jour de sécurité critiques.

- Impossibilité de corriger (légalement) les vulnérabilités
- Pas d'accès aux nouveaux correctifs et mises à jour
- Peu de ressources pour maintenir et sécuriser de manière fiable

Conclusion

Les correctifs de sécurité sont essentiels pour sécuriser les logiciels d'entreprise, y compris ceux d'Oracle. Si vous ne possédez pas le code, vous ne pouvez ni y accéder ni le modifier, laissant votre logiciel vulnérable aux attaques et votre entreprise exposée aux risques.



- Mises à jour de sécurité inappropriées
- Correctifs de sécurité inadaptés
- Protection insuffisante contre les vulnérabilités

Seul Oracle peut assurer la sécurité des logiciels Oracle

Le Support Technique Oracle est le seul moyen pour vous d'obtenir les mises à jour critiques de sécurité et garantir la protection de votre logiciel Oracle.

Oracle crée et détient le code source

- Identification et traitement à la source des vulnérabilités et des nouvelles menaces
- Mises à jour fiables de sécurité à la source

Oracle assure la sécurité à tous les niveaux

- Correctifs à chaque couche du socle logiciel
- Tests de régression sur l'ensemble du socle

Oracle dispose des outils, de l'expérience et des connaissances

- Processus proactif de gestion du changement
- Processus homogène de gestion des versions
- Innovation fiable, durable et sans égale

Obtenez plus d'Oracle.

Lorsque votre entreprise est en jeu, rien ne remplace une assistance fiable, sécurisée et complète.

Visitez le site Oracle Premier Support

Sources:
1. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020
2. https://www.securitymagazine.com/articles/100335-cyberattack-attempts-increased-104-in-2023
3. https://www.ibm.com/security/data-breach
4. https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

Version 1.04