PUMA: Relatório de Escopo, Objetivos e Avaliação de Riscos

Escopo e objetivos da auditoria

Escopo: O escopo é definido como todo o programa de segurança da PUMA. Isso significa que todos os ativos precisam ser avaliados, juntamente com os processos e procedimentos internos relacionados à implementação de controles e melhores práticas de conformidade.

Objetivos: Avaliar os ativos existentes e completar a lista de verificação de controles e conformidade para determinar quais controles e melhores práticas de conformidade precisam ser implementados para melhorar a postura de segurança da PUMA.

Ativos atuais

Os ativos gerenciados pela equipe de TI incluem:

- Gestão de sistemas, software e serviços: provedor de armazenamento de imagens (minio), provedor de e-mail (mailjet), banco de dados, segurança e alocação de memória de servidor (gigacandanga)
- Rede interna
- Retenção e armazenamento de dados
- Logs PM2

Avaliação de risco

Descrição do risco: Atualmente, há uma gestão inadequada dos ativos. Além disso, a PUMA não possui todos os controles adequados em vigor e pode não estar totalmente em conformidade com a LGPD (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018) e regulamentos e padrões internacionais.

Melhores práticas de controle: A primeira das cinco funções do NIST CSF é Identificar. A PUMA precisará dedicar recursos para identificar os ativos para que possam gerenciá-los adequadamente. Além disso, será necessário 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 adesão às melhores práticas de conformidade.

Comentários adicionais

O impacto potencial da perda de um ativo é classificado como médio, porque a equipe de TI não sabe quais ativos estariam em risco. O risco para os ativos ou multas de órgãos reguladores é alto porque a PUMA não possui todos os controles necessários em vigor e não está aderindo completamente às melhores práticas relacionadas a regulamentos de conformidade que mantêm os dados críticos privados/seguros. Revise os seguintes pontos para detalhes específicos:

- Atualmente, nem todos os funcionários e desenvolvedores (apenas membros do DevOps e Tech Lead) têm acesso aos dados armazenados internamente e podem acessar PII/SPII de clientes. Isso é ótimo para garantir que vazamentos internos sejam evitados.
- Controles de acesso relacionados ao princípio do menor privilégio e à separação de funções não foram implementados.
- O servidor possui um firewall que bloqueia o tráfego com base em um conjunto de regras de segurança devidamente definidas.
- Nenhum software antivírus está instalado e sendo monitorado regularmente por um membro da equipe de TI.
- A equipe de desenvolvimento não instalou um sistema de detecção de intrusão (IDS).
- A equipe implementou o Swagger para rastrear as rotas da API existentes e seus usos.
- A equipe não implementa uma biblioteca de registro ou um sistema de gerenciamento de logs em nenhum de seus serviços e produtos web. O único registro implementado é o terminal PM2 na máquina de implantação, que poderia ser facilmente apagado por um invasor se ele conseguisse acessar o servidor.
- Atualmente, não existem planos de recuperação de desastres, e a empresa não possui backups dos dados críticos.
- Embora uma política de senha tenha sido debatida, nenhum padrão foi adotado, sendo a única regra implementada a exigência de um mínimo de 8 caracteres. Isso não leva em consideração a necessidade de exigir caracteres especiais, maiúsculas e minúsculas para criar uma senha forte.

Avaliação de Controles

Controles Administrativos			
Nome do Controle	**Tipo de Controle e Explicação**	**Precisa ser Implementado (X)**	**Prioridade**
Políticas de Senha	Preventivo; estabelecer regras de força de senha para melhorar a segurança/reduzir a probabilidade de comprometimento de contas por meio de técnicas de força bruta ou ataques de dicionário	X	Alta
Separação de Funções	Preventivo; reduzir o risco e o impacto geral de insiders maliciosos ou contas comprometidas	X	Média

Controles Tecnicos			
Nome do Controle	**Tipo de Controle e Explicação**	**Precisa ser Implementado (X)**	**Prioridade**
Sistema de Detecção de Intrusão (IDS)	Detectivo; permite que a equipe de TI identifique possíveis intrusões (ou seja, tráfego anômalo) rapidamente	X	Alta
Logging	Preventivo/Detectivo; pode reduzir o risco de certos eventos; pode ser usado após o evento para investigação	X	Muito Alta
Backup	Corretivo; pode restaurar/recuperar de um evento	X	Alta

