### **Política de Segurança de Servidores**

**1. Introdução**

A Política de Segurança de Servidores visa garantir a proteção dos servidores e dos dados neles hospedados contra acessos não autorizados, violações e outras ameaças de segurança. Esta política se aplica a todos os servidores gerenciados pela nossa organização.

**2. Escopo**

Esta política abrange todos os servidores, incluindo servidores web, servidores de banco de dados, servidores de aplicativos e qualquer outro tipo de servidor utilizado na nossa infraestrutura de TI.

**3. Servidores**

**3.1 Segurança do Sistema Operacional**

Apenas softwares, serviços e aplicativos necessários são instalados nos servidores. Patches e atualizações de segurança são aplicados regularmente, com a desativação de serviços e protocolos desnecessários para minimizar riscos.

**3.2 Controle de Acesso**

São implementadas medidas rigorosas de controle de acesso, utilizando senhas fortes e únicas, alteradas regularmente. A autenticação multifator (MFA) é utilizada sempre que possível, com privilégios administrativos limitados ao pessoal essencial.

**3.3 Segurança de Rede**

Firewalls são utilizados para restringir o tráfego com base em políticas de segurança. Os servidores são segregados em diferentes segmentos de rede conforme suas funções e a sensibilidade dos dados.

**4. Proteção de Dados**

**4.1 Criptografia**

Dados em repouso e em trânsito são criptografados utilizando protocolos de criptografia padrão da indústria. Backups são armazenados em ambientes criptografados para segurança adicional.

**4.2 Backup e Recuperação**

Backups automáticos e manuais dos dados críticos dos clientes e do sistema são realizados, armazenados em infraestrutura resiliente da AWS. Esses backups são monitorados e alertas são configurados para garantir sua integridade.

**5. Monitoramento e Registro**

**5.1 Monitoramento e Registro**

Registros de eventos relevantes de segurança são habilitados em todos os servidores, protegidos contra acessos não autorizados. A atividade dos servidores é monitorada continuamente, utilizando ferramentas como o Datadog para alertas em tempo real.

**6. Gestão de Vulnerabilidades**

**6.1 Gestão de Patches**

A gestão de patches é um processo crítico para garantir que todos os servidores estejam atualizados com as últimas correções de segurança. Isso envolve a avaliação contínua de novas atualizações e patches disponibilizados pelos fornecedores, a priorização de sua aplicação com base na criticidade das vulnerabilidades que abordam e a implementação cuidadosa desses patches para evitar interrupções nos serviços.

**7. Resposta a Incidentes**

**7.1 Tratamento de Incidentes**

Existe um plano de resposta a incidentes, com treinamento para a equipe relevante. Incidentes de segurança são relatados imediatamente e tratados conforme o protocolo estabelecido.

**10. Conclusão**

A Política de Segurança de Servidores é essencial para manter a integridade, confidencialidade e disponibilidade de nossa infraestrutura de servidores. A adesão a esta política garante proteção robusta contra ameaças de segurança e conformidade com os padrões da indústria.

### **Server Security Policy**

**1. Introduction**

The Server Security Policy aims to ensure the protection of servers and the data they host from unauthorized access, breaches, and other security threats. This policy applies to all servers managed by our organization.

**2. Scope**

This policy covers all physical and virtual servers, including web servers, database servers, application servers, and any other types of servers used within our IT infrastructure.

**3. Server Hardening**

**3.1 Operating System Security**

* Install only necessary software, services, and applications.
* Regularly apply security patches and updates.
* Disable unnecessary services and protocols.

**3.2 Access Control**

* Implement strict access control measures.
* Use strong, unique passwords and change them regularly.
* Employ multi-factor authentication (MFA) where possible.
* Limit administrative privileges to essential personnel only.

**3.3 Network Security**

* Use firewalls to restrict incoming and outgoing traffic based on security policies.
* Segregate servers into different network segments based on their role and data sensitivity.
* Implement intrusion detection and prevention systems (IDS/IPS).

**4. Data Protection**

**4.1 Encryption**

* Encrypt data at rest using industry-standard encryption protocols.
* Ensure all sensitive data transmitted over networks is encrypted.

**4.2 Backup and Recovery**

* Perform regular backups of critical server data.
* Store backups securely and test recovery procedures periodically.

**5. Monitoring and Logging**

**5.1 Logging**

* Enable logging on all servers to capture security-relevant events.
* Secure logs against unauthorized access and tampering.

**5.2 Monitoring**

* Continuously monitor server activity for unusual or suspicious behavior.
* Use security tools like Datadog for real-time monitoring and alerting.

**6. Vulnerability Management**

**6.1 Regular Scanning**

* Conduct regular vulnerability scans and penetration tests.
* Address and remediate identified vulnerabilities promptly.

**6.2 Patch Management**

* Apply patches and updates in a timely manner to mitigate security risks.

**7. Incident Response**

**7.1 Incident Handling**

* Develop and implement an incident response plan for server-related security incidents.
* Train relevant personnel on incident response procedures.

**7.2 Reporting**

* Report security incidents to the designated security team immediately.

**8. Compliance and Auditing**

**8.1 Regular Audits**

* Conduct regular security audits to ensure compliance with this policy.
* Review and update the policy periodically to reflect changes in technology and threats.

**9. Roles and Responsibilities**

**9.1 IT Team**

* Responsible for implementing and maintaining server security measures.
* Regularly review and update server configurations and security settings.

**9.2 Employees**

* Adhere to the security guidelines and report any security concerns promptly.

**10. Conclusion**

The Server Security Policy is essential for maintaining the integrity, confidentiality, and availability of our server infrastructure. Adherence to this policy ensures robust protection against security threats and compliance with industry standards.