Estudo de Caso OfficeSolutions

Sistemas Computacionais e Segurança

Gabriel Pessini - 824129852
Gustavo Pinheiro de Amorim Melo - 824134456
João Gobbi - 824145710
Matheus Henrique da Costa e Silva - 82410661
Matheus Santos - 824212452
Matheus Yusuke Minakawa - 82416000

Sumário

Controle de Acesso Físico	Slide 1-3
Controle de Acesso Lógico	Slide 4-6
Análise de Riscos Físicos	Slide 7-9
Análise de Riscos Digitais	Slide 10-12
Estratégias de Contingência	Slide 13-14
Vulnerabilidades Físicas	Slide 15-18
Vulnerabilidades Lógicas	Slide 19-22
Medidas para melhorar a segurança das operações de TI	Slide 23-25
Custos	Slide 26

01

Análise do controle de acesso físico à edificação

Controle de acesso físico à edificação

Fragilidades Identificadas:

Entrada de Pedestres:

- Catraca simples com autenticação por crachá, oferecendo segurança mínima.

Entrada de Veículos:

- Controle manual na entrada de veículos, suscetível a falhas humanas.
- Ausência de monitoramento na doca, dificultando a supervisão de movimentações.

Soluções

Catracas com autenticação biométrica:

Substituir as catracas atuais por catracas com autenticação biométrica.

Automatização do controle de veículos:

Portões automáticos com sensores sensores de identificação e reconhecimento de placas

Instalação de câmeras na garagem:

Monitoramento visual dos acessos e movimentação de itens.

Cadastro eletrônico de veículos e pessoas:

Gerenciamento em tempo real de entradas e saídas de veículos e pessoas, tendo controle de quem está no local e restringindo o acesso a áreas sensíveis.

02

Análise do controle de acesso lógico dos sistemas

Críticas ao controle de acesso lógico dos sistemas

01

Ausência de Autenticação Multifator (MFA)

02

Desativação de Logs de Tentativas Falhas

03

Falta de Controle no Acesso aos Backups

O que esperaríamos encontrar

01
Autenticação Multifator

02
Segregação de Funções

03
Monitoramento de Logs e Alertas

04
Política de Senhas Fortes

05
Atualizações e Patches

06
Uma VPN (Rede Privada Virtual)

03

Análise dos Riscos Envolvidos por Ameaças Físicas

Possíveis Riscos Envolvidos por Ameaças Físicas

01

Acesso Físico Não Controlado aos Depósitos e Garagem

02

Concentração dos Servidores e Backups em um Único Local

03

Ausência de Câmeras de Segurança Adequadas

04

Gerador com Autonomía Limitada

Possíveis Melhorias de Acordo Com a Análise dos Riscos Físicos

01

Instalação de Câmeras Adicionais

02

Separação Física dos Backups

03

Automatização do Controle de Acesso

04

Aumento da Capacidade do Gerador

04

Análise dos Riscos Envolvidos por Ameaças Digitais

Ameaças identificadas

1- Acesso remoto sem MFA
- Possibilidade de invasão por credenciais comprometidas.

2- Desativação de alertas de tentativas de acesso remoto falhas
- Dificuldade em detectar e responder a ataques de força bruta ou acesso não autorizado.

3 - Backup no mesmo local dos servidores
- Perda simultânea de dados em caso de incêndio, ataque físico ou digital

4- Controle remoto sem criptografia avançada
- Interceptação de dados durante conexões remotas.

Efeitos Prioritárias

01
Implementar MFA e VPNs seguras

02
Criar backups em locais externos

03
Criptografia e monitoramento

05

Estratégias de Contingência

Sugestões para segurança

01
Backups Externos

Realizar backups diários e armazenados em locais externos.

02
Autenticação MultiFatores

Autenticação Multifatores é essencial para a prevenção contra acessos não autorizados.

03
Reativação de Logs

Realizar os monitoramentos de padrões suspeitos e relatórios automatizados.

04
Redundância Energética

Ampliar suporte do gerador para períodos prolongados

06

Vulnerabilidades Físicas

Ameaças

01

Acesso não autorizado a áreas restritas

02

Roubo ou vandalismo de equipamentos e materiais

03

Incêndio ou explosão

04

Perda de dados ou informações confidenciais

Vulnerabilidades

01

Controle de acesso simples (catraca) e falta de biometría

02

Ausência de câmeras de segurança em áreas críticas

03

Acesso remoto não seguro (senha única)

