RELATÓRIO DE IMPLEMENTAÇÃO DE MEDIDAS DE SEGURANÇA AWS

ABSTERGO INDUSTRIES

Setembro / 2023

Data: 05/09/2023

Empresa: Abstergo Industries

Responsável: Daniele Maciel Ferreira

1. Introdução:

Em um mundo cada vez mais digital e interconectado, a segurança da informação é uma preocupação crescente para todas as organizações, independentemente do tamanho ou setor de atuação. A empresa Abstergo Industries reconhece a importância crítica de proteger seus ativos digitais e dados confidenciais contra ameaças cibernéticas em constante evolução. Como parte de nosso compromisso com a segurança, estamos embarcando em um projeto estratégico de fortalecimento de nossas defesas cibernéticas, com foco na utilização dos serviços da Amazon Web Services (AWS) para aprimorar a segurança de nossa infraestrutura na nuvem.

2. Descrição do Projeto: Implementação de Medidas de Segurança

O objetivo deste projeto é implementar três medidas de segurança chave utilizando os serviços da AWS, a fim de fortalecer a postura de segurança da Abstergo Industries. As medidas de segurança escolhidas são as seguintes:

Modelo 1: Amazon GuardDuty

O Amazon GuardDuty é um serviço de segurança gerenciado pela AWS que oferece detecção de ameaças em tempo real, usando análise de comportamento e aprendizado de máquina. Abaixo, um breve resumo de como ele funciona:

- **Análise de Tráfego:** O GuardDuty monitora o tráfego de rede, registros de servidor e eventos de autenticação em busca de atividades suspeitas. Ele analisa esses dados para identificar comportamentos anômalos, como tentativas de acesso não autorizado ou tráfego de comunicação com servidores de comando e controle de malware.

- **Integração com Fontes de Dados:** O serviço se integra automaticamente com fontes de dados como CloudTrail, VPC Flow Logs e DNS logs, permitindo que ele avalie eventos em toda a sua infraestrutura na AWS.

- **Alertas em Tempo Real:** Quando o GuardDuty identifica uma atividade suspeita, ele gera alertas em tempo real, permitindo que você responda rapidamente a ameaças potenciais. Esses alertas incluem informações detalhadas sobre o evento, como endereços IP envolvidos e descrições das ameaças.

- **Investigação e Correção:** Além de alertar sobre ameaças, o GuardDuty também fornece informações detalhadas para ajudar na investigação e mitigação. Isso inclui dados de contexto que facilitam a compreensão do alcance da ameaça e a ação apropriada a ser tomada.

Implementaremos na Abstergo Industries o Amazon GuardDuty para monitorar continuamente nossa infraestrutura na AWS em busca de atividades suspeitas ou maliciosas. Isso inclui a detecção de tentativas de acesso não autorizado, comportamentos anômalos e atividades de malware. A integração do GuardDuty permitirá uma resposta rápida a ameaças em tempo real, ajudando a mitigar potenciais riscos de segurança.

Modelo 2: AWS Identity and Access Management (IAM)

O AWS IAM é um serviço que permite gerenciar o acesso aos recursos da AWS de forma granular e controlada. Veja como ele é implementado:

- **Políticas de Acesso:** Com o IAM, você pode criar políticas de acesso que especificam permissões para ações em recursos da AWS. As políticas são atribuídas a usuários, grupos ou funções, controlando o que eles podem fazer.

- **Princípio do Menor Privilégio:** É uma prática recomendada que você configure políticas do IAM seguindo o princípio do menor privilégio. Isso significa que os usuários ou serviços só têm acesso às ações e recursos necessários para realizar suas funções.

- **Auditoria e Monitoramento:** O IAM oferece recursos avançados de auditoria, permitindo que você acompanhe quem acessou quais recursos e quais ações foram realizadas. Isso é fundamental para rastrear atividades suspeitas.

Fortaleceremos nosso controle sobre identidades e acessos por meio do AWS IAM. Isso inclui a revisão e aprimoramento das políticas de acesso, a implementação do princípio do menor privilégio e a atribuição de permissões granulares. Com o IAM, garantiremos que apenas usuários autorizados tenham acesso aos recursos e ações necessários, reduzindo o risco de acesso não autorizado.

Modelo 3: Amazon Virtual Private Cloud (VPC) com Network Access Control Lists (NACLs) e Security Groups

Uma Amazon Virtual Private Cloud (VPC) é uma rede virtual isolada que permite que você execute recursos na AWS com controle completo sobre a rede. Os Network Access Control Lists (NACLs) e Security Groups são componentes-chave da segurança da VPC:

- **NACLs:** As NACLs são firewalls de nível de sub-rede que controlam o tráfego de entrada e saída em relação às sub-redes da sua VPC. Você pode definir regras de permissão e negação com base em endereços IP, portas e protocolos para proteger o tráfego.

- **Security Groups:** Os Security Groups são firewalls de nível de instância que controlam o tráfego para as instâncias em uma VPC. Eles permitem ou negam o tráfego com base em

regras de segurança que você define. Cada instância pode estar associada a um ou mais Security Groups.

Juntos, esses componentes da VPC garantem a segregação do tráfego de rede, a proteção contra tráfego não autorizado e a criação de ambientes isolados para recursos.

Implementando essas medidas de segurança com sucesso, a Abstergo Industries reforçará a proteção de seus ativos digitais e dados confidenciais, reduzindo os riscos de ameaças cibernéticas e garantindo a integridade e disponibilidade de seus serviços na AWS.

3. Conclusão do Projeto: Implementação de Medidas de Segurança

Ao implementar essas três medidas de segurança na AWS, a Abstergo Industries está dando passos significativos para aprimorar a segurança de nossos sistemas e dados. Reconhecemos que a segurança cibernética é uma jornada contínua e que novas ameaças surgem constantemente. Portanto, estamos comprometidos em manter e aprimorar continuamente nossas medidas de segurança, adaptando-as às evoluções do cenário de ameaças.

Este projeto representa um compromisso com a proteção dos interesses de nossos clientes, parceiros e colaboradores, garantindo que suas informações permaneçam seguras e confidenciais. Além disso, reflete nossa determinação em cumprir os mais altos padrões de conformidade e privacidade de dados.

A Abstergo Industries está ansiosa para colher os benefícios dessas melhorias na segurança, reforçando nossa posição como uma organização comprometida com a proteção de dados e a confiabilidade de nossos serviços.

Assinatura do Responsável pelo Projeto:

Daniele Maciel Ferreira