FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

Breno de Oliveira Veroneze

Vinicyus Ferrer Silveira

Aplicativos móveis em dispositivos Android: privacidade e segurança

Americana, SP
2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

Breno de Oliveira Veroneze

Vinicyus Ferrer Silveira

Aplicativos móveis em dispositivos Android: privacidade e segurança

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Análise e Gestão de Riscos de Segurança da Informação

Americana, SP.
2023

Breno de Oliveira Veroneze
Vinicyus Ferrer Silveira

Aplicativos móveis de pagamentos em dispositivos *Android*: Privacidade e Segurança

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Análise e Gestão de Riscos de Segurança da Informação.

Americana, 30 de novembro de 2023

Banca Examinadora:

Marcus Vinicius Lahr Giraldi
Especializado em MBA em Gestão de Segurança da Informação
Faculdade de Tecnologia de Americana

Maxwel Vitorino da Silva
Mestrado em Tecnologia
Faculdade de Tecnologia de Americana

Maria Elizete Luz Saes
Mestrado profissional em Tecnologia: Gestão Desenvolvimento e Formação
Faculdade de Tecnologia de Americana

APLICATIVOS MÓVEIS EM DISPOSITIVOS ANDROID: PRIVACIDADE E SEGURANÇA

MOBILE APPS ON ANDROID DEVICES: PRIVACY AND SECURITY

Breno de Oliveira Veroneze, Vinicyus Ferrer Silveira

Orientador: Marcus Vinicius Lahr Giraldi

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana)

Americana – SP – Brasil

breno.veroneze@fatec.sp.gov.br,
vinicyus.silveira@fatec.sp.gov.br,
Orientador: marcus.lahr@fatec.sp.gov.br

RESUMO

Este artigo visa apresentar uma análise sobre a segurança de aplicativos de pagamentos em *smartphones*, o cenário atual de segurança em aplicações móveis de pagamentos dos sistemas Android, para o desenvolvimento da pesquisa foram utilizados artigos científicos, pesquisa de campo para entender o comportamento dos usuários que utilizam *smartphones*, testes automatizados em aplicativos de pagamentos e uma entrevista com um profissional da área da segurança da informação. Os resultados esperados sobre o grau de segurança dos aplicativos de pagamentos em sistemas Android, apresentar como o público geral utiliza sistemas de pagamentos em smartphones e sua preocupação com a segurança de seus dados. Espera-se, ainda, que os resultados alcançados permitam uma melhor compreensão de como as empresas podem garantir a segurança dos dados coletados de terceiros em aplicativos.

Palavras-chave: android, dados, segurança, pagamentos.

ABSTRACT

This article aims to present an analysis of the security of payment applications on smartphones, the current security scenario in mobile payment applications on Android systems. Scientific articles, field research to understand the behavior of users who use smartphones, automated tests on payment applications and an interview with a professional in the field of information security were used to develop the research. The expected results on the degree of security of payment applications on Android systems, show how the general public uses payment systems on smartphones and their concern about the security of their data. It is also hoped that the results achieved will provide a better understanding of how companies can guarantee the security of data collected from third parties in applications.

Keywords*: android, data, security, payments.*

1 INTRODUÇÃO

Com o avanço tecnológico de celulares, as aplicações móveis vêm ganhando cada vez mais espaço no cotidiano das pessoas. Isso acontece, desde jogos para entretenimento e lazer, até mesmo sendo possível a realização de pagamentos e transferências bancárias instantaneamente. Devido a essa realidade, os aplicativos vêm solicitando e tendo cada vez mais acessos a dados sensíveis dos usuários.

Outro aspecto que requer atenção é a popularização dos meios de pagamento via aplicativos em *smartphones*, cotidianamente as pessoas utilizam o dispositivo para realização de compras, transferências e pagamento, muito por conta da praticidade e agilidade desses serviços.

