Botium Toys: escopo, metas e relatório de avaliação de risco

Escopo 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 que a Botium Toys possui e os controles e práticas de conformidade que eles possuem.

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

Ativos correntes

Os ativos gerenciados pelo Departamento de TI incluem:

- Equipamento local para necessidades de negócios no escritório
- Equipamentos dos funcionários: dispositivos do 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; armazenado no armazém 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 que requerem monitoramento humano

Avaliação de risco

Descrição do risco

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

Controle as melhores práticas

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

Pontuação de risco

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

Comentários adicionais

O impacto potencial da perda de um ativo é classificado como médio, porque o departamento de TI não sabe quais ativos estariam em risco. O risco para ativos ou multas por parte dos órgãos governamentais é alto porque a Botium Toys não possui todos os controles necessários e não adere totalmente às melhores práticas relacionadas aos regulamentos 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 aos dados armazenados internamente e podem acessar os dados do titular do cartão e PII/SPII dos clientes.
- Atualmente, a criptografia não é usada 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.
- Os controles de acesso relativos ao privilégio mínimo e à 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 possui um firewall que bloqueia o tráfego com base em

um conjunto de regras de segurança adequadamente definido.

- 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 existem planos de recuperação de desastres atualmente em vigor e a empresa não possui backups de dados críticos.
- O departamento de TI estabeleceu um plano para notificar a E.U. clientes dentro de 72 horas se houver uma violação de segurança. Além disso, políticas, procedimentos e processos de privacidade foram desenvolvidos e são aplicados entre membros do departamento de TI/outros funcionários, para documentar e manter adequadamente os dados.
- Embora exista uma política de senha, seus requisitos são nominais e não estão alinhados com os atuais requisitos mínimos de complexidade de senha (por exemplo, pelo menos oito caracteres, uma combinação de letras e pelo menos um número; caracteres especiais).
- Não existe 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 ticket ao departamento de TI para recuperar ou redefinir uma senha.
- Embora os sistemas legados sejam monitorizados e mantidos, não existe um calendário regular para estas tarefas e os métodos de intervenção não são claros.
- A localização física da loja, que inclui sede, frente de loja e armazém de produtos da Botium Toys, possui fechaduras suficientes, vigilância atualizada em circuito fechado de televisão (CCTV), bem como sistemas de detecção e prevenção de incêndio em funcionamento.