Atividade: Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

Objetivo: Os alunos do grupo devem se colocar no papel de consultores de segurança e criar um conjunto básico de políticas de segurança da informação para uma pequena empresa fictícia composto por:

Políticas de acesso e controle aos usuários;
Políticas de uso de dispositivos móveis e redes;
Diretrizes para resposta a incidentes de segurança;
Política de backup e recuperação de desastres;

Entrega: Documento com as Políticas propostas, detalhando as justificativas de cada uma.

Documento: Desenvolvimento de Políticas de Segurança para uma Pequena Empresa - Escola Particular

Atividade: Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

1. Introdução

O objetivo deste documento é desenvolver uma política prática de segurança da informação para uma escola privada fictícia que se concentra na proteção de ativos digitais, dados confidenciais de alunos e funcionários e na garantia da continuidade de suas operações. Uma estratégia sólida de segurança da informação é fundamental para proteger os dados contra ameaças cibernéticas, acesso não autorizado e outros riscos de segurança. As políticas aqui desenvolvidas têm em conta a dimensão e as necessidades específicas da organização, abrangendo áreas-chave como controlo de acessos, utilização de dispositivos móveis, resposta a incidentes de segurança, backup e recuperação de desastres.

2. Políticas de acesso e controle de usuários

Objetivo: Garantir que apenas utilizadores devidamente autorizados tenham acesso a dados e sistemas sensíveis, promover a separação de funções e minimizar o risco de acessos inadequados e vulnerabilidades

Política proposta:

Autenticação do usuário: Todos os usuários, incluindo funcionários, professores e administradores, devem ser autenticados para acessar qualquer sistema de TI escolar. Isso inclui sistemas de gestão acadêmica, e-mail corporativo e sistemas de controle financeiro. A autenticação deve incluir um login exclusivo (nome de usuário) e uma senha forte que siga as diretrizes de complexidade (pelo menos 12 caracteres, usando letras maiúsculas e minúsculas, números e símbolos).

Exemplo de senha: A@scHoOl2023!

Autenticação multifator (MFA): Para acessar informações confidenciais, como dados médicos de alunos ou registros financeiros, a autenticação multifator deve ser realizada usando métodos como um token de autenticação, um código enviado por mensagem de texto ou um aplicativo de autenticação.

Gerenciamento de permissões e separação de funções:

Todos os usuários devem ser divididos em grupos funcionais com níveis de permissão específicos. O corpo docente tem acesso limitado a informações acadêmicas sobre os alunos pelos quais são responsáveis, mas não a dados financeiros. A equipe de gestão tem acesso apenas aos dados financeiros e administrativos, e não ao desempenho acadêmico individual. Usar o princípio do menor privilégio é imperativo. Os funcionários devem ter apenas o nível de acesso necessário para executar suas tarefas.

Exemplo: Os Recursos Humanos poderão acessar e modificar os dados dos funcionários, mas não os registros financeiros ou as notas dos alunos.

Monitoramento de acesso:

Os sistemas de TI registram todas as tentativas de acesso a sistemas críticos. As equipes de TI devem monitorar os logs de acesso semanalmente, incluindo logins com falha e atividades incomuns. Em caso de atividade suspeita, um alerta será enviado à administração.

Justificativa:

Fortes controles de acesso protegem as escolas contra acesso não autorizado e vazamento de dados. Ao implementar a MFA e garantir o gerenciamento granular de permissões, a organização reduziu significativamente o risco de ameaças internas e externas. O monitoramento do acesso permite a detecção precoce de possíveis violações de segurança.

3. Política de Dispositivos Móveis e Uso da Internet

Objetivo: Desenvolver orientações claras para a utilização segura de dispositivos e redes móveis, garantindo os benefícios da mobilidade e da conectividade sem comprometer a integridade e a confidencialidade dos dados.

Política proposta: Dispositivos móveis pessoais (BYOD – traga seu próprio dispositivo): As escolas estão a permitir que funcionários e professores utilizem os seus próprios dispositivos móveis para trabalhar, desde que sigam regras de segurança rigorosas.

Requisitos de BYOD:

Os dispositivos devem ser criptografados para proteger dados confidenciais armazenados localmente. Eles devem ter o software antivírus e de segurança mais recente instalado. O acesso aos sistemas escolares através de dispositivos móveis só é permitido através de ligação VPN (rede privada virtual), o que garante uma ligação segura, mesmo em redes públicas.

Exemplo de aplicação: Os professores que utilizam tele móveis pessoais para aceder ao sistema de gestão académica residencial devem passar por VPN e utilizar MFA.

Uso de redes Wi-Fi com segurança:

A escola fornecerá diferentes redes Wi-Fi para diferentes grupos:

Rede de gestão: Para uso exclusivo da gestão, com criptografia WPA3 e monitoramento contínuo do tráfego. Somente dispositivos autorizados podem se conectar a esta rede.

Rede Educacional: Para uso de professores e alunos em atividades acadêmicas, com controles de largura de banda e filtros de conteúdo para evitar uso indevido.