O problema condutor da pesquisa está na pergunta: qual cenário atual da segurança em aplicativos de pagamentos no sistema Android? Também, interessa saber qual a visão de um profissional da área de segurança da informação sobre o tema. Também, é preciso ressaltar sobre o quanto as pessoas têm ciência dos dados que são coletados quando eles efetuam transações em seus *smartphones*.

Então, o objetivo desta pesquisa é apresentar o parâmetro da concessão e segurança dos dados coletados pelos *softwares* móveis de pagamentos, como bancos, lojas virtuais entre outros, do principal sistema móvel da atualidade, sendo ele o Android. A partir disso, é possível entender se os aplicativos de pagamentos atualmente são seguros no sistema Android, quais instrumentos são utilizados para garantir essa segurança e expor como o público geral entende o cenário atual de segurança em *smartphones*.

A justificativa de importância deste artigo é expor o grau de segurança que os dados coletados em aplicações que utilizam meios de pagamentos em *smartphones*, além disto entender o impacto das normas de segurança implementadas e a conformidade dessas aplicações em relações a elas. Isso, para conscientizar sobre o quão crítico deve ser tratado o assunto de segurança quando envolvem dados relacionados a transações financeiras.

O tema de pesquisa deste trabalho foi suportado pelas áreas de conhecimento: Governança de Segurança da Informação e Políticas de Segurança da Informação.

2 REFERENCIAL TEÓRICO

Os principais referenciais teóricos deste presente artigo científico estão inseridos em pesquisas e artigos que expõem e realizam análises relacionadas ao tema de segurança e privacidade em aplicativos de sistema móveis.

A utilização de *smartphones* se faz cada vez mais presente no cotidiano das pessoas. Segundo o levantamento anual divulgado pela Fundação Getúlio Vargas (FGV) em junho de 2022, o Brasil possui mais um *smartphone* por habitante, contabilizando assim 242 milhões de aparelhos em uso (CNN BRASIL, 2022).

Outro ponto que é necessário levar em consideração é o grande aumento de transações em aplicativos de celulares, como citado no artigo *Security Analysis of Mobile Money Applications on Android*, essa categoria de aplicativo está prosperando devido as facilidades e conveniência que trazem às pessoas (DARVISH; HUSAIN, 2018), no entanto os mesmos deixam claro que o maior desafio desse nicho é a relação de confiança, devido ao grau crítico de sigilo das informações utilizadas em pagamentos, transferências e transações financeiras (DARVISH; HUSAIN, 2018).

Com o avanço da tecnologia e a globalização, como citado no artigo *Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World*, atualmente a maior parte do comercio moderno no mundo dependente de transações sem dinheiro em sistemas de pagamento, devido ao fato da transferência ser realizada de maneira instantânea e mesmo com todos os riscos envolvidos, ainda é uma maneira mais segura que se deslocar por grandes distâncias levando grandes quantidades de dinheiro (REAVES et al., 2015)

Em toda aplicação existem ameaças, sendo impossível qualquer sistema estar completamente livre da possibilidade de um ataque, no entanto, é de suma importância que desenvolvedores, equipes de segurança e empresas sempre estejam buscando ferramentas que visam mitigar as vulnerabilidades para mapear e neutralizar possíveis ameaças. Neste cenário que buscamos entender quais meios essas empresas utilizam para garantir que os dados coletados em seus aplicativos sejam tratados e armazenados em segurança.

3 METODOLOGIA

A metodologia, a ser adotada, em linhas gerais: utilização de abordagem descritiva, quantitativa e qualitativa.

Na primeira etapa foi realizada uma pesquisa bibliográfica utilizando artigos científicos e livros sobre o tema: Privacidade e segurança em aplicações móveis em sistemas Android, sendo que os principais autores utilizados como referencial teórico: Darvish, Husain e Reaves e colaboradores.

