Formação AWS Cloud Foundations

Alexsandro Lechner

Arquiteto de Soluções AWS

linkedin.com/in/alexsandrolechner

Conteúdo Programático

❑ Módulo 9: Segurança na AWS

- ➢ **Práticas recomendadas de segurança na nuvem**
- ➢ Criptografia de dados na AWS
- ➢ AWS WAF: firewall de aplicativos da web

Segurança na AWS

Práticas recomendadas de segurança na nuvem

Práticas recomendadas

Não temos como falar de segurança na nuvem sem primeiro entender as responsabilidades dos envolvidos, neste caso:

VOCÊ vs AWS

Para isto teremos que analisar o “Modelo de Responsabilidade Compartilhada”

Práticas recomendadas

A segurança na nuvem da AWS é baseada em um modelo de responsabilidade compartilhada, onde tanto a AWS quanto os usuários têm papéis específicos a desempenhar para garantir um ambiente seguro e em conformidade.
Este modelo ajuda a dividir claramente as responsabilidades de segurança entre a AWS e os usuários finais.

Práticas recomendadas

A AWS é responsável pela segurança da nuvem, o que inclui a proteção da infraestrutura global que dá suporte a todos os serviços em nuvem oferecidos. Isso abrange:

Hardware físico, Infraestrutura dos data centers, Softwares e algumas coisas mais.

Práticas recomendadas

Já o papel do usuário é ser responsável pela segurança da configuração dos serviços utilizado e a proteção de seus dados. E isto varia de acordo com o tipo de serviço escolhido, vamos detalhar para melhor entendimento.

Práticas recomendadas

Serviços de infraestrutura, como Amazon EC2:

Os usuários têm controle completo sobre os sistemas operacionais que instalam e devem implementar medidas de segurança, como a aplicação de patches em sistemas operacionais, a configuração de firewalls, a definição de permissões de acesso e a proteção de dados sensíveis.

Práticas recomendadas

Serviços gerenciados, como Amazon S3 e Amazon DynamoDB:

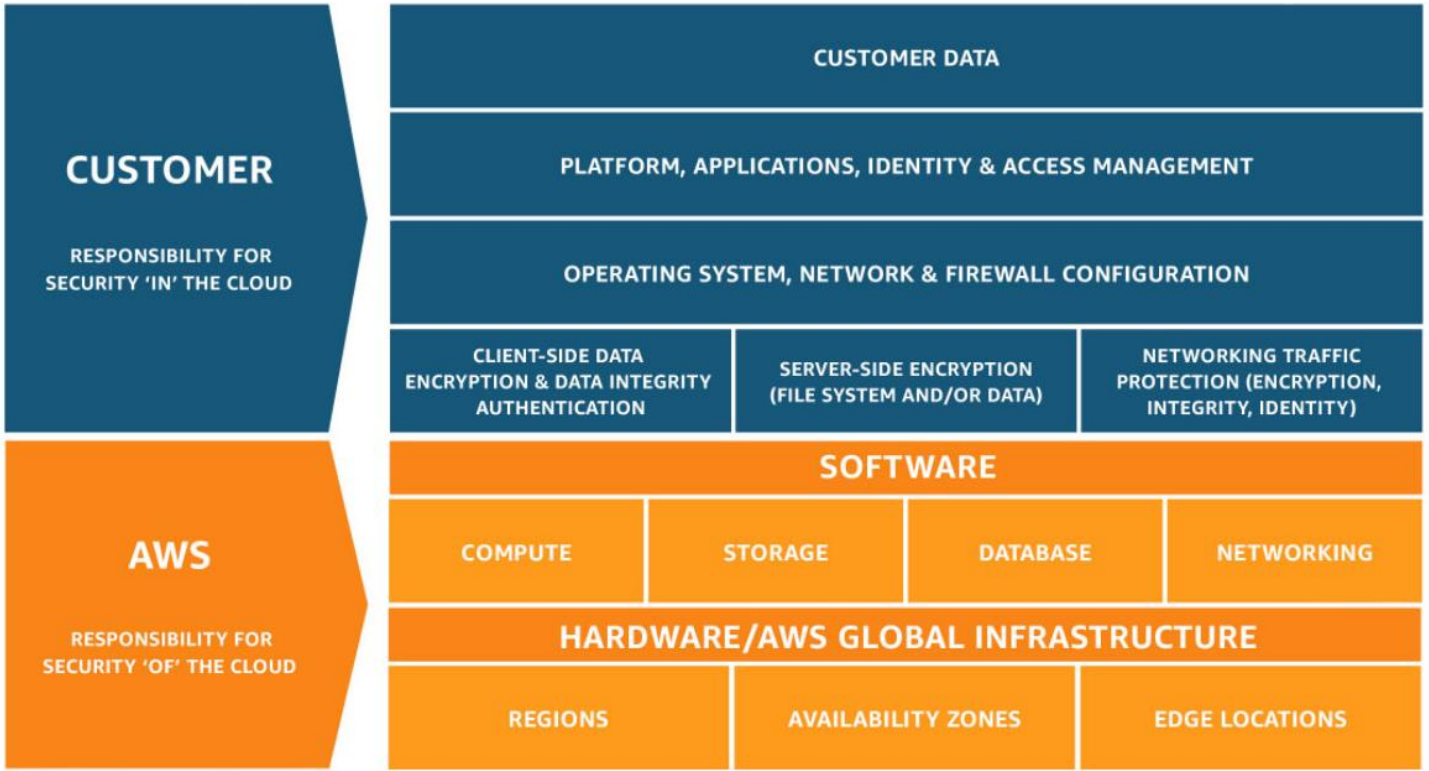
A AWS gerencia a infraestrutura subjacente, incluindo atualizações de software e segurança dos servidores.

