**Auditoria Interna de Segurança Cibernética da Botium Toys**

**1. Escopo e Metas**

**Escopo**

Abrange todo o programa de segurança da Botium Toys, incluindo:

* Todos os ativos físicos e digitais da empresa.
* Processos e procedimentos internos relacionados à implementação de controles e conformidade.

**Metas**

* Avaliar ativos existentes e completar a lista de verificação de controles e conformidade.
* Identificar os controles e práticas de conformidade necessários para melhorar a postura de segurança da empresa.

**2. Ativos Avaliados**

* Equipamentos no local (computadores, câmeras de vigilância, etc.).
* Equipamentos de funcionários (laptops, smartphones, estações remotas).
* Sistemas e serviços (e-commerce, banco de dados, gestão de inventário, telecomunicações).
* Infraestrutura de rede e internet.
* Sistemas legados que demandam manutenção manual.
* Produtos armazenados no depósito e na vitrine.

**3. Avaliação de Riscos**

**Pontuação de Risco**

**8/10** (Risco alto devido à falta de controles adequados e conformidade com padrões regulatórios).

**Problemas Identificados**

1. **Falta de controles:**
   * Privilégio mínimo.
   * Separação de funções.
   * Criptografia de dados sensíveis (e.g., dados de cartão de crédito).
   * Sistema de detecção de intrusões (IDS).
   * Planos de recuperação de desastres (DRP).
2. **Políticas de senha insuficientes:**
   * Requisitos de complexidade baixos.
   * Ausência de sistema de gestão centralizada de senhas.
3. **Sistemas legados:**
   * Monitoramento inconsistente e sem cronograma regular.
4. **Conformidade insuficiente com PCI DSS e GDPR:**
   * Acesso irrestrito a dados sensíveis.
   * Ausência de criptografia de dados financeiros e pessoais.

**4. Lista de Verificação de Controles e Conformidade**

**Controles**

| **Controle** | **Implementado?** | **Explicação** |
| --- | --- | --- |
| Privilégio Mínimo | Não | Todos os funcionários têm acesso a dados de clientes; é necessário restringir privilégios. |
| Planos de Recuperação de Desastres | Não | Não existem planos para continuidade de negócios em caso de incidentes. |
| Políticas de Senha | Não | Requisitos de senha são mínimos, permitindo vulnerabilidades a ataques de força bruta. |
| Separação de Funções | Não | CEO gerencia operações e folha de pagamento, aumentando o risco de fraude. |
| Firewall | Sim | Bloqueia tráfego baseado em regras de segurança definidas adequadamente. |
| Sistema de Detecção de Intrusões | Não | Necessário para identificar possíveis intrusões de atores mal-intencionados. |
| Backups | Não | Não há backups de dados críticos, comprometendo a continuidade do negócio em caso de falha. |
| Software Antivírus | Sim | Instalado e monitorado regularmente pelo departamento de TI. |
| Monitoramento de Sistemas Legados | Parcialmente | Monitoramento inconsistente e sem cronograma claro para manutenção. |
| Criptografia | Não | Não é utilizada atualmente; necessária para garantir a confidencialidade de informações sensíveis. |
| Sistema de Gestão de Senhas | Não | Ausente; sua implementação aumentaria a produtividade e segurança. |
| Fechaduras Físicas | Sim | A localização física da loja possui fechaduras suficientes. |
| Vigilância por CCTV | Sim | CCTV instalado e funcionando na localização física da loja. |
| Sistemas de Prevenção de Incêndios | Sim | Sistema funcional de detecção e prevenção de incêndios. |

**Conformidade**

**PCI DSS**

| **Prática Recomendada** | **Implementado?** | **Explicação** |
| --- | --- | --- |
| Apenas usuários autorizados têm acesso a dados de cartão de crédito. | Não | Todos os funcionários têm acesso aos dados internos. |
| Dados de cartão de crédito são processados em ambiente seguro. | Não | Não há criptografia ou restrição de acesso aos dados financeiros. |
| Implementar procedimentos de criptografia. | Não | Dados financeiros não são protegidos adequadamente. |
| Adotar políticas seguras de gestão de senhas. | Não | Políticas de senha fracas e falta de sistema centralizado. |

**GDPR**

| **Prática Recomendada** | **Implementado?** | **Explicação** |
| --- | --- | --- |
| Dados de clientes da UE são privados e seguros. | Não | Não há criptografia adequada para proteger informações financeiras e pessoais. |
| Plano para notificação em 72h em caso de violação. | Sim | Existe um plano para notificar clientes em caso de incidente de segurança. |
| Dados são classificados e inventariados. | Não | Dados foram inventariados, mas ainda não classificados. |
| Políticas de privacidade implementadas. | Sim | Políticas de privacidade foram desenvolvidas e aplicadas. |

**SOC (Tipos 1 e 2)**

| **Prática Recomendada** | **Implementado?** | **Explicação** |
| --- | --- | --- |
| Políticas de acesso de usuários | Não | Controle de privilégio mínimo e separação de funções não estão implementados. |
| Dados sensíveis são confidenciais/privados | Não | Ausência de criptografia para garantir confidencialidade. |
| Garantia de integridade de dados | Parcialmente | Integridade é mantida, mas não validada consistentemente. |
| Dados disponíveis apenas para autorizados | Não | Dados disponíveis para todos os funcionários, sem restrição baseada em função. |

**5. Recomendações**

Com base na análise realizada, recomenda-se:

1. **Implementar controles de privilégio mínimo**:
   * Restringir acesso apenas ao necessário para cada função.
2. **Desenvolver planos de recuperação de desastres (DRP)**:
   * Garantir backups regulares de dados críticos.
3. **Fortalecer políticas de senha**:
   * Exigir senhas mais complexas e implantar um sistema de gestão de senhas.
4. **Adotar criptografia de dados**:
   * Proteger informações financeiras e pessoais em trânsito e em repouso.
5. **Implementar um sistema de detecção de intrusões (IDS)**:
   * Monitorar e responder a tráfego anômalo na rede.
6. **Classificar ativos**:
   * Organizar os dados existentes para identificar e proteger os mais críticos.
7. **Estabelecer cronograma para manutenção de sistemas legados**:
   * Monitoramento consistente e intervenções programadas para minimizar riscos.

**Conclusão**

Esta auditoria destacou vulnerabilidades críticas na postura de segurança da Botium Toys. A implementação das recomendações listadas é essencial para reduzir riscos, melhorar a conformidade regulatória e proteger os ativos e dados da empresa.