PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Av. Brasil, 2023

Funcionários, Belo Horizonte – MG – CEP 30040-002

GERENCIAMENTO DE REDES DE COMPUTADORES

Antônio Gabriel Batista Vieira

Diogo Junio Pinheiro dos Santos

Everton Rezende Spadaccini

Gustavo Felipe Borges Pereira
Luiz Gustavo Giovanini

IMPLEMENTAÇÃO DE UMA REDE SEGURA DE COMPUTADORES

Projeto apresentado ao curso de graduação de Redes de Computadores da Instituição Pontifícia Universidade Católica de Minas Gerais, com objetivo de implementar uma rede segura de computadores.

Orientador: Luiz Alberto Ferreira Gomes

1. Introdução

Este documento tem como objetivo a formalização das diretivas de segurança da informação. Por meio da orientação e do estabelecimento das diretrizes do setor de Tecnologia da Informação para proteger seus ativos de quaisquer violações, a Política de Segurança da Informação visa determinar os padrões de comportamentos relacionados à segurança dos dados e as necessidades do negócio para proteção legal da entidade e de seus indivíduos. O principal propósito de uma Política de Segurança é informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação.

Os riscos que a aplicação deste documento pretende evitar são:

· Vazamento de informações corporativas;

· Quebra de autenticação de rede;

· Modificações e perdas de dados e programas;

· Destruição, violação ou perda de recursos e instalações da infraestrutura;

· Interdições ou interrupções de serviços essenciais;

· Roubo/furto de ativos;

· Utilização indevida dados;

· Acessos não autorizados.

2. Requisitos de Segurança

Os requisitos de segurança da informação foram elaborados após análise minuciosa das informações inerentes aos processos existentes na corporação, que contenham um fluxo de atividades correlacionadas e sua tratativa, seja ela direta ou realizada por fontes terceiras (comissão de segurança). Desta maneira sua segmentação continuou seguindo os conceitos básicos existentes em diversos outros documentos sendo os principais aspectos a serem considerados:

Confidencialidade:

Para promover a segurança dos dados, foram criadas ações preventivas atribuindo acesso as informações somente para pessoas autorizadas. Uma segmentação de níveis, onde os acessos aos dados crescem de acordo com o grau hierárquico, levando em consideração a distribuição de conteúdo por áreas, e conexões entras as mesmas. Outro ponto importante é a categorização dos dados de acordo com seu impacto nas operações.

É indicado treinar os colaboradores que possuam acesso e são responsáveis pelos conteúdos mais críticos, para que eles manipulem esses dados com cuidado e tenham maior noção sobre os riscos.

Em relação à infraestrutura, é possível aumentar as camadas de segurança integrando sistemas de criptografia de dados, autenticação de dois fatores e verificação biométrica.

Integridade:

Para reforçar a integridade nos processos de TI, é importante tomar medidas e reforçar a infraestrutura de proteção de dados. Isso pode ser feito dos seguintes modos:

- Estipulando controles de acesso para colaboradores;
- Definindo permissões de arquivos;

- Utilizando controles de versões para retornar arquivos a versões anteriores em caso de perda de dados inesperadas;
- Implantando sistemas de verificação para detectar alterações nos dados na rede por conta de eventos não ocasionados por interação humana (falhas em equipamentos, distúrbios elétricos e etc.);
- Usando somas de verificação (checksum) para checar a integridade de dados enviados por canais com ruídos ou armazenados em diferentes meios por determinado período;
- Disponibilizando backups prontos para recuperar dados alterados, entre outras medidas.

Disponibilidade:

A disponibilidade pode ser garantida através da implantação de processos rápidos e periódicos, como por exemplo: manutenções de hardware e software, voltados para a preservação de dados direta ou indiretamente. Outro requisito é a redundância e sobrevivências de alguns aspectos da infraestrutura, como um link principal de internet e um outro de redundância para disponibilidade da rede.

Há também a necessidade de uma equipe de crise para que ações como: plano de recuperação de desastres (ataques virtuais, catástrofes naturais e etc.), tenham seu escopo de ações predefinidas para minimizar danos.

3. Desenvolvimento de Políticas de Segurança

A política deve especificar os mecanismos através dos quais estes requisitos possam ser alcançados. Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos. Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido.

a) Acesso à rede e autenticação:

-Utilizar senhas de alta complexidade atendendo os requisitos mínimos de segurança (Letras maiúsculas e minúsculas, números e caracteres especiais), metodologias MFA (autenticação de múltiplos fatores exemplo: "Microsoft Authenticator");

-Níveis de acesso por setor, cargo e função. (Permissão inicial de nível baixo para todos os usuários e escalonamento gradativo.);

-Redes internas (cabeadas e WIFI) com autenticação automática através de equipamento (notebook, celular) que faz parte do domínio irão se autenticar. Hardware não autenticado na rede interna terão apenas acesso à internet.

b) Proteção de dados:

-Políticas de criptografia de dados, adequação de backup de acordo com a parametrização do negócio, seja ele realizado localmente, ou na nuvem. Mantendo os dados alocados virtualmente em território nacional, para quesitos legais;

-Backup regulares, sendo executados em modo FULL 2 vezes por mês e backups incrementais 3 vezes por semana;

- Serviço de link dedicado para garantir a segurança do transporte de dados através de serviços complementares.

c) Segurança da infraestrutura:

-Software de monitoramento e observabilidade;

-Escala de atualizações de software e hardware para garantir a segurança dos hosts e sua vida útil;

-Acompanhamento de licenças.

d) Conscientização e treinamento:

Políticas de anti-phising trimestrais, com levantamento de falhas e treinamento de melhores práticas para usuários.

Dicas de complexidade de senhas e boas práticas de TI, através de e-mails mensais.

4. Documentação e Comunicação

É essencial documentar todas as políticas de segurança de maneira clara e acessível. A comissão de segurança deve elaborar um documento com as normas estabelecidas, incluindo explicações minuciosas e exemplos práticos.

Além disso, é vital informar os usuários da rede sobre a política de segurança, assegurando que estejam cientes das diretrizes e responsabilidades. Esse processo pode ser feito através de treinamentos e a distribuição do documento.

5. Avaliação e Melhoria Contínua

Criação de um comitê de segurança da informação onde serão realizadas reuniões trimestrais para discussão de práticas eficazes, feedbacks, análises de dados, atualizações da política e melhoria contínua.