1.Introdução a Políticas de Segurança

Uma política de segurança é um conjunto de objetivos de segurança para uma empresa que inclui regras de comportamento para os usuários e administradores e especifica os requisitos do sistema. Esses objetivos, regras e requisitos garantem a segurança da rede, dos dados e dos sistemas de computador da organização.

Geralmente, uma política de segurança abrangente realiza várias tarefas como definir regras para o comportamento esperado, garante a consistência nas operações, aquisições e manutenção do sistema, define as consequências jurídicas das violações, dá apoio da gerência à equipe de segurança e outros.

Política de segurança também especifica os mecanismos necessários para atender aos requisitos de segurança, normalmente incluindo o seguinte:

- **Políticas de identificação e autenticação:** Especifica pessoas autorizadas para acesso aos recursos de rede e define procedimentos de verificação.
- **Políticas de senhas:** Garante que as senhas atendam aos requisitos mínimos e sejam alteradas regularmente.
- **Políticas de uso aceitável:** Identifica os recursos e o uso da rede que são aceitáveis para a empresa. Também pode identificar ramificações para violações de política.
- **Políticas de acesso remoto:** Identifica como os usuários remotos podem acessar uma rede e o que é remotamente acessível
- **Políticas de manutenção de rede:** Especifica procedimentos de atualização de sistemas operacionais e de aplicativos de usuários finais dos dispositivos de rede
- **Políticas de tratamento de incidentes:** Descreve como os incidentes de segurança são tratados.

As **políticas de uma empresa** estabelecem as regras de conduta e as responsabilidades dos trabalhadores e dos empregados, além de protegerem os direitos dos trabalhadores, bem como os interesses comerciais dos empregadores.

As **políticas de funcionários** são criadas e mantidas pela equipe de recursos humanos para identificar o salário dos funcionários, o cronograma de pagamento, os benefícios dos funcionários, o horário de trabalho, as férias e muito mais. Muitas vezes eles são fornecidos a novos funcionários para revisar e assinar.

Uma **política de segurança BYOD** deve ser desenvolvida para realizar os objetivos do programa BYOD, identificar quais funcionários podem trazer seus próprios dispositivos, identificar quais dispositivos serão suportados, identificar o nível de acesso que os funcionários são concedidos ao usar dispositivos pessoais, descrever os direitos de acesso às atividades permitidas ao pessoal de segurança no dispositivo, identificar quais regulamentos devem ser cumpridos ao usar dispositivos de funcionários e identificar as salvaguardas a serem implementadas se um dispositivo for comprometido.

Impedir os criminosos virtuais é difícil, porém, empresas e o próprio governo começaram a tomar medidas coordenadas para limitar ou se defender destes criminosos. Geralmente, suas ações incluem criar bancos de dados abrangentes de vulnerabilidades conhecidas do sistema e assinaturas de ataques, estabelecendo sensores de avisos precoce e redes de alerta, compartilhando informações de inteligência cibernética, estabelecendo padrões de gerenciamento de segurança e da informação e promulgando novas leis para desencorajar violações de dados e ataques cibernéticos.

1.1 Banco de dados de vulnerabilidade

O banco de dados de vulnerabilidades e exposições comuns (CVE) é um exemplo do desenvolvimento de um banco de dados nacional.

1.2 MITRE

A **Mitre Corporation** mantém uma lista de vulnerabilidades e exposições comuns (CVE) usadas por organizações de segurança proeminentes, facilitando o compartilhamento de dados. O CVE serve como um dicionário de nomes comuns para vulnerabilidades de segurança cibernética conhecidas.

1.3 FIRST

É uma empresa de segurança que une uma variedade de equipes de resposta a incidentes de segurança do computador provenientes de organizações governamentais, comerciais e educacionais, com o objetivo de promover a cooperação e a coordenação de compartilhamento de informações, prevenção de incidentes e a reação rápida.

1.4 CIS

O Center for Internet Security é um ponto focal para prevenção, resposta e recuperação de ameaças cibernéticas para governos estaduais, locais, tribais e territoriais por meio do MS-ISAC, que oferece alertas de ameaças cibernéticas 24 horas por dia, 7 dias por semana, identificação de vulnerabilidades e mitigação e resposta a incidentes.

2.Sistemas de aviso inicial

O projeto Honeypot é um exemplo de criação de sistemas de alerta precoce. O projeto fornece um HoneyMap, que exibe visualizações em tempo real de ataques.

2.1 Compartilhar inteligência cibernética

O compartilhamento amplamente disseminado de inteligência cibernética, programa InfraGrad, é uma parceria entre o FBI e o setor privado. Os participantes são dedicados a compartilhar informações e inteligência para evitar ataques cibernéticos.

3.Norma ISM

Os padrões ISO/IEC 27000 são exemplos de padrões de gerenciamento de segurança da informação. Os padrões fornecem uma estrutura para implementar medidas de segurança digital dentro de uma empresa.

4.Novas leis

O grupo ISACA monitora as leis aprovadas em relação à segurança digital. Essas leis podem abordar a privacidade individual para proteção de propriedade intelectual.

Um programa de conscientização sobre segurança é extremamente importante para uma organização. Um funcionário pode não ser intencionalmente malicioso, mas desconhecer quais são os procedimentos adequados. Há várias formas de implementar um programa de treinamento formal, como tornar o treinamento de segurança parte do processo de integração do funcionário, realizar sessões de treinamento presenciais, complemento com cursos on-line e outros.