Após isso, foi realizada uma entrevista com um profissional da área de cibersegurança. O objetivo desta entrevista é entender como os dados sensíveis dos usuários são tratados pela empresa e quais métodos são utilizados para garantir a segurança e confidencialidade deles.

Na próxima etapa foi realizada um teste automatizado em aplicativos muito utilizados no Brasil, para identificar se existem ou não vulnerabilidades, dentre as escolhidas para checagem.

Em seguida, os dados coletados foram analisados e os resultados descritos no tópico de resultados e discussões, com principal objetivo de demonstrar o grau de criticidade com que o público e as empresas tratam a segurança em aplicativos de pagamentos no sistema Android e se houve uma melhora nesse cenário.

4 RESULTADOS E DISCUSSÕES

4.1 Momento atual

Atualmente os *smartphones* tornaram-se itens essenciais para grande parte das pessoas, sendo utilizados em inúmeros contextos de comunicação, estudo, trabalho, compras etc. Segundo levantamento realizado pelo Instituto Brasileiro de Geografia e Estatística (IBGE) e publicado pela *Cable News Network* - CNN Brasil, “São 242 milhões de celulares inteligentes em uso no país, que tem pouco mais de 214 milhões de habitantes” (CNN BRASIL, 2022, on-line). Uma das principais facilidades que os aplicativos em celulares proporcionam é a possibilidade de ter aplicativos de bancos onde diversos processos que a alguns anos atrás seria necessário um deslocamento até uma agência bancária, hoje podem ser executados de qualquer local tendo um celular e uma conexão com internet, isso por meio de diversos aplicativos de instituições bancárias.

Ainda sobre a utilização de aplicativos bancários, o crescimento desse tipo de aplicação proporcionou a criação de diversos bancos nomeados como *Fintech*, diferente dos bancos tradicionais, as Fintechs criaram o modelo de um banco ontem todas as atividades são executadas online, não possuindo agências bancárias. Segundo uma pesquisa realizada em 2021 pelo *Boston Consulting Group* (BCG) e publicado pelo site Exame o mercado das Fintechs

cresceram 155% em relação ao ano anterior (BODETTI, 2022). Esse modelo de banco tornou uma opção atrativa para diversas pessoas, porém pela dinâmica de ser uma instituição financeira totalmente digital e em que na maioria dos processos é realizada apenas via aplicativos mostra que existe uma quantidade significativa de dados sendo coletados por essas intuições, ainda existe a preocupação na invasão de contas bancárias e diversos bancos como já desenvolvem ferramentas em busca a trazer maior segurança para seus usuários, como por exemplo o banco Nubank que trouxe o Modo Rua, essa funcionalidade atua como uma "trava", o usuário escolhe uma rede *wi-fi* de sua confiança, normalmente a utilizada em sua casa e, ao sair na rua, o aplicativo da Nubank vai automaticamente limitar as transações de transferência e pagamentos de boleto, isso conforme a configuração do usuário. Esse tipo de sistema de segurança auxilia em casos em que o usuário pode ter o celular roubado e invadido, ou ainda sua conta de banco invadida por meio de outro dispositivo.

Uma prática que tem sido utilizada para invasão de aplicativos por golpistas, tem sido a solicitação de mudança da titularidade da linha telefônica para a operadora pelos golpistas, por meio disso o invasor assume o controle do número e com o acesso ao SMS os fraudadores realizam acessos a aplicativos de bancos, WhatsApp, dentre outros. Em casos como esse o sistema de segurança citado anteriormente, iria ser efetivo, uma vez que o invasor precisaria ter acesso a rede *wi-fi* para realizar a alteração das preferências no aplicativo.

A pandemia de COVID-19 também influenciou diretamente em um nicho de aplicativos móveis, o isolamento ocasionou um aumento exponencial nos pedidos de comida via *delivery*, com isso aplicativos como iFood, Rappi, Uber Eats, dentre outros. Tiveram um crescimento significativo no volume de transações, um levantamento realizado pela data.ai e publicado pelo site iFood News, aponta que comparando o primeiro trimestre de 2022 com o mesmo período no ano anterior, houve um aumento de 65% na utilização de aplicativos de delivery no mundo todo, quando olhamos para as estatísticas apenas do Brasil esse percentual aumenta para 380% (IFOOD NEWS, 2022).

