Botium Toys: Relatorio de escopo, metas, e gerenciamento de risco.

Escopo e Metas da Auditoria

**Escopo:** O escopo é definido como o programa de segurança completo na Botium Toys. Isso significa que todos os ativos precisam ser avaliados juntamente com os processos internos e procedimentos relacionados à implementação de controles e melhores práticas de conformidade.

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

Ativos atuatis

Os ativos gerenciados pelo Departamento de TI incluem:

* Equipamentos locais para necessidades comerciais no escritório.
* Equipamentos de funcionários: dispositivos de usuário final (desktops/laptops, smartphones), estações de trabalho remotas, headsets, cabos, teclados, mouses, estações de ancoragem, câmeras de vigilância, etc.
* Produtos disponíveis para venda no varejo na loja física 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 inventário.
* Acesso a Internet
* Rede Interna
* Retenção de dados e armazenamento
* Manutenção de sistemas legados: sistemas fora de vida útil que exigem monitoramento humano.

Avaliação de riscos

Descrição do risco

Atualmente, há uma gestão inadequada de ativos. Além disso, a Botium Toys não possui todos os controles adequados em vigor e pode não estar totalmente em conformidade com as regulamentações e normas dos Estados Unidos e internacionais.

Boas práticas de Controles

A primeira das cinco funções do NIST CSF é Identificar. A Botium Toys precisará alocar recursos para identificar ativos, para que possa gerenciá-los adequadamente. Além disso, será necessário classificar os ativos existentes e determinar o impacto da perda desses ativos, 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 considerado bastante elevado. Isso se deve à falta de controles e aderência às melhores práticas de conformidade.

Comentários adicionaisAdditional comments

O impacto potencial decorrente da perda de um ativo é classificado como médio, pois o departamento de TI não sabe quais ativos estariam em risco. O risco para os ativos ou multas de órgãos reguladores é alto, pois a Botium Toys não possui todos os controles necessários e não está totalmente aderente às melhores práticas relacionadas às regulamentações de conformidade que mantêm os 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 ter acesso aos dados do titular do cartão e às informações pessoais/financeiras dos clientes.
* Atualmente, não é utilizado nenhum método de criptografia 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 ao princípio do menos privilégiado e separação de funções não foram implementados.
* O departamento de TI garantiu a disponibilidade e integrou controles para assegurar a integridade dos dados.
* O departamento de TI possui um firewall que bloqueia o tráfego com base em um conjunto apropriadamente definido de regras de segurança.
* Um software antivírus está instalado e é monitorado regularmente pelo departamento de TI..
* O departamento de TI não instalou um sistema de detecção de intrusões (IDS).
* Não existem planos de recuperação de desastres(DRP) atualmente em vigor, e a empresa não possui backups dos dados críticos.
* O departamento de TI estabeleceu um plano para notificar os clientes da União Europeia dentro de 72 horas em caso de violação de segurança. Além disso, políticas, procedimentos e processos de privacidade foram desenvolvidos e são aplicados entre os membros do departamento de TI e outros funcionários, para documentar e manter adequadamente os dados.
* Embora exista uma política de senhas, seus requisitos são mínimos e não estão alinhados com os requisitos atuais mínimos de complexidade de senha (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 aplique os requisitos mínimos da política de senhas, o que, por vezes, afeta a produtividade quando os funcionários/fornecedores precisam enviar um chamado ao departamento de TI para recuperar ou redefinir uma senha..
* Embora os sistemas legados sejam monitorados e mantidos, não há um cronograma regular estabelecido para essas tarefas, e os métodos de intervenção não estão claros.
* A localização física da loja, que inclui os principais escritórios da Botium Toys, a frente da loja e o depósito de produtos, possui fechaduras adequadas, sistema de vigilância por circuito fechado (CCTV) atualizado e em funcionamento, bem como sistemas de detecção e prevenção de incêndios.