CIBERSEGURANÇA: EXORCISTAS DO CÓDIGO

FIREWALL CONTRA AMEAÇAS DIGITAIS

Os Sete Pilares da Segurança da Informação segundo a Microsoft

RELTON LEANDRO BARBOSA

Os Sete Pilares da Segurança da Informação segundo a Microsoft

A Microsoft uma das maiores empresas de tecnologia do mundo

A cibersegurança é um dos tópicos mais importantes no mundo digital de hoje. Com o aumento das ameaças e dos ataques cibernéticos, é crucial entender os pilares que garantem a proteção dos dados e sistemas. A Microsoft, definiu sete pilares essenciais para garantir a segurança da informação. Vamos conhecer cada um deles de forma simples e prática.

01

CONFIDENCIALIDADE: PROTEGENDO OS DADOS SENSÍVEIS

O primeiro pilar é a confidencialidade, que garante que somente as pessoas autorizadas tenham acesso a dados sensíveis. Exemplos práticos incluem criptografar e-mails ou informações financeiras, como a Microsoft faz com os dados armazenados em seus servidores.

CONFIDENCIALIDADE: PROTEGENDO OS DADOS SENSÍVEIS

Exemplo real: Em 2020, a Microsoft reforçou sua política de criptografia para proteger os dados de clientes após um ataque de hackers à sua infraestrutura de nuvem. Isso garantiu que, mesmo que os hackers acessassem os sistemas, os dados ainda estivessem protegidos.

02

INTREGRIDADE: GARANTINDO A QUALIDADE DA INFORMAÇÃO

A integridade se refere à garantia de que os dados não foram alterados de maneira indevida, seja por erro ou ataque. A Microsoft utiliza técnicas como verificação de integridade para assegurar que a informação permaneça precisa e confiável.

Integridade: Garantindo a Qualidade da Informação

Exemplo real: Em um incidente de 2017, a Microsoft ajudou a corrigir falhas de integridade de dados quando um software de contabilidade foi comprometido por um malware, garantindo que os registros financeiros não fossem manipulados.

03

DISPONIBILIDADE: MANTER O ACESSO SEMPRE DISPONÍVEL

Disponibilidade significa garantir que a informação e os sistemas estejam acessíveis quando necessário. Isso inclui ter backups e sistemas de recuperação em caso de falhas.

DISPONIBILIDADE: MANTER O ACESSO SEMPRE DISPONÍVEL

Exemplo real: Em 2014, a Microsoft enfrentou um grande ataque cibernético contra seus servidores de nuvem, mas sua infraestrutura de backup garantiu que os clientes não perdessem dados importantes, mantendo os serviços operacionais.

04

AUTENTICIDADE: VERIFICAÇÃO DE IDENTIDADE

Autenticidade assegura que os usuários ou sistemas sejam quem dizem ser. Para isso, a Microsoft usa autenticação multifatorial (MFA), onde o usuário precisa fornecer mais de uma prova de identidade para acessar sistemas.

AUTENTICIDADE: VERIFICAÇÃO DE IDENTIDADE

Exemplo real: Em 2021, um ataque de phishing foi detectado em um dos serviços da Microsoft. No entanto, a autenticação multifatorial ajudou a evitar que os hackers obtivessem acesso, bloqueando a tentativa de invasão.

05

Não Repúdio: Garantia de Responsabilidade

O pilar do não repúdio assegura que uma pessoa ou organização não possa negar a autoria de uma ação, como uma transação ou um envio de e-mail. Isso é fundamental para auditorias e investigações.

Não Repúdio: Garantia de Responsabilidade

Exemplo real: Em 2020, após um incidente de fraude, a Microsoft conseguiu rastrear e confirmar todas as ações executadas por um usuário indevido em sua rede, utilizando os logs de atividades que não podiam ser apagados ou alterados.

.

06

Controle de Acesso: Limitando o Uso de Dados

O controle de acesso estabelece restrições sobre quem pode ver e modificar informações dentro de um sistema. A Microsoft utiliza políticas de controle de acesso com base em funções (RBAC) para limitar a visão de dados sensíveis a pessoas com permissões específicas.

Monitoramento e Resposta: Detectando e Respondendo a Ameaças

Exemplo real: Em um ataque de ransomware ocorrido em 2019, a Microsoft conseguiu limitar o impacto ao restringir o acesso dos invasores a informações críticas por meio de políticas de controle de acesso bem configuradas.

.

07

Monitoramento e Resposta: Detectando e Respondendo a Ameaças

O monitoramento contínuo é essencial para detectar qualquer atividade suspeita. A Microsoft usa ferramentas de monitoramento e resposta automatizada, como o Azure Sentinel, para identificar e neutralizar ameaças rapidamente.

Monitoramento e Resposta: Detectando e Respondendo a Ameaças

Exemplo real: Durante um ataque de DDoS (Distributed Denial of Service) em 2018, a Microsoft identificou o problema em tempo real e neutralizou a ameaça antes que causasse danos aos seus clientes, garantindo a continuidade do serviço..

CONCLUSÃO

Protegendo o Mundo Digital

A segurança da informação é uma responsabilidade compartilhada e requer a implementação de medidas eficazes para proteger dados, sistemas e usuários. Os sete pilares da Microsoft são fundamentais para garantir uma infraestrutura de TI robusta e resistente a ameaças cibernéticas. Ao adotar essas práticas, as empresas podem se proteger de ataques e garantir a segurança dos seus usuários.

AGRADECIMENTOS

OBRIGADO POR LER ATÉ AQUI

Este eBook foi gerado por IA, e diagramado por mim.

Este conteúdo foi gerado para fins didáticos de construção, não realizamos uma validação cuidadosa no conteúdo e podem conter erros cometidos por uma IA.

https://github.com/ReltonLeandro-hub/EBooK-Ciberseguran-a-Exorcistas-do-C-digo/upload/main

Autor: Relton Leandro Barbosa