Análise Crítica da Solução de TI: Fortalecimento da Segurança

Matheus Moniakas Ra: 82422355
Gustavo Almeida RA: 824138271
Paulo Passiano RA:824219946

Controle de Acesso: Físico e Lógico

Lógico

O controle de acesso lógico dos sistemas carece de autenticação multifator (MFA), tornando os acessos remotos vulneráveis. A falta de relatórios detalhados sobre
tentativas de acesso falhas impede a análise de segurança e a gestão de credenciais é frágil.

Físico

O controle de acesso físico à edificação apresenta vulnerabilidades significativas. A ausência de catracas eletrônicas nos depósitos e garagem expõe o local a
intrusões, e a limitação das câmeras prejudica a vigilância.
A falta de redundância no sistema de registro também é preocupante.

Riscos Físicos

1 Segurança dos Depósitos

A falta de controle nos depósitos e garagem facilita a entrada de intrusos, aumentando o risco de roubo ou vandalismo. A implementação de catracas eletrônicas associadas ao crachá dos funcionários e câmeras adicionais são essenciais.

2 Risco de Incêndio

A proximidade do gerador e botijões de gás eleva o risco de incêndios e explosões. É crucial segregá-los com barreiras físicas, realizar manutenções periódicas no gerador e instalar sensores de fumaça e temperatura.

3 Prevenção e Treinamento

O treinamento de segurança física para todos os funcionários, simulando situações de risco, é crucial para preparar a equipe para lidar com emergências e fortalecer a cultura de segurança.

Ameaças Físicas: Prevenção e Proteção

Incêndio e Explosão

O gerador e os botijões de gás próximos elevam o risco de incêndio ou explosão. Adicionar sprinklers automáticos e detectores de gás, além de fortificar os portões e entradas com vigilância 24 horas, é crucial.

Roubo e Vandalismo

A vulnerabilidade dos depósitos e garagem exige medidas de segurança mais robustas, como portões reforçados, câmeras e vigilância 24 horas. A implementação de catracas eletrônicas também é essencial.

Desastres Naturais

A falta de menção a estruturas resistentes a desastres naturais é preocupante. É fundamental avaliar o risco de desastres naturais na região e tomar medidas para proteger a edificação e os dados.

Ameaças Lógicas: Combater Ataques e Erros

1

Ataques Ransomware

O armazenamento de dados sensíveis torna a empresa um alvo crítico para ataques ransomware. É fundamental implementar treinamento regular em cibersegurança para todos os funcionários e utilizar soluções de Endpoint Detection and Response (EDR).

2

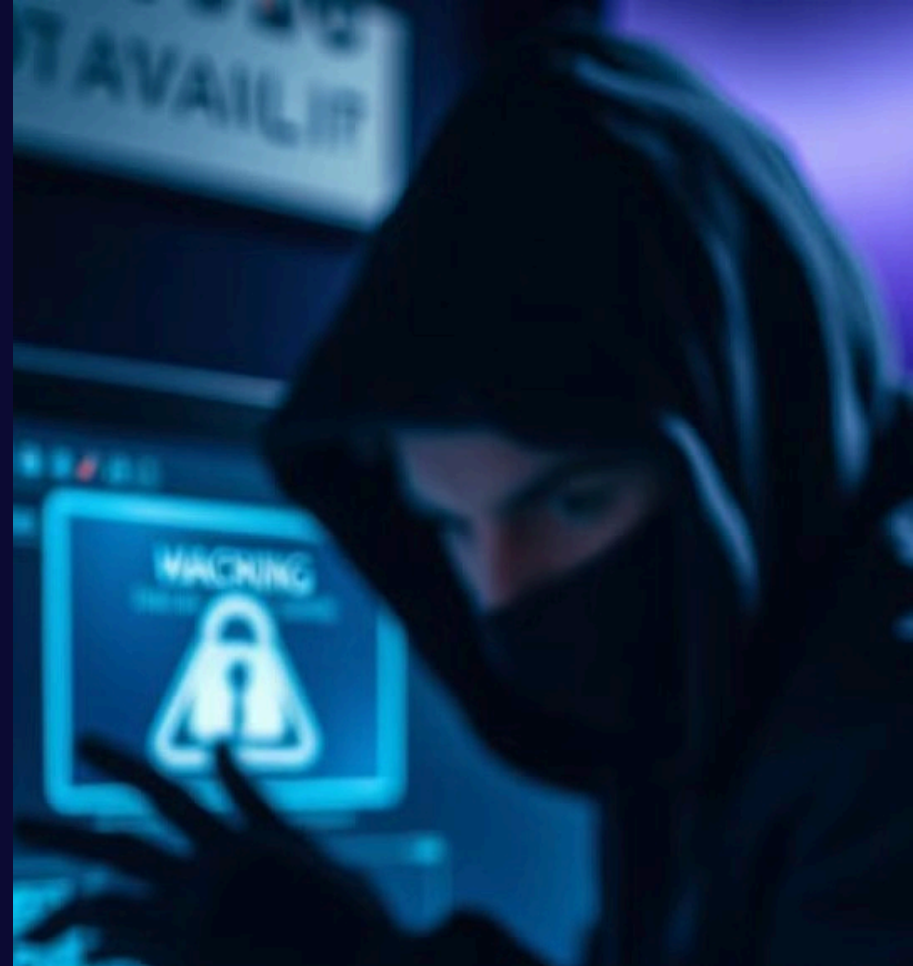
Invasões Externas

A ausência de MFA deixa os sistemas mais expostos a invasões externas. É crucial implementar a MFA para todos os acessos remotos e revisar as políticas de segurança para englobar práticas modernas, como Zero Trust.

3

Erro Humano

Credenciais comprometidas podem ser exploradas por hackers. O treinamento em segurança cibernética e a utilização de gerenciadores de senhas podem prevenir esses erros.



Protegendo Contra Riscos Lógicos

Firewall

A implementação de firewalls avançados e segmentação de rede é essencial para restringir acessos não autorizados e proteger os sistemas de invasões externas.

Backup em Nuvem

A centralização dos backups no prédio de TI representa um risco de perda total em caso de ataque. É fundamental configurar backups automáticos em nuvem, garantindo segurança das informações.

MFA

A ausência de MFA eleva o risco de invasões externas. A implementação da MFA para todos os acessos remotos é essencial para fortalecer a segurança.

Monitoramento Contínuo

A falta de monitoramento ativo permite que tentativas de acesso mal-intencionadas passem despercebidas. É essencial adotar sistemas de monitoramento contínuo com alertas em tempo real.

Plano de Contingência: Garantir Continuidade

Infraestrutura

O plano de contingência deve garantir a continuidade do negócio em situações críticas. É essencial manter um gerador secundário e um data center secundário fora do prédio, garantindo a redundância.

1

2

Processos e Comunicação

Definir equipes de resposta rápida com planos de ação para cada tipo de incidente e simular situações de crise regularmente. Estabelecer um canal redundante para comunicação com funcionários e clientes.

Solução de TI: Uma Abordagem Estratégica

1

Backup Estratégico

A centralização dos backups é uma vulnerabilidade. É essencial expandir a infraestrutura para incluir armazenamento em nuvem e locais externos, garantindo redundancia geografica

2

Monitoramento Avançado

O monitoramento e auditoria são insuficientes. É fundamental adotar ferramentas SIEM (Security Information and Event Management) para análise de eventos em tempo real e fortalecer a vigilância.