Introdução

A segurança de uma empresa depende de uma combinação eficaz de controles físicos e lógicos, visando proteger ativos, dados e operações contra ameaças internas e externas. A OfficeSolutions, com suas operações baseadas em um modelo digital e dependente de infraestrutura física, apresenta um cenário complexo, mas passível de melhorias significativas. Este relatório busca analisar os controles de acesso e riscos relacionados à segurança física e lógica, identificando vulnerabilidades e propondo soluções práticas e eficientes. Além disso, aborda um plano de contingência para assegurar a continuidade dos negócios em situações adversas, sempre considerando os custos e viabilidade das mudanças.

1. Controle de acesso físico à edificação

O que se esperaria encontrar:

- **Sistemas robustos**: Controle eletrônico para entradas e saídas.
- **Vigilância constante**: Monitoramento por câmeras em todos os acessos críticos, especialmente nos depósitos e garagem.
- **Auditoria de acessos**: Registro detalhado de entradas/saídas, associando funcionários e veículos aos horários.

Críticas ao cenário descrito:

- **Controle insuficiente nos depósitos e garagem**: Portões abertos manualmente expõem vulnerabilidades significativas.
- **Câmeras limitadas**: Apenas uma câmera na entrada principal é inadequada para monitorar toda a instalação.
- **Ausência de redundância**: Um único ponto de falha para registros (servidor de TI) pode comprometer o monitoramento em caso de problemas técnicos.

Propostas de mudança:

1. **Implementar catracas eletrônicas nos depósitos e garagem**, associadas ao crachá dos funcionários.
2. **Adicionar câmeras nos pontos de acesso** e corredores interligados para melhor vigilância.
3. **Manter backups dos registros de câmeras em local externo** ao prédio da TI.
4. **Automatizar portões com acesso restrito**, integrando o controle ao sistema eletrônico.

---

2. Controle de acesso lógico dos sistemas

O que se esperaria encontrar:

- Autenticação multifator (MFA) para acessos remotos.
- Relatórios detalhados de **tentativas de acesso bem-sucedidas e falhas**.
- Senhas fortes e políticas de troca periódica.

Críticas ao cenário descrito:

- **Falta de autenticação multifator (MFA)**: Isso torna os acessos remotos vulneráveis.
- **Relatórios incompletos**: Desativar informações sobre acessos falhos prejudica a análise de segurança.
- **Gestão de credenciais frágil**: Não foi mencionada nenhuma política de rotação de senhas ou uso de ferramentas de gerenciamento.

Propostas de mudança:

1. **Ativar autenticação multifator (MFA)** para todos os acessos remotos.
2. **Reativar relatórios de acessos falhos** e incluir monitoramento em tempo real.
3. **Implementar uma política de rotação de senhas** (ex: troca obrigatória a cada 90 dias).
4. **Auditoria mensal dos acessos por um sistema automatizado**, para identificar comportamentos anômalos.

---

3. Riscos físicos ao negócio

Vulnerabilidades e intensidade dos riscos:

- **Depósitos e garagem**: Acesso manual facilita intrusões.
- **Câmeras limitadas**: Risco de atividades não monitoradas.
- **Gerador e botijões de gás próximos**: Eleva o risco de incêndios e explosões.

Propostas de mitigação:

1. **Segregar áreas de alto risco**, como o gerador e botijões de gás, instalando barreiras físicas.
2. **Manutenção periódica do gerador** para garantir sua operação durante emergências.
3. **Implementar sensores de fumaça e temperatura** em todos os prédios.
4. **Treinamento de segurança física** para todos os funcionários, simulando situações de risco.

---

4. Riscos lógicos ao negócio

Vulnerabilidades e intensidade dos riscos:

- **Ausência de MFA**: Eleva o risco de invasões externas.
- **Backups centralizados**: Risco de perda total em caso de ataque ao prédio de TI.
- **Falta de monitoramento ativo**: Tentativas de acesso mal-intencionadas podem passar despercebidas.

Propostas de mitigação:

1. **Configurar backups automáticos em nuvem**, garantindo redundância geográfica.
2. **Adotar sistemas de monitoramento contínuo** com alertas em tempo real.
3. **Realizar testes de intrusão periodicamente**, avaliando vulnerabilidades no sistema.
4. **Implementar firewalls avançados e segmentação de rede**, restringindo acessos não autorizados.

---

5. Plano de contingência

Objetivo: Garantir continuidade do negócio em situações críticas.

- **Infraestrutura**:
    - Manter um gerador secundário, caso o principal falhe.
    - Criar um data center secundário fora do prédio.
- **Processos**:
    - Definir equipes de resposta rápida com planos de ação para cada tipo de incidente.
    - Simular situações de crise regularmente.
- **Comunicação**:
    - Estabelecer um canal redundante para comunicação com funcionários e clientes.

---

6. Ameaças físicas ao ambiente e negócios

Principais ameaças:

- **Incêndio ou explosão**: Gerador e botijões próximos elevam o risco.
- **Roubo ou vandalismo**: Depósitos e garagem vulneráveis.
- **Desastres naturais**: Nenhuma menção a estruturas resistentes.

Soluções:

1. **Adicionar sprinklers automáticos** e detectores de gás.
2. **Fortificar portões e entradas** com vigilância 24h.
3. **Planejar evacuação em emergências**, com saídas claramente marcadas.

---

7. Ameaças lógicas ao ambiente e negócios

Principais ameaças:

- **Ataques ransomware**: Alvo crítico por armazenar dados sensíveis.
- **Invasões externas**: Sem MFA, sistemas estão mais expostos.
- **Erro humano**: Credenciais comprometidas podem ser exploradas.

Soluções:

1. **Implementar treinamento regular em cibersegurança** para todos os funcionários.
2. **Utilizar soluções de Endpoint Detection and Response (EDR)** para identificar ameaças.
3. **Segregar dados críticos** em servidores isolados.

---

8. Análise crítica da solução de TI

Deficiências identificadas:

- **Centralização total dos backups**.
- **Falta de MFA e relatórios detalhados**.
- **Monitoramento e auditoria insuficientes**.

Medidas propostas:

1. **Expandir a infraestrutura de backup** para incluir armazenamento em nuvem e locais externos.
2. **Revisar as políticas de segurança** para englobar práticas modernas, como Zero Trust.
3. **Adotar ferramentas SIEM (Security Information and Event Management)** para análise de eventos em tempo real.

Conclusão

Após uma análise abrangente, identificamos que a OfficeSolutions enfrenta vulnerabilidades significativas em seus controles de acesso físico e lógico, bem como riscos associados à centralização de dados e infraestrutura. As propostas apresentadas, como a implementação de autenticação multifator, automação de controles físicos e a diversificação de backups, visam reduzir esses riscos de maneira sustentável. Reforçar a segurança por meio de tecnologias avançadas e treinamentos regulares permitirá não apenas mitigar ameaças, mas também fortalecer a confiança dos clientes e parceiros no modelo de negócios da empresa. Com essas mudanças, a OfficeSolutions estará preparada para operar de forma segura e resiliente diante de possíveis desafios futuros.