Auditoria de Segurança - Botium Toys

Lista de Verificação de Avaliação de Controles

Controle	Possui?
Menor Privilégio	Não
Planos de recuperação de desastres	Não
Políticas de senha	Sim
Separação de funções	Não
Firewall	Sim
Sistema de detecção de intrusão (IDS)	Não
Backups	Não
Software antivírus	Sim
Monitoramento manual, manutenção e intervenção para sistemas legados	Sim
Criptografia	Não
Sistema de gerenciamento de senhas	Não
Fechaduras (escritórios, vitrines, armazéns)	Sim
Vigilância por circuito fechado de televisão (CFTV)	Sim
Detecção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.)	Sim

Lista de Verificação de Conformidade

Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS)

Melhor prática	Adere?
Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes.	Não
As informações do cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro.	Não
Implemente procedimentos de criptografia de dados para proteger melhor os pontos de contato e os dados das transações com cartão de crédito.	Não
Adote políticas seguras de gerenciamento de senhas.	Não

Regulamento Geral de Proteção de Dados (RGPD)

Melhor prática	Adere?
Os dados dos clientes da U.E. são mantidos privados/seguros.	Sim
Existe um plano para notificar os clientes da U.E. dentro de 72 horas se seus dados forem comprometidos/houver uma violação.	Sim
Garanta que os dados sejam classificados e inventariados adequadamente.	Não
Aplique políticas, procedimentos e processos de privacidade para documentar e manter dados adequadamente.	Sim

Recomendações (Resumidas)

Com base na auditoria, as seguintes recomendações são propostas para a Botium Toys para melhorar sua segurança:

Controles de Segurança

1. Menor Privilégio e Separação de Funções

Problema: Acesso excessivo a dados sensíveis e falta de separação de funções.
Recomendação: Implementar o princípio do menor privilégio e a separação de funções

para limitar o acesso aos dados e sistemas, minimizando riscos. Mapear funções, criar grupos de acesso e revisar permissões regularmente.

2. Planos de Recuperação de Desastres e Backups

Problema: Ausência de planos de recuperação de desastres e backups de dados críticos. **Recomendação:** Desenvolver um Plano de Recuperação de Desastres (DRP) e implementar uma estratégia de backup robusta, incluindo backups regulares, armazenamento off-site e testes de restauração. Isso garante a continuidade dos negócios e a recuperação de dados em caso de incidentes.

3. Sistema de Detecção de Intrusão (IDS)

Problema: Falta de um Sistema de Detecção de Intrusão (IDS). **Recomendação:** Instalar e configurar um IDS para monitorar o tráfego de rede, detectar atividades suspeitas e permitir uma resposta rápida a incidentes. Isso adiciona uma camada essencial de segurança e visibilidade.

4. Criptografia para Dados de Cartão de Crédito

Problema: Dados de cartão de crédito não são criptografados. **Recomendação:** Implementar criptografia forte para todos os dados de cartão de crédito em repouso e em trânsito, conforme exigido pelo PCI DSS. Isso protege a confidencialidade das informações sensíveis dos clientes.

5. Políticas de Senha e Gerenciamento Centralizado

Problema: Políticas de senha fracas e ausência de um sistema de gerenciamento de senhas centralizado. **Recomendação:** Fortalecer a política de senhas com requisitos de complexidade rigorosos e implementar um sistema de gerenciamento de senhas centralizado. Considerar a autenticação multifator (MFA) para contas críticas. Isso melhora a segurança das contas e a produtividade.

6. Ambiente Seguro para Dados de Cartão de Crédito (PCI DSS)

Problema: Ambiente de dados de cartão de crédito não é comprovadamente seguro. **Recomendação:** Garantir um ambiente seguro para dados de cartão de crédito através de segmentação de rede, controles de acesso físico, monitoramento contínuo, gerenciamento de vulnerabilidades e políticas documentadas. Isso é crucial para a conformidade com o PCI DSS.

7. Classificação e Inventário Adequado de Dados (RGPD)

Problema: Dados não são classificados nem inventariados adequadamente.
Recomendação: Criar um inventário completo e classificar todos os dados pessoais com base em sua sensibilidade e criticidade. Utilizar ferramentas de descoberta de dados e manter a documentação atualizada. Isso é fundamental para a conformidade com o RGPD e a gestão eficaz da privacidade dos dados.

Controles de Sistemas e Organizações (SOC tipo 1, SOC tipo 2)

Melhor prática	Adere?
Políticas de acesso do usuário são estabelecidas.	Não
Dados sensíveis (PII/SPII) são confidenciais/privados.	Não
A integridade dos dados garante que os dados sejam consistentes, completos, precisos e tenham sido validados.	Sim
Os dados estão disponíveis para indivíduos autorizados a acessá-los.	Sim