Segurança Cibernética

A segurança cibernética protege os dados e sistemas da empresa contra ameaças como vazamentos, fraudes e sequestros de informações (ransomware). Um único ataque pode paralisar operações, causar grandes prejuízos financeiros e abalar a reputação da empresa.

Por exemplo, empresas que sofreram vazamento de dados perderam clientes e enfrentaram multas milionárias por violar leis como a LGPD.

Investir em segurança digital é essencial para garantir a confiança dos clientes, a continuidade do negócio e o cumprimento das obrigações legais.

1. Senhas Seguras e Políticas de Troca Periódica

Senhas são a primeira linha de defesa contra acessos não autorizados. Boas práticas incluem:

- Criar senhas complexas (com letras maiúsculas, minúsculas, números e símbolos);
- Evitar usar senhas óbvias como "123456" ou nomes pessoais;
- Trocar as senhas periodicamente (por exemplo, a cada 3 meses);
- Não reutilizar a mesma senha em vários sistemas.

2. Uso Seguro de E-mails e Links Suspeitos

O e-mail é uma das principais portas de entrada para ataques como phishing. Boas práticas incluem:

- Não clicar em links ou abrir anexos de remetentes desconhecidos;
- Verificar erros de ortografia e endereços de e-mail suspeitos;
- Nunca fornecer senhas ou dados pessoais por e-mail;
- Denunciar mensagens suspeitas ao setor de TI.

3. Políticas de Uso de Dispositivos Móveis (BYOD – Bring Your Own Device)

Permitir que colaboradores usem seus próprios dispositivos (como celulares e notebooks) no trabalho traz flexibilidade, mas exige regras claras, como:

- Instalar softwares de segurança (antivírus, VPN);
- Separar dados pessoais e corporativos;
- Proibir o uso de redes Wi-Fi públicas sem proteção;
- Autorizar o acesso apenas a sistemas essenciais.

4. Adoção de Autenticação Multifatorial (MFA)

A autenticação multifatorial é um método de segurança que exige mais de uma forma de verificação, como:

- Senha + código enviado por SMS;
- Senha + reconhecimento facial ou biometria;
- Senha + app autenticador.

3. Procedimentos de Segurança

3.1. Suspeita de Ataques (ex: phishing):

- Não clicar em links ou anexos suspeitos.
- Comunicar imediatamente o setor de TI.
- Isolar o e-mail e registrar a ocorrência para análise.

3.2. Proteção de Dados Confidenciais:

- Restringir o acesso apenas a pessoas autorizadas.
- Usar criptografia para armazenar e transmitir dados.
- Evitar o uso de dispositivos não autorizados.

3.3. Backups e Integridade:

- Realizar backups regulares (diários, semanais).
- Armazenar cópias em locais seguros (nuvem + mídia externa).
- Testar periodicamente a restauração dos backups.

3.4. Violação de Segurança:

- Identificar rapidamente o tipo e origem da ameaça.
- Isolar o sistema afetado para evitar propagação.

- Notificar os responsáveis e iniciar o plano de resposta.
- Registrar o incidente e revisar medidas preventivas.

4. Treinamento e Conscientização

É essencial implementar um programa contínuo de capacitação para os colaboradores. O objetivo é reforçar a importância da segurança cibernética, ensinar boas práticas no uso da tecnologia e orientar sobre como identificar e reportar ameaças (como e-mails falsos, comportamentos suspeitos ou falhas de sistema). A conscientização constante reduz os riscos causados por erros humanos.

5. Plano de Resposta a Incidentes Cibernéticos

Um bom plano deve definir etapas claras para lidar com incidentes de segurança. Isso inclui:

- **Identificação:** Detectar e classificar o tipo de ameaça.
- **Resposta:** Isolar sistemas afetados, conter o impacto e notificar os responsáveis.
- **Recuperação:** Restaurar sistemas e dados com segurança.
- **Análise pós-incidente:** Avaliar causas e ajustar políticas para evitar novas ocorrências.

Ass.: Yago de Lima Pavan