Memorando de Axel

PARA: Gerente de TI, partes interessadas
DE: AXEL FRANKLIN
DATA: 01/07/2023
ASSUNTO: Constatações e recomendações da auditoria interna de TI

Caros colegas,

Revise as seguintes informações sobre o escopo, metas, descobertas críticas, resumo e recomendações da auditoria interna da Botium Toys.

Escopo:

- Permissões de usuário atuais definidas nos seguintes sistemas: contabilidade, detecção de ponto final, firewalls, sistema de detecção de intrusão, informações de segurança e ferramenta de gerenciamento de eventos (SIEM).
- Controles atualmente implementados nos seguintes sistemas: contabilidade, detecção de endpoints, firewalls, sistema de detecção de intrusão, ferramenta de gerenciamento de eventos e informações de segurança (SIEM).
- Procedimentos e protocolos atuais definidos para os seguintes sistemas: contabilidade, detecção de ponto final, firewall, sistema de detecção de intrusão, ferramenta de gerenciamento de eventos e informações de segurança (SIEM).
- Certificar-se de que as permissões, controles, procedimentos e protocolos atuais do usuário estejam alinhados com os requisitos de conformidade necessários.
- Certificar-se de que a tecnologia atual seja considerada. Acesso ao hardware e ao sistema.

Metas:

- Aderir ao Instituto Nacional de Padrões e Tecnologia de Segurança Cibernética Estrutura (NIST CSF)
- Estabelecer um processo melhor para seus sistemas para garantir que estejam em conformidade

- Fortalecer os controles do sistema
- Implemente o conceito de menos permissões quando se trata de credencial de usuário gerenciamento
- Estabelecer suas políticas e procedimentos, que incluem seus manuais
- Certificar-se de que eles atendem aos requisitos de conformidade

Achados Críticos (deve ser tratado imediatamente):

- Gestão inadequada de ativos
- Controles adequados não estão em vigor
- Pode não estar em conformidade com os regulamentos e diretrizes internacionais e dos EUA
- A pontuação de risco atual é 8/10 (alta), devido à falta de controles e adesão aos regulamentos e padrões de conformidade
- Não possui uma plataforma VPN
- Não possui proteção adequada para o banco de dados do usuário

Achados (devem ser abordadas, mas não há necessidade imediata):

- Não possui interface para celular, para ser acessado pelos funcionários da empresa

Sumário/Recomendações:

Após avaliar as possibilidades quanto à segurança da organização, identificou-se que algumas boas práticas precisam ser implementadas, a auditoria visa promover a mitigação dos riscos que estão sendo percebidos por vulnerabilidades listadas na documentação com controle de ativos, previamente anexada, classificada como “alto risco”, deve ser feita uma abordagem diretamente com os funcionários da empresa para verificar se há possibilidade de vazamento de credenciais de usuários com privilégios elevados, fazendo assim uma análise de controle patrimonial. A recomendação seria a implantação de um firewall que controle o tráfego de pacotes iminentes, e também a criação de uma intranet para que sejam acessados apenas pela equipe de administração, isso com sessões token que tenham entrada para usuários avançados com domínio de email terceirizados pela empresa, além de autenticação multifator e captchas de login para evitar vulnerabilidades da web até mesmo força bruta.