4.2 Escolha de sistema operacional

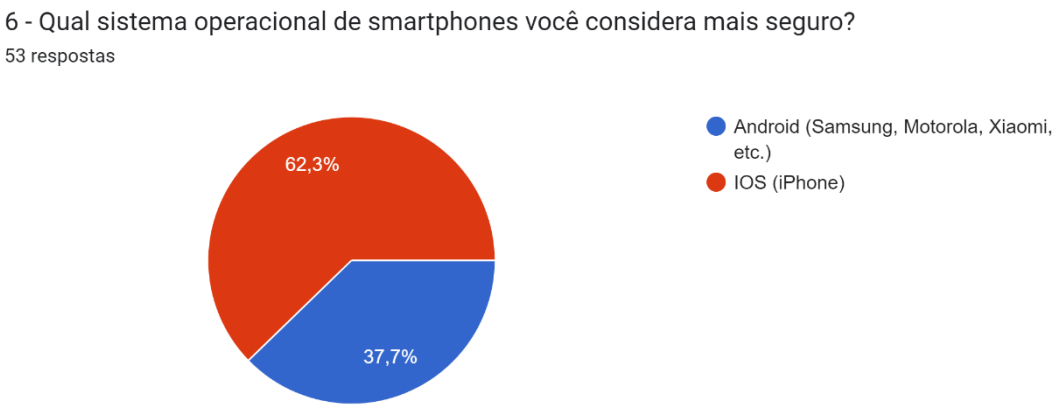
De acordo com estatísticas de uma pesquisa publicada no site IstoéDinheiro em julho de 2023, 81% dos usuários utilizam sistema operacional Android em seus celulares (PAVAN, 2023), sendo assim, o ecossistema por onde grande parte das transações é realizado. O sistema Android traz como característica um sistema operacional (SO) de código aberto, que possuí

liberdade de modificações, tanto que normalmente cada fabricante de celular tem sua versão customizada do SO, que pode assim ter suas vulnerabilidades especificas de versão para versão, aumentando assim as possibilidades de haver fragilidades a serem exploradas por pessoas mal-intencionadas. Já o IOS é praticamente o oposto de seu concorrente, trazendo um SO que é o mesmo para todos os seus *smartphones*, os *iPhones*, tendo como sua principal característica ser um sistema completamente fechado, por mais que esse aspecto limite o usuário nas possibilidades de alterações e funcionalidades com seu celular, o IOS torna-se um sistema com menos vulnerabilidades que o Android, por mais que elas ainda existam.

Um levantamento realizado pela empresa de cibersegurança Zimperium, em 2023, e publicado pelo site Cisoadvisor, constatou que houve um aumento de 138% de vulnerabilidades críticas encontradas em dispositivos Android em relação ao ano de 2021 (CISOADVISOR, 2023).

De maneira geral, os consumidores também têm a mesma sensação de que dispositivos IOS são mais seguros, para comprovar isto foi realizada uma pesquisa de autoria própria, em setembro de 2023, via ferramenta Formulários do Google, com participação de cinquenta e três usuários, foi possível observar que a grande maioria das pessoas acreditam que os dispositivos da Apple são mais seguros.

Gráfico 1: Segurança de sistemas móveis



Fonte: Autoria própria.

Como é possível observar no gráfico 1, 62,3% das pessoas que responderam à pesquisa acreditam que o SO IOS é mais seguro para utilização, o que é um dado interessante visto que, como observado anteriormente, grande parte dos usuários utilizam sistema Android, esse cenário ocorre por conta do difícil acesso a dispositivos da Apple, sendo um dos fatores sua elevada faixa de preço.

