Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

Prof. Robson Calvetti

João Luiz Da Silva e Rafael Tiago Scisci Arciénega

RA: 82420546 e 824216105

1. Reconhecimento dos Recursos Vitais

A SecureNet necessita dos seguintes recursos essenciais para funcionar:

Tecnologia da Informação:

Servidores na Nuvem: Guardam informações vitais e constituem a base para backup e supervisão.

Firewall e Instrumentos de Defesa: Fundamentais para se defender de ataques cibernéticos.

Redes de Vigilância: Analisam o fluxo de tráfego dos clientes em tempo real.

Gestão de Recursos Humanos:

Equipe de Assistência Técnica: Fundamental para o acompanhamento e intervenção em situações de emergência.

Especialistas em Segurança Digital: Encarregados de configurar os sistemas e recuperar informações.

Equipe de Comunicação: Assegura a clareza e comunicação ágil com clientes e partes interessadas.

Informações e Documentos Importantes:

Dados de Recuperação dos Clientes: Abrange informações protegidas e cópias de segurança diárias.

Operações Procedimentais: Protocolos de segurança e respostas a incidentes.

Documentação de Planos de Continuidade e Riscos.

Equipe de Assistência Técnica: Fundamental para o acompanhamento e intervenção em situações de emergência.

Especialistas em Segurança Digital: Encarregados de configurar os sistemas e recuperar dados.

2. Análise de Impacto Empresarial (BIA)

Eventos que provocam rupturas:

1. Falha de Servidor na Nuvem: Poderia levar à perda temporária de informações e à suspensão do monitoramento.

Efeito: Durante o período de paralisação, os clientes tornam-se suscetíveis a ataques, resultando em prejuízos financeiros e de imagem.

Meta de Tempo para Recuperação (RTO): 2 horas.

Objetivo de Recuperação de Ponto: 15 minutos.

2. Ataque Digital (por exemplo, ransomware): Impede o acesso a informações e prejudica a proteção dos clientes.

Efeito: Perigo de perda de informações dos clientes e diminuição da confiança, além de possíveis penalidades por descumprimento de normas.

RTO: 30 minutos.

RPO: Cinco minutos.

3. Ausência de Conexão (Internet): Interrompe a supervisão.

Efeito: Durante o período de paralisação, os clientes tornam-se suscetíveis a ataques, resultando em prejuízos financeiros e de imagem.

RTO: 30 minutos de duração.

3. Métodos de Recuperação Estratégicos

Para reduzir os efeitos, a SecureNet sugere as táticas a seguir:

Replicação de Sistemas na Nuvem: Salvaguarda automática das informações dos clientes em diversas áreas geográficas.

Defesa Avançada: Firewall moderno, detecção de invasões e defesa contra ransomware.

Plano de Comunicação de Emergência: Distribuição de uma nota padrão aos clientes em até 30 minutos após um incidente.

Formação Continuada da Equipe: Realizações mensais de respostas a incidentes cibernéticos para assegurar que a equipe esteja preparada.

Conexão de Internet Redundante: Os provedores secundários de internet asseguram que a conexão nunca seja completamente interrompida.

4. Estratégia de Ação

1. Defeito em Servidor na Nuvem:

Passo 1: Comunicar imediatamente à equipe de Tecnologia da Informação.

Passo 2: Encaminhamento de dados para o servidor replicado.

Passo 3: Comunicar aos clientes a retomada dos serviços.

Equipe de Tecnologia da Informação e Comunicação.

2. Ciberataque:

Passo 1: Implementar protocolos de isolamento para conter a ofensiva.

Passo 2: Recuperar o backup mais recente e seguro.

Passo 3: Analisar as vulnerabilidades e aplicar correções.

Encarregados: Especialistas em segurança e tecnologia da informação.

3. Ausência de Conexão:

Passo 1: Conferir e ativar as conexões secundárias.

Passo 2: Conectar-se ao provedor de internet principal.

Equipe de Tecnologia da Informação.

5. Verificação do Plano

1. Para assegurar sua efetividade, o plano passará por um teste de crise a cada dois meses. A atividade inclui:

2. Simulação de Intrusão Cibernética: A equipe de Tecnologia da Informação simula uma invasão hipotética, na qual deve implementar o isolamento e a recuperação de dados.