Segurança da Informação e Proteção de dados

Segurança da informação é a proteção de informações importantes contra acesso não autorizado, divulgação, uso, alteração ou interrupção. Ajuda a garantir que os dados organizacionais confidenciais estejam disponíveis para usuários autorizados, permaneçamconfidenciais e mantenham sua integridade.

Baseada em princípios estabelecidos há décadas, a segurança da informação evolui constantemente para proteger ambientes cada vez mais híbridos e multi-nuvem em um cenário de ameaças em constante mudança. Dada a natureza evolutiva dessas ameaças, várias equipes precisam trabalhar juntas para atualizar a tecnologia e os processos usados nessa defesa.

1º Ameaças e Vulnerabilidades:

Uma vulnerabilidade é qualquer ponto fraco na infraestrutura de TI (tecnologia da informação)que os adversários possam explorar para obter acesso não autorizado aos dados. Por exemplo,os hackers podem aproveitar os erros de um programa de computador para introduzir um malware ou código malicioso em um aplicativo ou serviço legítimo. Os usuários humanos também podem constituir vulnerabilidades em um sistema de informação. Por exemplo, ciber criminosos podem manipular os usuários para compartilhar informações confidenciais pormeio de ataques de engenharia social, como phishing.

Por outro lado, uma ameaça é qualquer coisa que possa comprometer a confidencialidade, integridade ou disponibilidade de um sistema de informação. Uma ameaça cibernética é umaameaça que explora uma vulnerabilidade digital. Por exemplo, um ataque de negação de serviço (DoS) é uma ameaça cibernética em que os ciber criminosos sobrecarregam parte do sistema de informação de uma empresa com tráfego, causando falhas.

As ameaças também podem ser físicas. Desastres naturais, ataques físicos ou armados e até mesmo falhas sistêmicas de hardware são considerados ameaças ao sistema de informação deuma empresa.

2º Engenharia Social:

Engenharia Social é o nome utilizado para definir o método mais habitual de se obter informações confidenciais de acesso a sistemas restritos a usuários autorizados. É o caso em que uma pessoa de má-fé abusa da ingenuidade ou da confiança de um usuário para persuadi-la a fornecer informações sensíveis, como números de cartões de crédito, senhas, documentospessoais, entre outros. Essa categoria de fraude ou de crime digital também pode acontecer dentro das empresas. O criminoso começa a ter contato com um colaborador, ou então utiliza artimanhas para induzir essa pessoa a realizar uma ação que favoreça o ataque.

Apesar de o nome Engenharia Social sugerir técnicas sofisticadas ou mirabolantes, a maioriados ataques é feita de forma simples. Não é preciso nem mesmo encontrar e

explorar falhasem sistemas de segurança, além de não acontecer apenas em ambientes digitais.

2.1 Alguns exemplos são:

Baiting

Essa técnica costuma acontecer com mais recorrência em ambientes de trabalho. Nela, o criminoso infecta um dispositivo (geralmente um pendrive) com um malware e o deixa em algum lugar aleatório. Um colaborador encontra o dispositivo e o conecta, por curiosidade, emalgum PC ou Notebook para conferir o conteúdo. Geralmente, a vítima também instala os arquivos do pendrive em seu dispositivo para saber do que se trata. Fazendo isso, o criminoso passa a ter acesso a praticamente todos os sistemas do dispositivo infectado.8

Phishing

Apesar de ser uma técnica antiga da Engenharia Social, o e-mail de phishing ainda é muito eficiente. Ele ocorre quando um ciber criminoso forja comunicações com a vítima, que acreditaestar diante de um e-mail legítimo. Os fraudadores costumam se passar por bancos ou empresas de cartão de crédito, por exemplo. Eles solicitam informações sensíveis, como senhas e dados de cadastro, ou mesmo pedem para a pessoa fazer a instalação de falsos softwares de segurança, por exemplo.

2.2Algumas Prevenções:

Evitar compartilhar informações:

Quanto menos divulgar informações, ainda que elas não pareçam tão confidenciais assim, melhor. Detalhes que parecem sem importância pode ser a última peça do quebra-cabeça quefaltava para o ciber criminoso cometer o seu ataque. As informações confidenciais, seja sobre você ou a sua empresa, não podem ser divulgadas para pessoas desconhecidas, seja por telefone, seja online ou pessoalmente. É fundamental sempre verificar a identidade do interlocutor. Procure descobrir se a pessoa realmente é quem ela diz ser. Analise a procedência das credenciais e, se não for possível realizar essas análises, solicite o auxílio de outra pessoa. Enfim, evite tomar decisões duvidosas por conta própria.

Evitar cliques com risco potencial:

Sites falsos entram e saem do ar com uma rapidez muito grande. São páginas criadas para atrair vítimas, e isso pode funcionar, já que esses sites muitas vezes tem uma aparência muitosimilar às páginas das grandes empresas — algo que costuma acontecer com frequência no e-commerce. Evitar navegar por essas páginas com procedência suspeita e também evite clicar em links recebidos por mensagem de texto (SMS) ou por e-mail é melhor. Prefira fazer pesquisas por conta própria quando se trata de oportunidades de negócios ou de promoções. Por fim, analisar os sites em que você navega verificando os recursos de segurança e páginas institucionais é muito eficiente.

