Migalhas

APIs nas OSCs: Desafios Legais e Práticas Seguras

Beatriz de Oliveira Moraes

As OSCs buscam promover o bem-estar social e a participação democrática, adotando a tecnologia para expandir suas operações internas e externas, incluindo o uso de APIs para padronizar a comunicação entre diferentes softwares, melhorando a eficiência e o alcance de suas atividades.

sexta-feira, 17 de novembro de 2023
Atualizado às 14:29

As Organizações da Sociedade Civil (OSCs) desempenham um papel fundamental na sociedade com objetivos claros da promoção do bem-estar social, a justiça, o desenvolvimento sustentável e a participação democrática. Para alcançar esses objetivos, elas precisam ampliar o alcance de suas atividades para além do contexto físico e local e isso é possível por meio da implementação da tecnologia no seu dia a dia.

Ela pode ser usada para melhorar a eficiência das operações internas das OSCs, como a gestão de dados, o relacionamento com os beneficiários e a captação de recursos. Também pode ser usada para ampliar o alcance das atividades, por exemplo, por meio de plataformas de comunicação online, aplicativos móveis e ferramentas de mapeamento.

Nesse contexto tecnológico e de trânsito de dados, as APIs desempenham um papel importante. Elas consistem em conjuntos de rotinas e padrões que permitem que diferentes softwares se comuniquem entre si. Elas definem a maneira pela qual uma aplicação pode solicitar e compartilhar dados ou funcionalidades de outra aplicação de forma padronizada.

Em outras palavras, as APIs podem ser comparadas a uma ponte que conecta dois sistemas independentes, permitindo a troca de informações sem que os detalhes internos de cada sistema sejam revelados. Nesse caso, elas permitem que as OSCs desenvolvam e implementem novas funcionalidades ou integrações, sem a necessidade de reescrever todo o sistema.

As APIs são ferramentas versáteis e poderosas, com uma ampla gama de aplicações. No entanto, podem ser vulneráveis a ataques, o que as tornam um alvo atraente para os cibercriminosos. A Salt Security e a Akamai Technologies divulgaram relatórios que mostram um aumento recorde de ataques a APIs em 2022. De acordo com a Salt Security, houve um aumento de 400% de atacantes únicos direcionados a seus clientes nos seis meses anteriores. Já a Akamai Technologies aponta que houve um crescimento de 137% em relação a 2021.

Dessa forma, considerando o interesse crescente cibercriminosos e a ampla conexão viabilizada por essas interfaces, o perigo de expor dados, pessoais ou estratégicos é cada vez maior. Além disso, os danos de reputacionais para as OSCs e perda da confiança de beneficiários, doadores e financiadores podem impactar significativamente.

Assim, a segurança dos dados em trânsito é crucial com o aumento do uso de sistemas interconectados, especialmente em OSCs que lidam com dados pessoais de titulares em situações vulneráveis e dados sensíveis de projetos sociais. Nesse sentido, é fundamental ponderar os aspectos territoriais para avaliar a aplicação das leis nas operações que serão realizadas e garantir a conformidade adequada com as legislações relevantes, como o GDPR e a LGPD.

Entidades e organizações em todo o mundo, como a Digital Transformation Agency e o Standard Business Reporting da Austrália, a Technology Community do Governo da Inglaterra, o National Institute of Standards and Technology (NIST) e o W3C Working Group, se manifestaram sobre a estruturação da transformação digital, com ênfase na segurança do tráfego de dados pessoais para garantir a proteção das informações dos titulares.

Assim, no desenvolvimento de atividades com utilização de APIs, é essencial conduzir avaliações de impacto à proteção de dados (DPIA), identificando e minimizando riscos à privacidade sempre que houver alto risco para os direitos e liberdades das pessoas físicas.

Para garantir uma estrutura adequada para o tráfego de informações, é essencial avaliar riscos e implementar ferramentas de segurança. Isso inclui a análise das operações de tratamento de dados pessoais, identificando dados, titulares, agentes de tratamento, compartilhamentos, bases legais e outros fatores relevantes.