Rede de Visitantes: Acesso disponível para convidados e prestadores de serviços, com tempo restrito de utilização e sem ligação direta a sistemas críticos da instituição.

Exemplo de Medida de segurança: A rede administrativa será separada das demais redes, assegurando que dispositivos conectados à rede pública não possam acessar sistemas internos.

Monitoramento de Rede e uso de Internet:

A equipe de TI deve empregar ferramentas de monitoramento de rede para detectar tráfego anômalo, tentativas de acesso não autorizado e infrações das políticas de uso da internet (como downloads de software não autorizado).

Exemplo: Um alerta será gerado caso um aluno ou professor tente acessar sites restritos ou realizar downloads de arquivos potencialmente prejudiciais.

Justificativa:

Dispositivos móveis, quando fora de controle, podem representar uma fonte significativa de vulnerabilidade, pois são mais propensos a roubo ou perda. A adoção de criptografia e VPN garante a confidencialidade dos dados, mesmo fora do ambiente escolar. O uso de redes Wi-Fi segmentadas ajuda a proteger a rede.

Diretrizes para Resposta a Incidentes de Segurança:

Objetivo: Elaborar e manter um Plano de Resposta a Incidentes (PRI) detalhado. O PRI incluirá:

Identificação de possíveis incidentes (ex.: ataques de ransomware, violações de dados, falhas sistêmicas).

Procedimentos para a contenção rápida do incidente (como desconectar os sistemas afetados da rede).

Notificação das partes interessadas (direção da escola, alunos e pais, caso os dados dos alunos estejam comprometidos).

Análise pós-incidente para identificar vulnerabilidades exploradas e planejar melhorias.

Equipe de Resposta a Incidentes:

Uma equipe de resposta será designada, composta por membros da TI, administradores e, se necessário, consultores externos de segurança. Cada incidente deverá ser escalado conforme sua gravidade, e a equipe atuará de acordo com as diretrizes do PRI.

Exemplo de Incidente: Em caso de ataque de ransomware, a equipe de resposta deve isolar os sistemas comprometidos, avaliar o impacto e iniciar a restauração dos backups.

Notificações e Relatórios:

Todos os incidentes devem ser documentados em relatórios minuciosos, que incluam as ações executadas e o tempo de resposta. A escola tem a obrigação de comunicar alunos e pais em casos de vazamento de dados pessoais.

Exemplo de Ação Pós-Incidente: Após a contenção de um ataque cibernético, a escola fará uma revisão de seus controles de segurança para identificar vulnerabilidades e implementar melhorias necessárias.

Justificativa:

A resposta rápida e eficiente a incidentes de segurança é crucial para minimizar os impactos e assegurar a continuidade dos serviços. Um Plano de Resposta a Incidentes bem estruturado e uma equipe treinada garantem que a escola mantenha sua resiliência diante de ameaças emergentes.

Política de backup e recuperação de desastres:

Objetivo: Garantir que todos os dados críticos da escola estejam protegidos e possam ser recuperados rapidamente em caso de falhas, ataques ou desastres.

Backup diário e incremental:

A escola deve realizar backups completos de todos os dados sensíveis, como registros acadêmicos, financeiros e de saúde, diariamente, tanto em armazenamento local quanto em servidores na nuvem. Backups incrementais (que capturam apenas as alterações) serão feitos a cada hora, a fim de reduzir a janela de perda de dados.

Armazenamento de Backups em locais Seguros:

O backup será armazenado em dois locais distintos, provendo um backup criptografado, além do backup em nuvem. Isto permitirá redundância e recuperação em caso de situações físicas de desastre, como incêndio e enchentes.

Exemplo: Se os servidores locais da escola forem corrompidos por um ataque ransomware, os backups poderão ser rapidamente restaurados, utilizando a cópia armazenada no cliente (destino remoto de backup).

Testes de Recuperação Regulares:

A escola deve testar sua capacidade de recuperação de backup pelo menos uma vez por trimestre, testes de recuperação podem ajudar a identificar problemas na restauração antes que um incidente ocorra.

Plano de Recuperação de Desastres (PRD):

O PRD detalhará os procedimentos para restaurar as operações da escola em caso de catástrofe, como um incêndio que destruiria a infraestrutura local. O plano incluirá o tempo máximo aceitável para recuperação (RTO - Recovery Time Objective) e o volume máximo de dados que pode ser perdido sem grandes impactos (RPO - Recovery Point Objective).

Justificativa:

A tecnologia da informação e a política de backup e recuperação de desastres ajudariam a escola a recuperar rapidamente todos os dados essenciais em caso de falha. Portanto, protegeria a escola conta a perda irreparável de informação vital e restauraria as operações educacionais.

6. Conclusão

As políticas apresentadas neste documento fornecem uma abordagem abrangente e robusta à segurança da informação em uma escola privada. A implementação adequada dessas políticas garantirá uma escola preparada para as ameaças internas e externas, pronta para proteger seus dados e manter a continuidade dos negócios. Dada a natureza evolutiva da ameaça cibernética, a revisão regular dessas políticas será crítica para garantir que se mantenham relevantes e eficazes.