04

Gerador e botijões de gás próximos ao refeitório

05

Falta de sistema de detecção de incêndio e sprinklers

06

Ausência de protocolo de resposta a incidentes de segurança

07

Desligamento da funcionalidade de relatório de tentativas de acesso falhas

Mitigação

01

Implementar sistema de controle de acesso mais seguro

02

Instalar câmeras de segurança em áreas críticas

03

Implementar autenticação de dois fatores para acesso remoto

04

Realocar o gerador e botijões de gás para área mais segura

05

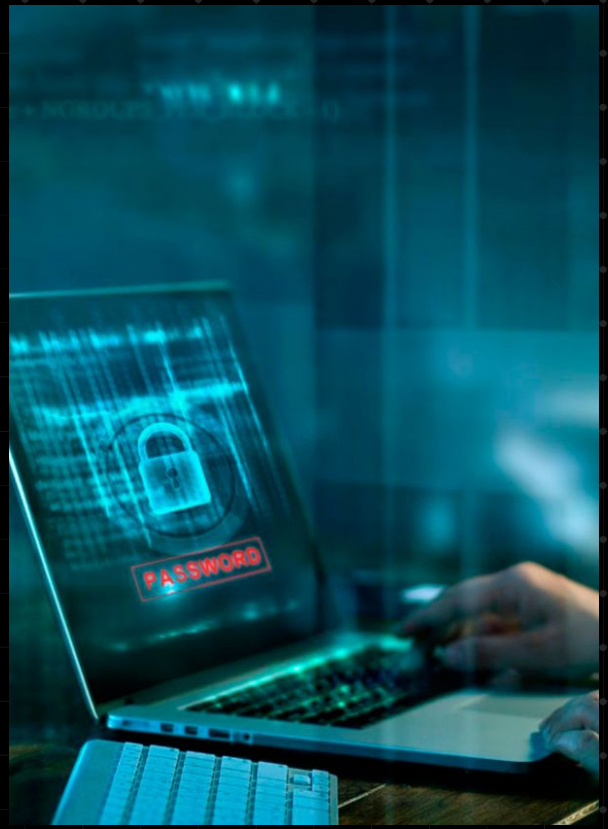
Instalar sistema de detecção de incêndio e sprinklers

06

Desenvolver protocolo de resposta a incidentes de segurança

07

Vulnerabilidades Lógicas



Ameaças

01

Ataques Cibernéticos

02

Vazamento de dados da empresa

03

Perda de dados ou informações confidenciais

Vulnerabilidades

01

Todos os servidores são acessíveis externamente

02

Acesso total ao sistema remotamente

03

Entrada no sistema utilizando somente usuário e senha

04

Não informa os Logs de Tentativas Falhas

05

Falta de Controle no Acesso aos Backups

Mitigação

01

Privilégios de acesso conforme cargo

02

Entrada remota através da máquina da empresa ou liberação de intermediario

03

Implementar autenticação de dois fatores para acesso remoto

04

Informar Logs de falha e de onde veio a tentativa

05

Utilizar backups em cloud ou em cloud híbrida

06

Criptografia dos dados

08

Medidas para melhorar a segurança das operações de TI

Ameaças identificadas

1- Ausência de segurança em backups

Problema: Backup armazenado apenas no prédio da TI, vulnerável a desastres.
Solução: Implementar estratégia com multi copias, locais e off-sites

2- Controle remoto vulnerável

Problema: Acesso remoto com autenticação básica.
Solução: Autenticação multifator (MFA), VPN segura e monitoramento em tempo real.

3- Desligamento do monitoramento de acessos falhos

Problema: Falta de monitoramento de tentativas de acesso falhas.
Solução: Reativar monitoramento e configurar alertas automáticos.

4- Controle físico inadequado

Problema: Controle manual e poucas câmeras de segurança.
Solução: Instalar mais câmeras, leitores de crachá e monitoramento integrado.

5- Dependência do gerador na garagem

Problema: Gerador compartilhado e vulnerável a falhas de abastecimento.
Solução: Instalar UPS, monitorar combustível e avaliar gerador dedicado.

Medidas Complementares

01

Criptografia de dados.

02

Segmentação de rede.

03

Treinamento em cibersegurança para funcionários

Orçamento

Item		Custo Estimado (R$)	Categoria
Catracas biométricas (x3)	R$	16.000,00	Infraestrutura
Câmeras de segurança (minimo 12)	R$	18.000,00	Infraestrutura
Portão automático	R$	11.000,00	Infraestrutura
Sistema de RFID ou reconhecimento de placas	R$	4.000,00	Infraestrutura
Software de cadastro e gerenciamento (veículos e pessoas)	R$	6.000,00	Infraestrutura
Servidor para armazenamento	R$	20.000,00	Infraestrutura
Gerador	R$	120.000,00	Infraestrutura
Treinamento de funcionários em segurança	R$	10.000,00	Treinamento
Contratação de analistas de segurança ou vigilantes	R$	5.000,00	Treinamento
Sistema de monitoramento e relatórios	R$	5.000,00	Software e Licenciamento
Licenças para softwares de controle de acesso	R$	15.000,00	Software e Licenciamento
Custos Totais (sem implementação)	**R$**	**230.000,00**	
Energia elétrica adicional (câmeras, servidores, etc.) - Mensal	R$	2.000,00	Manutenção
Manutenção de equipamentos (Semestral)	R$	16.000,00	Manutenção
Custos Adicionais Mensal	**R$**	**4.666,67**	
Mão de obra (Todas as implementações)	R$	52.600,00	Implementação
Custos Total	**R$**	**282.600,00**	

Obrigado!

Sistemas Computacionais e Segurança

Gabriel Pessini - 824129852
Gustavo Pinheiro de Amorim Melo - 824134456
João Gobbi - 824145710
Matheus Henrique da Costa e Silva - 82410661
Matheus Santos - 824212452
Matheus Yusuke Minakawa - 82416000