4.3 Dados coletados por aplicativos

Pode variar os dados coletados de aplicativo para outros, mas o padrão coletado vai de dados como: Nome, CPF, RG, e-mail, telefone, cartões e relacionamento bancário. E com essas informações e comportamento do usuário dentro do app de vai alimentar ainda mais com dados importantes, pois com esses dados é possível traçar o gosto e sugerir novos produtos e até mesmo aquilo que a pessoa já tem em mente comparar.

Além disso, são coletados a localização, e é usada para saber os locais mais frequentados pelos usuários, e assim traçar o seu comportamento, e com isso saber quando pode estar acontecendo uma transação fraudulenta, e assim já bloqueando na hora.

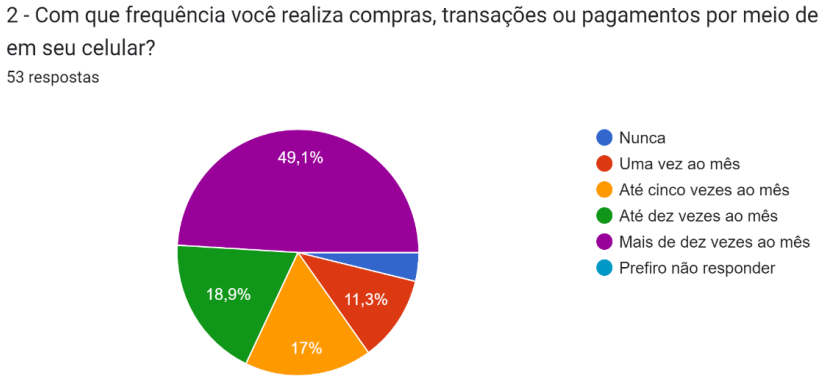
Tais dados são considerados dados pessoais sob a LGPD e a GDPR, portanto, sujeitos às regulamentações de proteção de dados. Ambas as regulamentações exigem que os usuários forneçam consentimento informado e inequívoco para a coleta e o processamento de seus dados pessoais. É importante que os usuários sejam devidamente informados sobre como seus dados serão usados e tenham a opção de consentir ou recusar.

A LGPD e a GDPR têm o objetivo de proteger a privacidade e os direitos dos indivíduos em relação aos seus dados pessoais. Para cumprir essas regulamentações, é importante que as empresas que coletam e processam dados pessoais adotem práticas adequadas de privacidade e segurança, forneçam transparência aos usuários e obtenham seu consentimento quando necessário. Além disso, é fundamental estar ciente das nuances e especificidades de cada regulamentação, uma vez que pode haver diferenças entre elas.

4.4 Ponto de vista dos usuários

Independente do ocorrido, o nicho mais afetado por qualquer tipo de invasão ou vazamento de dados é o titular dele, pensando nisso, foi realizada uma pesquisa de autoria própria, em setembro de 2023, com cinquenta e três usuários, onde no gráfico 2 é possível observar a grande frequência em que compras são realizadas em aplicativos móveis.

Gráfico 2: Frequência de compra mensal via aplicativos

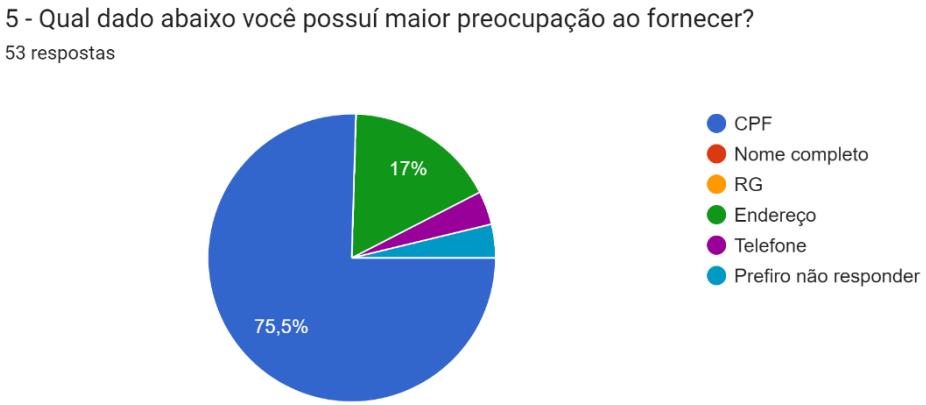


Fonte: Autoria própria.

