Trabalho - Pensamento de Segurança

João Vitor Maia Neves Cordeiro (19100532)

26 de março de 2023

Resumo

O objetivo desse relatório é utilizar um software desenvolvido pela empresa em que trabalho como material de análise para os items: ativos, adversários, gerenciamento de risco, contra medidas e custo benefício.

O sistema é uma aplicação de gerenciamento de eventos com público, que faz desde a venda online e presencial dos ingressos, passando por controle de capacidade, impressão de ingressos e finalmente validação e contabilização dos ingressos no momento do evento.

Nossos principais clientes são times de futebol, que vendem ingressos para jogos de diferentes tamanhos, já trabalhamos desde jogos da Série D do campeonato Brasileiro até jogos da seleção brasileira promovidos pela CBF.

Por ser uma aplicação com múltiplos módulos que rodam em plataformas diferentes, uma análise completa envolveria muito mais do que é possível fazer nesse trabalho, portanto focarei principalmente em ataques focados na parte da venda online e da validação de ingressos, que é onde tem as partes mais divertidas.

Ativos

Como principal ativo, por se tratar de uma plataforma online com cadastros de usuários, temos os dados pessoais de usuários, entre as informações confiadas estão endereço, documentos e contatos. Não armazenamos dados de pagamento.

Além dos ativos mais óbvios citados acima, temos que levar em consideração a proteção da integridade do evento que está sendo vendido, portanto

os códigos de ingressos precisam ser protegidos, caso contrário o evento ficará sujeito a ação de atacantes que visem comercializar em mercado paralelo ingressos legítimos para o evento.

Adversários

Por se tratar de um software que lida com um esporte de alta exposição midiática, não podemos deixar de incluir na lista de possíveis adversários as próprias torcidas. Nesse caso, não apenas as 2 torcidas dos times que envolvem a partida, mas também torcidas de rivais que poderiam se beneficiar com um escândalo público ou um evento desastroso do time rival. Para esse tipo de adversário, normalmente não se espera uma sofisticação muito alta de ataques, porém isso pode escalonar de acordo com o tamanho da torcida do time em questão e a importância da partida sendo vendida.

Além disso, existem quadrilhas de cambistas sem ligação direta com torcidas interessadas em conseguir códigos de ingressos ou mesmo descontos indevidos. Aqui estamos lidando com adversários mais organizados, que costumam fazer um investimento maior e são mais insistentes.

Não podemos esquecer também de adversários que estão apenas atrás dos dados pessoais de usuários, nesse caso podem ser grupos de criminosos especializados em vendas de pacotes de dados sensíveis, é comum que usem num geral ataques de baixa sofisticação e as vezes até ridículos, pois atacam de forma automatizada uma grande quantidade de sites e se contentam com aqueles que conseguirem.

Gerenciamento de Risco

Existem algumas barreiras prévias que podem ser colocadas apenas por regras de negócios bem pensadas. Como falamos na seção sobre os possíveis adversários, cambistas muitas vezes tentam obter descontos indevidos para aumentar suas margens de lucro. São descontos destinados a sócios do clube, ações beneficentes e outros. Nesse caso, podemos limitar a quantidade de ingressos que podem ser comprados por cada CPF, reduzindo o impacto, mas apenas isso não é suficiente.

Temos conhecimento prévio de que esses grupos de cambistas trabalham com uma quantidade grande de cadastros em nome de laranjas, por isso

também limitamos o número de compras por IP do cliente. Claro que essa é uma barreira relativamente simples de ser transposta, mas ela consegue manter boa parte dos grupos menos organizados sob controle.

Uma decisão tomada no início do projeto foi não armazenar dados de pagamento, portanto não temos certificação PCI, os dados de cartão são trafegados e armazenados exclusivamente pela adquirente, que fornece um SDK capaz de criptografar os dados no client e gerar um token de cartão que podemos utilizar para transacionar posteriormente. Esse token só é válido na nossa conta e para requisições partindo do nosso domínio.

Contra Medidas

Trabalhamos constantemente no combate a fraudes em conjunto com as adquirentes de cartão de crédito, utilizando perfis de compra dos usuários para identificar compras legítimas ou não. As adquirentes possuem contato direto com as bandeiras e bancos, portanto conseguem identificar traços de compras suspeitas em outros estabelecimentos no mesmo cartão.

Além disso, em jogos de grande porte, são realizadas análises humanas em cima das transações. Transações consideradas suspeitas recebem contato de nossa equipe de suporte, e caso não confirmem os dados, a transação é cancelada e o ingresso é bloqueado.

Por último, nossos ingressos tanto digitais quanto físicos possuem mecanismos de combate a fraude e os operadores de catraca são treinados para reconhecer esses itens. Ainda temos casos reportados de falsificações bem sucedidas, porém essas medidas tomadas de forma preventiva conseguiram reduzir boa parte dos problemas que existiam antes delas serem colocadas em prática.

Custo Benefício

Como dito em aula, a segurança é uma grande inimiga da usabilidade. Algumas medidas que aplicamos impactam diretamente na facilidade que nossos usuários tem de utilizar o sistema de forma legítima, e outras medidas que poderiam ser tomados possuem impacto tão alto que a decisão é simplesmente aceitar o risco de termos alguns ingressos forjados por jogo para não deteriorar o software tanto assim.

Uma dessas medidas não tomadas na maior parte dos eventos é a nominalidade instrasferível do ingresso, apesar do software permitir o uso desse tipo de regra, a maior parte dos clientes (produtores de eventos, não o cliente final) optam por não utilizar, alegando que as reclamações frequentes de compradores são mais importantes do que poucos ingressos falsificados por evento.

Além disso, temos medidas que custam dinheiro diretamente, como o uso de proteções antifraude das adquirentes de cartão de crédito, que nos cobram por transação analisada. Nesse caso, o risco de não utilizar essas soluções é maior do que o custo real delas, portanto optamos por deixar ligado para todos os clientes.