Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

Profº Robson Calvetti

Lucas Gabriel Hora Benetti - 825134041

Aula 6 - Atividade 1

Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

1. Políticas de Acesso e Controle de Usuários

Política de Senhas Fortes:

Proposta: Exigir senhas com um mínimo de 10 caracteres, combinando letras maiúsculas, minúsculas, números e símbolos. Impor a troca obrigatória a cada 90 dias e evitar a reutilização de senhas por pelo menos 12 ciclos.

Justificativa: Reduz a probabilidade de acesso não autorizado por meio de ataques de força bruta, dicionário ou por vazamento de credenciais externas, garantindo a confidencialidade.

Princípio do Menor Privilégio:

Proposta: Conceder aos usuários apenas as permissões de acesso (leitura, escrita, execução) estritamente necessárias para o desempenho de suas funções. O acesso a dados sensíveis deve ser rígidamente controlado e auditado.

Justificativa: Minimiza o risco de que um erro humano ou o comprometimento de uma conta (phishing, malware) resulte em acesso indevido ou alteração de dados críticos, limitando o dano potencial.

Controle de Acesso Físico:

Proposta: Restringir e registrar o acesso físico a áreas críticas, como a sala de servidores, apenas a pessoal autorizado.

Justificativa: Protege os ativos de hardware e informação contra roubo, danos físicos ou acesso não autorizado, assegurando a integridade e disponibilidade dos sistemas.

2. Política de Uso de Dispositivos Móveis e Redes

Controle de Acesso à Rede Corporativa (Wi-Fi):

Proposta: O acesso à rede Wi-Fi deve ser restrito a dispositivos autorizados e autenticados. Redes de convidado/visitante devem ser implementadas e isoladas da rede principal de produção.

Justificativa: Garante que apenas usuários e equipamentos validados possam interagir com os sistemas internos, prevenindo a propagação de ameaças ou acessos não autorizados a partir de dispositivos externos.

Segurança para Dispositivos Pessoais (BYOD - Bring Your Own Device):

Proposta: Dispositivos pessoais utilizados para acessar dados da empresa devem possuir obrigatoriamente proteção por senha/biometria e criptografia de disco. A empresa deve ter a capacidade de apagar remotamente dados corporativos em caso de perda ou roubo do dispositivo.

Justificativa: O uso de BYOD traz benefícios, mas aumenta o risco de violação de dados corporativos. A política mitiga esse risco, garantindo a confidencialidade e a segurança dos dados da organização.

Uso Aceitável de Internet e E-mail:

Proposta: Proibir o download ou a instalação de softwares não autorizados e o envio de informações confidenciais por e-mails não criptografados.

Justificativa: Reduz a superfície de ataque a malware, ransomware e ataques de engenharia social (phishing), protegendo os sistemas e a informação.

3. Diretrizes para Resposta a Incidentes de Segurança

Notificação Imediata de Incidentes:

Proposta: Qualquer funcionário que suspeitar ou identificar um incidente de segurança (ex: e-mail de phishing, perda de dispositivo, acesso não autorizado) deve notificá-lo imediatamente ao ponto de contato designado (ex: Gerente de TI).

Justificativa: A comunicação e notificação eficientes são essenciais para iniciar rapidamente a gestão de incidentes, minimizar o dano, conter a violação e iniciar a recuperação o mais breve possível.

Procedimento Básico de Resposta:

Proposta: O time responsável deve seguir um fluxo de resposta estruturado, incluindo as etapas de: 1. Contenção (isolar o sistema afetado); 2. Erradicação (remover a causa); 3. Recuperação (restaurar o serviço).

Justificativa: Fornece um roteiro organizado para lidar com incidentes, garantindo que a resposta seja eficaz e que a causa raiz do problema seja tratada, prevenindo recorrências.

Análise e Registro de Incidentes:

Proposta: Todos os incidentes devem ser documentados, incluindo data, hora, sistemas afetados, como foi contido e as ações tomadas.

Justificativa: O registro permite a análise de padrões de ataque e ajuda a identificar e corrigir fraquezas na segurança (melhoria contínua), além de fornecer trilhas de auditoria para conformidade.

4. Política de Backup e Recuperação de Desastres

Frequência e Verificação de Backup:

Proposta: Realizar backups completos dos dados críticos diariamente. Os backups devem ser periodicamente verificados para garantir a integridade e a capacidade de restauração.

Justificativa: É um requisito fundamental para a disponibilidade da informação. Garante que a empresa possa recuperar dados rapidamente em caso de falha de

hardware, erro humano ou ataque cibernético (como ransomware), assegurando a continuidade dos negócios.

Implementação da Regra 3-2-1:

Proposta: Exigir 3 cópias dos dados (original + 2 backups), em 2 tipos de mídia diferentes, com 1 cópia armazenada fora do local (off-site ou em nuvem).

Justificativa: A redundância e o armazenamento off-site protegem contra desastres localizados e falhas catastróficas, maximizando a garantia de que os dados estarão acessíveis quando necessário.

Plano de Teste de Recuperação (DRP - Disaster Recovery Plan):

Proposta: O plano de recuperação de desastres deve ser documentado e testado, no mínimo, anualmente.

Justificativa: Assegura que os procedimentos de recuperação funcionem conforme o esperado e que o tempo de inatividade após um desastre (RTO) seja aceitável para o negócio, mitigando o risco de interrupções prolongadas.