Conforme é possível observar no gráfico 2, 49.1% dos usuários realizam mais de dez compras no mês, isso considerando pedidos de *delivery* de comida, compras de produtos etc. Esses dados confirmam o cenário que foi informado anteriormente, principalmente após a pandemia de COVID-19, houve um grande aumento no volume de compras que as pessoas realizam por meios digitais, muito pelo fato do período de quarentena e mesmo após o término do isolamento social existem diversas pessoas que não se sentem mais confortáveis em frequentar grandes centros de lojas onde ocorrem aglomerações, sendo o meio digital uma alternativa segura e confortável para receber seu produto diretamente na sua casa.

Outro aspecto abordado na pesquisa foi qual o dado que os usuários tinham mais preocupação em ceder, onde no gráfico 3 é possível observar que grande parte das pessoas tem como sua maior preocupação compartilhar o CPF com terceiros.

Gráfico 3: Dados mais preocupantes fornecidos



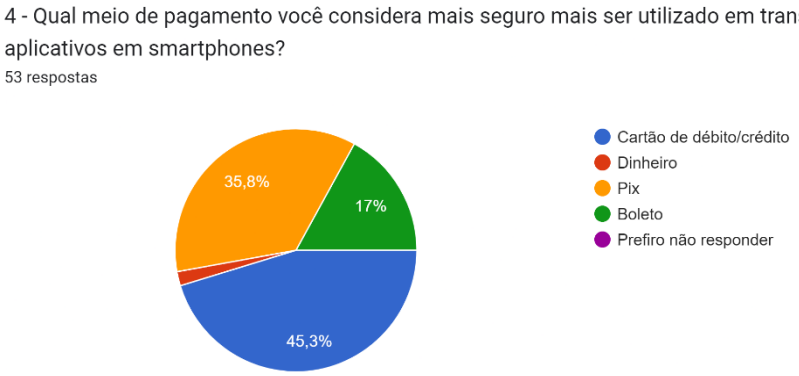
Fonte: Autoria própria.

A compreensão da necessidade do uso indevido do CPF é justificável, vez que ele pode ser utilizado para abertura de contas sem autorização, contratação de empréstimos e golpes, já

que diversos serviços utilizam o CPF como uma maneira de validar se realmente é o titular do serviço que está fazendo aquela solicitação.

Por fim o último ponto que a pesquisa abordou foi entender quais são os meios de pagamentos que os usuários consideram mais seguros para utilizar em aplicativos, os resultados estão expostos no gráfico 4.

Gráfico 4: Meio de pagamento mais seguro



Fonte: Autoria própria.

O meio de pagamento de cartões de débito/crédito continua sendo considerado a maneira mais segura de realizar pagamentos em aplicativos com 45,3%, no entanto o pix vem logo em seguido com 35,8% o que é surpreendente, uma vez que esse meio de pagamento começou a ser utilizado em fevereiro de 2020, sendo o mais contemporâneo entre as alternativas.

Criado pelo Banco Central em 2020, o pix é um sistema de pagamento instantâneo onde os recursos podem ser transferidos entre contas em poucos segundos em qualquer hora do dia durante todos os dias da semana. Além da sua velocidade de transação, diferente de outros meios de transferências como TED e DOC, o pix não possui nenhum tipo de taxa de transferência. Por esses motivos, como é possível observar na pesquisa realizada, o meio de pagamento passou a ser popular entre os brasileiros, sendo utilizadas tanto para transferência entre pessoas físicas, quanto como meio de pagamentos em compras.

