



IMPLEMENTAÇÃO DE MEDIDAS DE SEGURANÇA

21/09/2023

PHARMANOVA

ANA CLARA R R M BECKER

AGENDA

- 1. Políticas de Controle de Acesso e IAM (Identity and Access Management)
- 2. Monitoramento e Registro de Atividades
- 3. Criptografia de Dados

INTRODUÇÃO



O objetivo do projeto foi elencar 3 medidas de segurança em conjunto dos serviços da AWS, com a finalidade de realizar o aumento da segurança na empresa.



Essas medidas de segurança em conjunto proporcionarão uma defesa mais robusta contra ameaças cibernéticas e irão garantir a proteção adequada dos recursos e dados críticos.



POLÍTICAS DE CONTROLE DE ACESSO E IAM

(IDENTITY AND ACCESS MANAGEMENT | KMS)

QUEM



PODE ACESSAR



O QUÊ ?



- Definirão quais recursos da AWS os usuários e serviços têm permissão de acesso e quais ações podem ser feitas. Isso auxilia no controle de acesso de recursos, dando permissões para usuários ou serviços específicos.
- Para facilitar, o IAM conta com a criação de usuários, grupos, políticas de acesso e roles

Autenticação Multifatorial (MFA):

Exige que os usuários autentiquem suas identidades por meio de uma autenticação de vários fatores, que adiciona uma camada adicional de segurança além de senhas e login (como exemplo, a solicitação de um código enviado por SMS ou e-mail cadastrados). Isso torna mais difícil os ataques às contas dos usuários.



Métodos MFA disponíveis:

1. Chaves de segurança FIDO

(disponibilizadas por terceirizadas)



2. Aplicações de autenticadores virtuais

(Microsoft Authenticator, Google Authenticator, Symantec VIP, entre outros apps compatíveis com Android e iOS)



3. Tokens TOTP de hardware

(tokens fornecidos pela Thales, fornecedor terceirizado)



Rotação de Credenciais:

Implemente a rotação regular de chaves de acesso e segredos, como senhas ou chaves de API, para reduzir o risco associado à exposição de credenciais.





MONITORAMENTO E REGISTRO DE ATIVIDADES

(AWS CLOUDWATCH | AWS CLOUDTRAIL | AMAZON GUARDDUTY)

Amazon CloudWatch

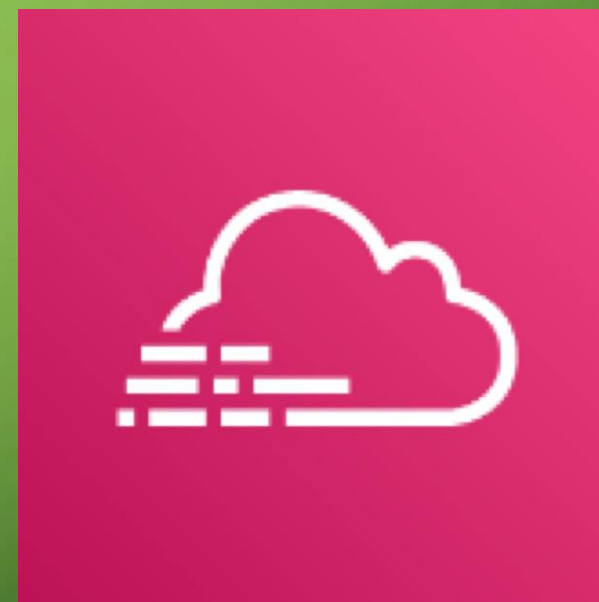
Com ele podemos configurar alertas e monitorar o desempenho, a disponibilidade e a integridade dos recursos da AWS. Este serviço ajudará a identificar e responder a eventos de segurança em tempo real.



Amazon CloudWatch

AWS CloudTrail

Ao ativá-lo obteremos os registros de todas as ações realizadas nas contas da AWS. Ele fornecerá um registro detalhado de atividades que pode ser usado para auditoria de segurança e investigação de incidentes.



Amazon GuardDuty

Utilizado para detectar ameaças de segurança automaticamente, como atividades suspeitas ou tentativas de invasão em diversas fontes de dados (Logs DNS, VPC, CloudTrail, S3, EBS, RDS).

Ele utiliza Machine Learning para prever atividades inesperadas.





AWS KEY MANAGEMENT SERVICE

(AWS KMS)

GERENCIAMENTO DE CHAVES DE CRIPTOGRAFIA

- O KMS é um serviço de controle de chaves utilizado para gerenciar e proteger as chaves de criptografia que protegerão os dados. O AWS KMS também é integrado ao AWS CloudTrail, que ajudará a verificação de quem usou quais chaves, em quais recursos e quando.

Criptografia de dados em REPOUSO

A criptografia protegerá os dados em repouso em serviços como Amazon S3, Amazon RDS e Amazon EBS. Isso garantirá que, mesmo que os dispositivos de armazenamento sejam comprometidos, os dados permaneçam inacessíveis sem a chave de criptografia.



Criptografia de dados em TRÂNSITO

Possibilidade de configurar a criptografia SSL/TLS para proteger os dados em trânsito entre os usuários e os serviços da AWS. Isso impedirá a interceptação de informações confidenciais durante a transferência.



CONCLUSÃO

A implementação dessas ferramentas AWS na PharmaNova Labs tem como esperado o fortalecimento da postura de segurança da empresa, proporcionando uma defesa mais robusta contra ameaças cibernéticas e garantindo a proteção adequada dos recursos e dados críticos.

Recomenda-se a continuidade da utilização das ferramentas implementadas e a busca por novas tecnologias que possam melhorar ainda mais os processos da empresa.



OBRIGADA!

Ana Clara R R M Becker



becker.anaclara@gmail.com
<https://github.com/Ana-Becker/>
www.linkedin.com/in/anacbecker