Software Antivirus (AV)	Corretivo; vai detectar e colocar em quarentena ameaças conhecidas	X	Alta
Monitoramento, manutenção e intervenção manual	Preventivo; necessário para identificar e gerenciar ameaças, riscos ou vulnerabilidades em sistemas desatualizados	X	Média

Conformidade com a Lei

Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) do Brasil é uma lei abrangente de proteção de dados projetada para regular o tratamento de dados pessoais. Oficialmente conhecida como Lei Nº 13.709, foi sancionada em 14 de agosto de 2018 e entrou em vigor em 18 de setembro de 2020. A LGPD é influenciada pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e visa proporcionar aos indivíduos maior controle sobre seus dados pessoais, garantir transparência no tratamento de dados e estabelecer diretrizes claras para empresas e organizações que lidam com dados pessoais.

Componentes Chave da LGPD

- **Escopo e Aplicação**: A LGPD se aplica a qualquer tratamento de dados pessoais realizado por indivíduos ou entidades legais, públicas ou privadas, que operem no Brasil ou tratem dados coletados no Brasil. Abrange tanto atividades de tratamento de dados online quanto offline.
- **Dados Pessoais**: Dados pessoais, segundo a LGPD, incluem qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso abrange uma ampla gama de dados, desde nomes e números de identificação até dados de localização e identificadores online.

- **Princípios de Tratamento de Dados**: A LGPD estabelece vários princípios que devem ser seguidos ao tratar dados pessoais, incluindo:
    - **Limitação de Finalidade**: Os dados devem ser tratados para finalidades específicas, legítimas e claramente declaradas.
    - **Adequação**: O tratamento de dados deve ser compatível com as finalidades para as quais os dados foram coletados.
    - **Necessidade**: Apenas os dados mínimos necessários devem ser tratados para alcançar a finalidade pretendida.
    - **Transparência**: Os titulares dos dados devem receber informações claras, precisas e facilmente acessíveis sobre como seus dados estão sendo utilizados.
    - **Segurança**: Medidas técnicas e organizacionais apropriadas devem ser tomadas para proteger os dados contra acesso não autorizado, perda acidental, destruição ou dano.
- **Direitos dos Titulares dos Dados**: A LGPD concede aos indivíduos vários direitos em relação aos seus dados pessoais, incluindo:
    - **Acesso**: O direito de acessar seus dados pessoais.
    - **Correção**: O direito de solicitar a correção de dados incorretos ou incompletos.
    - **Eliminação**: O direito de solicitar a eliminação de dados que sejam desnecessários ou tratados em violação à lei.
    - **Portabilidade**: O direito de transferir seus dados para outro provedor de serviços.
    - **Informação**: O direito de ser informado sobre as atividades de tratamento de dados.
- **Base Legal para o Tratamento de Dados**: A LGPD especifica dez bases legais para o tratamento de dados pessoais, incluindo consentimento do titular dos dados, cumprimento de obrigações legais e interesses legítimos do controlador de dados.

- **Consentimento**: Quando o consentimento é a base para o tratamento de dados, ele deve ser livre, informado e explícito. Os titulares dos dados têm o direito de retirar seu consentimento a qualquer momento.
- **Encarregado de Proteção de Dados (DPO)**: As organizações são obrigadas a nomear um Encarregado de Proteção de Dados para supervisionar as estratégias de proteção de dados e garantir a conformidade com a LGPD.
- **Notificação de Violação de Dados**: A LGPD exige que as violações de dados sejam reportadas à Autoridade Nacional de Proteção de Dados (ANPD) e, em alguns casos, aos titulares dos dados afetados, de maneira oportuna.
- **Penalidades e Aplicação**: A não conformidade com a LGPD pode resultar em multas significativas, que podem chegar a 2% da receita de uma empresa no Brasil, limitadas a R$50 milhões por violação. A ANPD é responsável por aplicar a lei e tem a autoridade para emitir multas e outras sanções.