Práticas recomendadas

Entretanto, os usuários são responsáveis por:

- Configurar as permissões de acesso aos recursos.
- Definir políticas de controle que protejam os dados.
- Monitorar o uso dos serviços e implementar práticas de segurança, como a criptografia de dados em repouso e em trânsito.

Práticas recomendadas



Práticas recomendadas

Em casa On Premise	Clube IaaS	Casa do amigo PaaS	Buffet SaaS
Quintal	Quintal	Quintal	Quintal
Música	Música	Música	Música
Churrasqueira	Churrasqueira	Churrasqueira	Churrasqueira
Carne	Carne	Carne	Carne
Comida	Comida	Comida	Comida
Farofa	Farofa	Farofa	Farofa
Bebidas	Bebidas	Bebidas	Bebidas
Água	Água	Água	Água

Práticas recomendadas

Exemplos práticos:

EC2 (Elastic Compute Cloud):
O usuário precisa garantir que as instâncias estejam configuradas de maneira segura, incluindo a escolha de sistemas operacionais atualizados, firewalls, e medidas de autenticação, como chaves SSH seguras.

Práticas recomendadas

Exemplos práticos:

S3 (Simple Storage Service): A AWS gerencia a infraestrutura de armazenamento, mas o usuário precisa configurar políticas de acesso para garantir que os dados não estejam publicamente acessíveis sem necessidade e deve usar criptografia para aumentar a segurança dos dados.

Práticas recomendadas

Em resumo:
O modelo de responsabilidade da AWS nos ajuda a entender onde terminam as obrigações da AWS e onde começam as nossas.

A AWS se dedica em manter uma infraestrutura mundial com altos níveis de segurança e o usuário adota práticas de segurança robustas para proteger seus dados e aplicações.

Práticas recomendadas

AWS Well-Architected Framework
O pilar de segurança do framework, cobre áreas essenciais para uma arquitetura segura, incluindo:

Gerenciamento de Identidade e Acesso: Uso de práticas como o princípio do menor privilégio, gerenciamento de usuários e grupos com o AWS IAM (Identity and Access Management).

Práticas recomendadas

Proteção de Dados: Estratégias para proteger dados em repouso e em trânsito, incluindo criptografia e a gestão de chaves usando o AWS Key Management Service (KMS).

Práticas recomendadas

Resposta a Incidentes: Preparação para responder a eventos de segurança com serviços como o AWS CloudTrail, que fornece auditoria e monitoramento das atividades.

Práticas recomendadas

Segurança da Infraestrutura: Uso de serviços como AWS Shield e AWS WAF para proteger contra ataques de negação de serviço e outras ameaças.

Práticas recomendadas

AWS Well-Architected Framework, que é um recurso muito valioso que nos ajuda a entender e aplicar boas práticas de segurança, incluindo o modelo de responsabilidade compartilhada.
Este framework é composto por seis pilares, e um deles o **pilar de segurança**, ajuda os usuários a projetar e operar cargas de trabalho seguras na nuvem.