ORACLE

Les correctifs logiciels sont essentiels pour la sécurité: Êtes-vous prêt ?

Votre stratégie de sécurité est-elle sûre et complète?
Ne prenez aucun risque.

"Le support technique d'Oracle offre des niveaux de capacité et de sécurité bien supérieurs à ceux proposés par les fournisseurs de support logiciel tiers, non-Oracle." [1]

Pourquoi des correctifs?

L'enquête annuelle la plus récente de la société de recherche technologique Omdia a identifié les trois grandes tendances, qui sont la gestion de la sécurité, la gestion des identités et la protection de la vie privée.

L'absence de correctifs et de maintenance appropriés des logiciels met en danger les résultats et la réputation de votre entreprise.

Menaces auxquelles vous pourriez être confronté :

Vol | **Perte financière** | **Réputation de la marque endommagée** | **Fraude** | **Amendes**

Les correctifs sont une mesure clé de votre stratégie de protection proactive et sont essentiels à toute bonne gouvernance de la sécurité informatique. Il est impératif pour toute entreprise d'assurer une maintenance une application régulière des correctifs logiciels réguliers.

"L'application immédiate des correctifs logiciels fournis par les éditeurs est primordiale pour éviter les risques dus à des vulnérabilités de sécurité non adressées". [2]

Avantages des correctifs

Il y a de nombreuses raisons d'appliquer des correctifs de manière régulière sur vos logiciels. Oracle estime que ces deux raisons sont essentielles :

1. **Pour maintenir une sécurité logicielle forte:** Un programme rigoureux de sécurité et de maintenance des logiciels exige une vigilance et une maintenance constantes.
2. **Pour répondre aux besoins de gouvernance et de conformité des systèmes d'information:** Une base solide et une culture de la conformité ne peuvent exister sans des services réguliers de correction et de maintenance des logiciels.

"[Maintenir votre] parc logiciel à jour avec les correctifs fournis par les éditeurs de logiciel est le moyen, le meilleur et le plus opportun de se protéger contre les menaces liées aux logiciels".[3]

La Commission fédérale du commerce (FTC) recommande de mettre à jour et de corriger les logiciels tiers, de tenir compte des alertes de sécurité des éditeurs et de les traiter immédiatement.

Comment intégrer une stratégie de mise à jour des logiciels?

Voici les lignes directrices en matière de correctifs qui conduisent à **une sécurité renforcée:**

1. Favoriser une culture de changement afin que la mise en place de correctifs soit considérée comme un élément essentiel du bien-être organisationnel.
2. Donner la priorité aux correctifs en fonction du **risque commercial et technique.**
3. S'engager à appliquer les correctifs est un élément clé de votre **maintenance régulière en terme de sécurité.**
4. Pour éviter les risques, **n'utilisez que les patchs de votre éditeur de logiciels.**

"Les entreprises devraient travailler en étroite collaboration avec leurs éditeurs de logiciels, car ce sont eux qui ont le plus d'expérience et d'expertise en matière de correctifs, de support et de sécurisation de leurs propres produits." [4]

Pourquoi un partenaire de confiance est-il essentiel?

Les entreprises doivent s'associer à un éditeur de confiance pour mettre en place des procédures permettant de **maintenir à jour la sécurité** de leurs logiciels et de remédier aux vulnérabilités potentielles.

Il existe **trois caractéristiques** qui vous aident à identifier un partenaire de confiance, comme Oracle.

Partenaire de confiance

Possède des connaissances et une expertise en matière de sécurisation des données dans un environnement informatique d'entreprise.

A une longue expérience de la sécurité et du support en entreprise.

Sécurisé

Est expérimenté dans la sécurisation de l'ensemble du socle informatique.

Est expert dans la fourniture de ressources de support proactives et en temps réel.

Complet

Fournit une suite complète et intégrée d'offres de sécurité et de support en constante évolution et amélioration.

Est en mesure de vous aider à établir

Que vous manque-t-il en v sur un support tiers ?

1. Des correctifs de sécurité:

Les supports tiers ne peuvent pas fournir de correctifs majeurs de sécurité car :

- **Ils ne peuvent pas modifier des parties du code source d'Oracle.**
- **Ils ne sont pas au fait des détails techniques des vulnérabilités corrigées par Oracle.**

"La provenance inadéquate des fournisseurs de services tiers no risque potentiel, mais peut également entraîner une augmentatio en raison de l'éloignement des futures évolutions standard du l introduisant des coûts de régression par la suite".[5]

Le résultat final

L'application des correctifs de sécurité est essentielle pour sécuriser les logiciels d'entreprise, y compris ceux d'Oracle. **Si vous ne disposez pas de droits suffisants sur le code, vous ne pouvez pas y accéder ni le mettre à jour.** Cela expose vos logiciels aux attaques et votre entreprise à des risques.

Le Support par des tiers et la maintenance autonome signifient:

- **Des mises à jour de sécurité inadéquates**
- **Des solutions de sécurité inadéquates**
- **Élimination insuffisante des vulnérabilités**

Obtenez une sécurité renforcée avec Oracle

Appliquez les mises à jour de sécurité et renforcez la protection de vos logiciels Oracle qui sont critiques pour votre entreprise, tout en répondant aux besoins de gouvernance informatique et de conformité. Avec Oracle, vous obtenez:

- **Un programme régulier d'application de correctifs** et un engagement fort à l'échelle de toute l'entreprise sur la sécurité informatique, qui garantissent des systèmes moins vulnérables et plus sûrs.
- Des mises à jour de **sécurité fiables à la source.**
- Des processus **proactifs de gestion du changements.**

Lisez l'intégralité du rapport d'Omdia

Visitez le site Oracle Premier Support

[1-5] Omdia. (2020). Sustainable Software Patching : Critical for Solid Security, Reduced Risk, and Meeting Compliance Challenges.