Wordpress

Regras de Segurança

Francisco Silva
E-Tutor

master.D

Resumo

1. Importância;
2. Estatísticas;
3. Tipos comuns de ataques;
4. Importância das atualizações;
5. Atualizações automáticas;
6. Plugins e Temas seguros;
7. Verificação de Vulnerabilidades;
8. Criação de senhas fortes;
9. Permissões de utilizadores;
10. Limite de tentativas de login;
11. 2FA;
12. SSL/HTTPS;
13. Firewalls e scanners;
14. Backups;
15. Questões.

master.D

A Importância da Segurança no Wordpress

- Proteção de dados sensíveis;
- Prevenção contra ataques e vulnerabilidades;
- Manutenção da confiança do utilizador.

Estatísticas de Segurança no Wordpress

- Mais de 70% dos sites Wordpress são vulneráveis;
- 60% das violações de segurança ocorrem por plugins desatualizados;
- Sites Wordpress são alvo de 90% dos ataques a CMSs.

Tipos comuns de ataques

- Injeção de SQL: Explora falhas para acessar a base de dados;
- XSS (Cross-Site Scripting): Insere scripts maliciosos no site;
- Ataques de Força Bruta: Tenta adivinhar passwords para ganhar acesso.

A Importância das Atualizações

- Evita falhas de segurança;
- Melhora o desempenho do site;
- Assegura compatibilidade de plugins e temas.

Atualizações Automáticas

- No painel de administração do Wordpress;
- No "wp-config.php";
- Com plugins de gestão de atualizações:
  - Easy Updates Manager;
  - WP Auto Updater.

```
define('WP_AUTO_UPDATE_CORE', true);
```

master.D

Escolher Plugins e Temas Seguros

- Verificar a reputação e as avaliações;
- Analisar a frequência de atualizações;
- Conferir o suporte e a documentação.

Verificação de Vulnerabilidades: Ferramentas Essenciais

- WPScan: Análise detalhada de segurança;
- Sucuri Security Scanner: Verificações de integridade do site;
- Theme Check: Conformidade com padrões do Wordpress para temas.

Criação de Senhas Fortes

- Utilizar uma mistura de caracteres (maiúsculas, minúsculas, números, símbolos);
- Evitar palavras comuns ou informações pessoais;
- Preferir senhas longas (mínimo de 12 caracteres);
- Considerar o uso de geradores de senha.

Gestão de Permissões de Utilizadores

- Definição de papéis e capacidades - AAM;
- Princípio do menor privilégio - Activity Log;
- Revisão regular das permissões.

Limitar Tentativas de Login

- Reduz risco de ataques de força bruta;
- Protege contra acessos não autorizados;
- Plugins recomendados: Limit Login Attempts Reloaded, WP Limit Login Attempts.

Autenticação de Dois Fatores (2FA): Um Escudo Extra

- Reforça a segurança das credenciais de acesso;
- Reduz significativamente o risco de acessos não autorizados;
- Implementação via plugins confiáveis, como Google Authenticator ou Two Factor Authentication.

Segurança Reforçada com SSL/HTTPS

- SSL/HTTPS para encriptação e autenticidade;
- Firewalls para defesa contra ameaças externas;
- Scanners de segurança para detecção proativa de vulnerabilidades.

Segurança com Firewalls e Scanners

- Bloqueio de tráfego c/ malware;
- Detecção precoce de ameaças;
- Plugins recomendados: Wordfence, Sucuri.

A Importância dos Backups

- Salvaguarda contra perda de dados;
- Ferramenta essencial de recuperação de desastres;
- Paz de espírito e continuidade de negócios.

Estratégias de Backup Eficientes

- Backups automáticos e programados;
- Armazenamento em locais seguros e diversificados;
- Testes regulares de restauração.

Questões?

Obrigado e até à próxima!

- Próximo Webinar: 06.02.2024 - 10h - Wordpress - Plugins Imprescindíveis

master.D