ORACLE

O Patching de software é essencial para se manter seguro: Você está preparado?

A sua estratégia de segurança é robusta e abrangente?
Não se arrisque.

"O Suporte da Oracle fornece níveis de recursos e segurança que são muito mais abrangantes na comparação com os que podem ser oferecidos por fornecedores terceiros." [1]

Por que aplicar patches?

O levantamento anual mais recente da empresa de pesquisa em tecnologia Omdia identificou que a **gestão em segurança, a identidade e a privacidade** são as três tendências mais importantes.

Falhar em executar adequadamente o patching e a manutenção de softwares coloca os resultados e a reputação de sua empresa em risco.

Ameaças que você pode enfrentar:

Roubo | **Perdas Financeiras** | **Prejuízos à reputação da marca** | **Fraude** | **Multas**

O patching é uma medida fundamental para sua estratégia de proteção proativa e é crucial para toda boa gestão de segurança de TI. Garantir a manutenção e patching de softwares de forma regular é imperativo para toda empresa.

"A aplicação pontual de patching de software de fornecedores é a base indispensável para evitar o risco decorrente da presença de vulnerabilidades de segurança." [2]

Benefícios do patching

Existem vários motivos para aplicar patches regularmente em seu software. A Oracle acredita que estes dois são os principais:

1. **Manter uma forte segurança de software:**
   Um rigoroso programa de segurança e manutenção de software requer vigilância e manutenção contínuas.

2. **Atender às necessidades de gestão e conformidade de TI:**
   Uma forte base e uma cultura de conformidade não podem existir sem correções de software regulares e serviços de manutenção.

"[Mantendo sua] propriedade atualizada com patches do fornecedor é o principal e mais conveniente meio de proteção contra ameaças relacionadas ao software." [3]

A Comissão Federal de Comércio dos Estados Unidos (FTC, em inglês) recomenda a atualização e patching de software de terceiros, considerando quaisquer avisos de segurança dos fornecedores e abordando-os imediatamente.

Como você adota uma estratégia de patching de software?

Estas são as diretrizes de patching que levam a uma **segurança mais efetiva:**

1. Incentivar uma mudança de cultura para garantir que a aplicaçao de patches seja considerada um elemento essencial de organização e bem-estar.

2. Priorizar correções baseadas em **riscos técnicos e financeiros.**

3. Comprometer-se a executar a correção como parte fundamental de sua **manutenção de segurança regular.**

4. Para evitar riscos, fazer patching somente com seu **fornecedor de software.**

"As empresas devem trabalhar em estreita colaboração com seus fornecedores de software, porque eles têm mais experiência e expertise quando se trata de patching, apoiar e proteger seus próprios produtos." [4]

Por que um parceiro confiável é crucial?

As empresas devem fazer parceria com um provedor confiável para implementar procedimentos que mantenham sua **segurança de software** atualizada e lidem com **potenciais vulnerabilidades.**

Existem **três características** que ajudam a identificar um parceiro confiável, como a Oracle.

Confiável

Possui conhecimento e experiência em proteger dados em um ambiente de TI empresarial.

Tem experiência de longo prazo em lidar com segurança e suporte da classe empresarial.

Seguro

É experiente em proteger toda o stack de TI.

É um especialista em fornecer recursos de suporte proativos e em tempo real.

Abrangente

Fornece um conjunto completo e integrado de ofertas de segurança e suporte que está constantemente evoluindo e melhorando.

O que você está perdendo com o suporte de terceiros?

1. Patching de segurança:

Os fornecedores terceiros não podem oferecer patches de segurança essenciais porque:

- **Eles não podem alterar partes do código-fonte da Oracle.**
- **Eles não estão familiarizados com os detalhes técnicos das vulnerabilidades que a Oracle corrige.**

"A proveniência inadequada dos provedores de serviços terceirizados não só introduz um risco potencial, mas também pode causar um aumento dos custos de propriedade por causa de sua divergência do caminho de desenvolvimento padrão do software, introduzindo custos de regressão em um estágio posterior." [5]

Conclusão

O patching de software de segurança é essencial para proteger o software empresarial, incluindo o da Oracle. **Se você não tem direitos suficientes para o código-fonte, você não pode acessá-lo ou atualizá-lo.** Isso deixa seu software vulnerável a ataques e seu negócio exposto a riscos.

Suporte terceirizado e manutenção própria significam:

- **Atualizações de segurança inadequadas**
- **Patches de segurança inadequados**
- **Eliminação de vulnerabilidades inadequada**

Obtenha uma segurança robusta com a Oracle

Garanta atualizações de segurança essenciais para a proteção do seu software Oracle, satisfazendo as necessidades de gestão e conformidade de TI.
Com a Oracle você tem:

- **Um cronograma de patching regular** e uma forte ênfase na segurança de TI em toda a empresa, o que fornece a garantia de que seus sistemas são menos vulneráveis e mais seguros.
- **Atualizações de segurança confiáveis** para o código-fonte.
- Processos **proativos de gerenciamento de mudanças.**

Leia o relatório completo da Omdia

Visite o Oracle Premier Support

[1-5] Omdia (2020) Patching Sustentável de Software: Essencial para obter Segurança Robusta, Menos Riscos, e Atender aos Desafios de Compliance.