Conformidade com a LGPD

Problema

A crescente intensidade dos ataques cibernéticos e a falta de uma estratégia abrangente e atualizada de segurança cibernética, seja para órgãos públicos ou privados, com foco na proteção dos dados e sistemas críticos, aumenta a vulnerabilidade da infraestrutura tecnológica, tanto em ambiente computacional em nuvem quanto on-premises. Diante deste cenário, o volume, a constância e a sofisticação das ameaças cibernéticas exigem uma ferramenta que avalie e gere alertas de forma contínua, para proteção dos dados e manutenção da integridade dos sistemas. O robustecimento da infraestrutura contra as ameaças cibernéticas conhecidas, certamente, é um dos caminhos mais importantes para promover a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 2018.

Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

LGPD

Promulgada em 2018, com foco na proteção dos direitos fundamentais de liberdade, privacidade e desenvolvimento de personalidade de cada indivíduo. Aplica-se no tratamento de dados pessoais, em meios físicos ou digitais, por pessoas físicas ou jurídicas, de direito público ou privado.

Existe necessidade de adoção de medidas de segurança que garantam a proteção dos dados pessoais coletados e tratados, conforme descrito no artigo 46.

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."*

A ausência de ferramentas avançadas de detecção e resposta a incidentes cibernéticos, prejudica a capacidade de identificar e conter as ameaças de forma rápida e eficiente.

Solução

O emprego do Arkhe Athena oferece proteção ao perímetro de rede de dados e estabelece uma comunicação segura entre as diferentes localidades de acesso. Os dados e a reputação das instituições são protegidos e estão em conformidade regulatória, atendendo os requisitos da LGPD. As comunicações são protegidas, utilizam VLANs, permitindo, apenas, o tráfego autorizado entre as redes de dados. O mecanismo de detecção de vulnerabilidades possibilita que o administrador de redes identifique as vulnerabilidades nos sistemas operacionais e aplicativos instalados nos servidores que são monitorados. O Athena também é integrado aos bancos de dados CVEs dos fornecedores oficiais de aplicações, assim, as atualizações necessárias são implementadas de acordo com as informações disponibilizadas pelos próprios desenvolvedores das aplicações. Importante que o administrador poderá priorizar as tratativas em relação às vulnerabilidades, visto que estas são visualizadas através de interface simples e intuitiva. Os critérios de classificação das vulnerabilidades, Baixa/Média/Alta/Crítica, tornam-se essenciais para garantir o tratamento proativo de uma possível brecha de segurança e o respectivo vazamento de dados. Alertas são exibidos na interface de monitoramento e são compartilhados por email, desde que cadastrados.

Benefícios

O Arkhe Athena tem um emprego transversal, atende diversos segmentos, seja civil ou militar. Destacam-se entre os seus benefícios, as capacidades de integração e interoperabilidade com diferentes sistemas, escalabilidade e modularidade, visibilidade e monitoramento contínuo, melhoria da resiliência cibernética, monitoramento de infraestrutura, além do monitoramento e controle de vulnerabilidades. A flexibilidade de uso do Arkhe Athena, certamente, promove uma experiência diferenciada ao usuário no trato dos temas relacionados às questões cibernéticas. O administrador de redes tem todos os recursos e informações necessárias para o atendimento da LGPD.

Arkhe Athena, monitoramento de ocorrências cibernéticas.