Além desses aspectos, as cláusulas contratuais devem definir os procedimentos de notificação em caso de violações ou incidentes e garantir a efetiva cooperação para conformidade com as regulações aplicáveis. Essas cláusulas devem definir limites para o tratamento de dados bem como do acesso e ou compartilhamento dos dados com terceiros.

Além das questões sobre os dados pessoais, a OSC pode ser comprometida quanto a realização de suas atividades e alcance de sua missão, prejudicando tanto beneficiários diretamente quanto a sua credibilidade.

Os custos financeiros decorrentes de incidentes de segurança podem ser altos, incluindo despesas com investigações, recuperação de dados, notificações e ações legais. Esses custos podem representar um ônus significativo para as OSCs, impactando a utilização dos recursos que poderiam ser empregados na realização de suas atividades.

Diante desses potenciais desafios, torna-se imperativo estabelecer uma base sólida de segurança e conformidade legal para mitigar de forma eficaz as possíveis questões decorrentes do uso e

estruturação das APIs. O primeiro passo é esboçar o fluxo dos dados para compreender todo trânsito, bem como possíveis interceptações e vulnerabilidades, identificando e documentando os requisitos de segurança existentes e os necessários.

A lista de 2023 da OWASP destaca os principais riscos de segurança das APIs. Com base nela, é possível identificar algumas práticas fundamentais para mitigar esses riscos. Essas práticas incluem a implementação de mecanismos de autenticação e autorização robustos, validação rigorosa dos dados em termos de tipos e extensão, emprego de criptografia para proteção das informações confidenciais em seu trânsito, monitoramento constante para identificar e corrigir vulnerabilidades e comportamentos anormais, e a familiaridade com as vulnerabilidades comuns que podem afetar as APIs, tomando as precauções apropriadas.

As OSCs que utilizam APIs deve considerar a presença de terceiros como parceiros, prestadores de serviços contratados ou financiadores e incluir além de cláusulas gerais sobre propriedade intelectual, conformidade regulatória, limitações de responsabilidade, mudanças e atualizações, ao estabelecer um contrato de API, é importante considerar outros aspectos específicos na SLA.

Isso traz definições sobre os níveis de serviço esperados, como tempo de resposta e tempo de atividade mínimo, bem como acordos sobre manutenção, suporte técnico, segurança da informação, integração com outros sistemas, documentação, testes de qualidade e garantia, além de especificar a frequência de atualizações e a disponibilidade de suporte contínuo para garantir o funcionamento seguro e eficaz da API ao longo do tempo.

O Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para APIs divulgado pelo Programa de Privacidade e Segurança da Informação é um ótimo documento para parametrizar a avaliação de segurança. Ele tem por finalidade apresentar orientações específicas para auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a especificar as questões de segurança e privacidade para APIs no âmbito institucional, ele é ótimo documento para ser utilizado como parâmetro de avaliação de segurança.

O Guia baseia-se no conceito do API Security Top 10, categorizando riscos em três níveis: explorabilidade, prevalência da vulnerabilidade, detecção da fraqueza e impacto técnico. A partir desse alicerce, o Guia oferece uma profunda compreensão de cada risco, expondo a abordagem dos atacantes e fornecendo insights sobre as medidas que podem ser implementadas para mitigar cada um desses riscos.

Para garantir a conformidade legal e a segurança adequada das APIs, a colaboração entre desenvolvedores, profissionais jurídicos e especialistas em segurança da informação é primordial. A equipe multidisciplinar pode ajudar a identificar os riscos envolvidos, implementar as medidas de segurança apropriadas e garantir que todos os aspectos técnicos, de segurança e legais sejam devidamente abordados. Isso demonstra um comprometimento claro com a segurança e a

privacidade dos dados, enquanto avança em direção a um ambiente digital mais confiável e protegido.

Beatriz de Oliveira Moraes

Advogada de Direito Digital e Proteção de Dados de Szazi, Bechara, Storto, Reicher e Figueirêdo Lopes Advogados, especialista em Direito Digital pelo Mackenzie e cursando MBA em Cybersecurity: Governance & Management na FIAP.