Cuidado com anexos:

Os anexos são um problema muito grande porque, para acessar, muitas vezes precisamos fazer o download para dentro do nosso dispositivo. Essa ação favorece acessos não autorizados e infeções, facilitando bastante o trabalho do criminoso. Por meio de programasmaliciosos escondidos, ele conseguirá acesso a todos os dados e informações contidos na máquina e no sistema. Só é aconselhável baixar anexos provenientes de fontes conhecidas e de confiança. Mesmo assim, se for possível, vale apenas solicitar a visualização do arquivo ou documento, evitando fazer o download direto para a máquina.

3º Proteção e Criptografia:

A segurança em sistemas IoT é crucial, dada a crescente interconexão de dispositivos e a coletamassiva de dados. A criptografia é uma ferramenta fundamental para proteger a comunicação entre dispositivos IoT.

Uma estrutura de proteção robusta para um sistema IoT deve considerar os seguintes aspectos:

Autenticação: Verificar a identidade de dispositivos e usuários para garantir que apenasentidades autorizadas tenham acesso ao sistema.

Confidencialidade: Garantir que os dados transmitidos estejam protegidos contra acesso nãoautorizado.

Integridade: Assegurar que os dados não sejam alterados durante a transmissão.

Disponibilidade: Manter o sistema funcionando de forma contínua e resistente a ataques.

Existem alguns métodos de Criptografia para Dispositivos IoT, os Assimétricos e os simétricos.**Simétricos:** Esse método usa as mesmas chaves tanto para criptografar dados inseridos pela pessoa usuária em um formulário, como para descriptografá-los em um sistema ou dispositivoautorizado.

Chaves: Utiliza uma única chave tanto para criptografar quanto para descriptografar os dados.
Vantagens: Rápida e eficiente em termos computacionais.

Desafios: A gestão de chaves pode ser complexa, especialmente em grandes redes IoT.

Assimétricos: Esse tipo de criptografia adota pares de chaves, sendo uma pública e uma privada, para criptografar e descriptografar dados. Dessa forma, cada parte envolvida na comunicação deve possuir um par de chaves. A pública será conhecida por todas as partes,enquanto a privada deve ser mantida protegida.

Chaves: Utiliza um par de chaves, uma pública e outra privada.
Vantagens: Permite a autenticação de dispositivos e a troca segura de chaves.

Desafios: Mais lenta que a criptografia simétrica e exige maior poder computacional.

A segurança em sistemas IoT é um desafio complexo, mas fundamental para garantir a confiabilidade e a proteção dos dados. Ao implementar uma estrutura de proteção robusta eutilizando as técnicas de criptografia adequadas, é possível minimizar os riscos de ataques e garantir a segurança dos dados.

4º Normas de segurança:

A segurança da informação é um tema cada vez mais crítico, especialmente com a crescente digitalização e a proliferação de dispositivos conectados. Para garantir a proteção de dados einformações, é fundamental adotar normas e políticas de segurança robustas.

Normas de Segurança Aplicáveis:

Existem diversas normas e regulamentações que estabelecem requisitos mínimos para a segurança da informação. Algumas das mais relevantes incluem:

Lei Geral de Proteção de Dados (LGPD): A LGPD, presente em diversos países, estabelece princípios e regras para a proteção de dados pessoais, incluindo coleta, armazenamento, tratamento e compartilhamento.

ISO/IEC 27001: Essa norma internacional define um Sistema de Gestão de Segurança da Informação (SGSI), fornecendo um conjunto de controles para proteger ativos de informação.

PCI DSS: É um conjunto de requisitos de segurança para organizações que manipulam dadosde cartões de pagamento.

Políticas para o Gerenciamento de Dados e Informações:

As políticas de segurança devem ser personalizadas para cada organização, levando em consideração suas especificidades e o nível de risco a que estão expostas. No entanto, algumas políticas comuns incluem:

Política de Senhas: Estabelecer requisitos mínimos para criação de senhas fortes, como combinação de letras maiúsculas e minúsculas, números e caracteres especiais,além de proibir o reuso de senhas.

Política de Acesso: Definir regras claras para o acesso a sistemas e informações, incluindo a necessidade de autenticação forte, autorização baseada em papéis e a revogação de acessos quando necessário.

Política de Backup: Estabelecer um plano de backup regular para garantir arecuperação de dados em caso de perda ou danos.

Política de Segurança de Dispositivos: Definir regras para o uso de dispositivos pessoais em ambientes corporativos, incluindo a instalação de software de segurança e acriptografia de dados.

Ao implementar essas normas e políticas, as organizações podem reduzir significativamente o risco de incidentes de segurança e proteger seus dados e informações.

REFERÊNCIAS

https://www.ibm.com/br

https://blogbr.clear.sale

https://www.alura.com.br

https://www.gov.br/governodigital

https://www.planalto.gov.br