Botium Toys: Escopo, objetivos e relatório de avaliação de riscos

Âmbito e objetivos da auditoria

Escopo: O escopo desta auditoria é definido como todo o programa de segurança da Botium Toys. Isso inclui seus ativos, como equipamentos e dispositivos dos funcionários, sua rede interna e seus sistemas. Você precisará revisar os ativos da Botium Toys e os controles e práticas de conformidade implementados.

Metas: Avalie os ativos existentes e preencha a lista de verificação de controles e conformidade para determinar quais controles e práticas recomendadas de conformidade precisam ser implementados para melhorar a postura de segurança da Botium Toys.

Ativos circulantes

Os ativos gerenciados pelo Departamento de TI incluem:

- Equipamentos no local para necessidades comerciais no escritório
- Equipamentos para funcionários: dispositivos de usuário final (desktops/laptops, smartphones), estações de trabalho remotas, fones de ouvido, cabos, teclados, mouses, estações de acoplamento, câmeras de vigilância, etc.
- Produtos de vitrine disponíveis para venda no varejo no local e online; armazenados no depósito adjacente da empresa
- Gestão de sistemas, software e serviços: contabilidade, telecomunicações, banco de dados, segurança, comércio eletrônico e gestão de estoque
- acesso à Internet
- Rede interna
- Retenção e armazenamento de dados
- Manutenção de sistemas legados: sistemas em fim de vida útil que exigem monitoramento humano

Avaliação de risco

Descrição do risco

Atualmente, a gestão de ativos é inadequada. Além disso, a Botium Toys não possui todos os controles adequados e pode não estar em total conformidade com as regulamentações e padrões dos EUA e internacionais.

Melhores práticas de controle

A primeira das cinco funções do NIST CSF é Identificar. A Botium Toys precisará dedicar recursos para identificar ativos para que possam gerenciá-los adequadamente. Além disso, precisará classificar os ativos existentes e determinar o impacto da perda de ativos existentes, incluindo sistemas, na continuidade dos negócios.

Pontuação de risco

Em uma escala de 1 a 10, a pontuação de risco é 8, o que é bastante alto. Isso se deve à falta de controles e de adesão às melhores práticas de conformidade.

Comentários adicionais

O impacto potencial da perda de um ativo é classificado como médio, pois o departamento de TI não sabe quais ativos estariam em risco. O risco de perda de ativos ou multas por parte de órgãos reguladores é alto, pois a Botium Toys não possui todos os controles necessários e não adere integralmente às melhores práticas relacionadas às normas de conformidade que mantêm dados críticos privados/seguros. Revise os seguintes pontos para obter detalhes específicos:

- Atualmente, todos os funcionários da Botium Toys têm acesso a dados armazenados internamente e podem acessar dados do titular do cartão e PII/SPII dos clientes.
- A criptografia não é usada atualmente para garantir a confidencialidade das informações de cartão de crédito dos clientes que são aceitas, processadas, transmitidas e armazenadas localmente no banco de dados interno da empresa.
- Controles de acesso referentes a privilégios mínimos e separação de funções não foram implementados.
- O departamento de TI garantiu disponibilidade e controles integrados para garantir a integridade dos dados.
- O departamento de TI tem um firewall que bloqueia o tráfego com base em um

conjunto apropriadamente definido de regras de segurança.

- O software antivírus é instalado e monitorado regularmente pelo departamento de TI.
- O departamento de TI não instalou um sistema de detecção de intrusão (IDS).
- Não há planos de recuperação de desastres em vigor atualmente, e a empresa não possui backups de dados críticos.
- O departamento de TI estabeleceu um plano para notificar os clientes da UE em até 72 horas em caso de violação de segurança. Além disso, políticas, procedimentos e processos de privacidade foram desenvolvidos e aplicados entre os membros do departamento de TI/outros funcionários, para documentar e manter os dados adequadamente.
- Embora exista uma política de senhas, seus requisitos são nominais e não estão de acordo com os requisitos atuais de complexidade mínima de senhas (por exemplo, pelo menos oito caracteres, uma combinação de letras e pelo menos um número; caracteres especiais).
- Não há um sistema centralizado de gerenciamento de senhas que imponha os requisitos mínimos da política de senhas, o que às vezes afeta a produtividade quando funcionários/fornecedores enviam um tíquete ao departamento de TI para recuperar ou redefinir uma senha.
- Embora os sistemas legados sejam monitorados e mantidos, não há um cronograma regular para essas tarefas e os métodos de intervenção não são claros.
- A localização física da loja, que inclui os escritórios principais da Botium Toys, a fachada da loja e o depósito de produtos, conta com fechaduras suficientes, sistema de vigilância por circuito fechado de televisão (CFTV) atualizado, além de sistemas de detecção e prevenção de incêndio em funcionamento.