Segundo artigo público pelo Banco Central do Brasil, a segurança do pix está baseada em quatro dimensões, sendo elas:

A autenticação do usuário: toda transação pix ou gerenciamento de chaves, só pode ser realizada em um ambiente seguro, esse por sua vez deve ter ferramentas de controles de acesso como reconhecimento facial, biométrico ou uso de token.

Rastreabilidade das transações: todas as transações realizadas via pix são totalmente rastreáveis, sendo possíveis a identificação das contas que participaram da transferência, por

meio desses dados é possível a identificação de fraudes, crimes e golpes.

Tráfego seguro de informações: a transferência de dados é feita de forma criptografada na Rede do Sistema Financeiro Nacional (RSFN), que é uma rede separada da internet dedicada para transação do Sistema de Pagamentos Brasileiro (SPB). Todos os participantes do pix precisam de certificados para acessarem essa rede para realizarem transações, por fim todas as informações das transações e dados pessoais vinculados às chaves são armazenados em segurança com a utilização de criptografia em sistemas internos do Banco Central do Brasil (BANCO CENTRAL DO BRASIL, 2023).

4.5 Teste automatizado de segurança em aplicativos

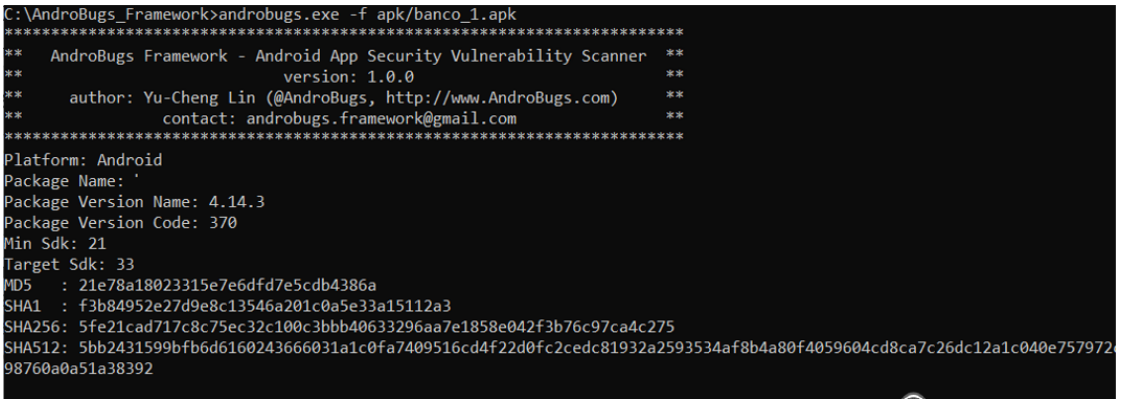
Para entender melhor qual parâmetro de segurança adotado por diversos aplicativos utilizados nacionalmente por centenas de pessoas, foi realizado um processo de análise de vulnerabilidade dos aplicativos utilizando um framework chamado *AndroBugs*, os testes realizados nessa etapa são baseados em dois artigos, sendo eles Darvish e Husain, 2018 e Reaves et al., 2017*,* os quais utilizaram a mesma ferramenta para realização de testes automatizados, neste presente artigo adaptamos parte da metodologia utilizada, na qual foi aplicada em aplicativos de pagamentos no Brasil. A escolha da ferramenta *AndroBugs*, apesar de não tem 100% de precisão nas suas análises, vem por conta da sua acessibilidade, sendo possível executá-la no Windows tendo apenas uma versão de Python instalada como base, no entanto segundo o artigo *Security Analysis of Mobile Money Applications on Android*, que executou o teste com a mesma ferramenta e validou o utilizando engenharia reversa, identificou que o *AndroBugs* possui uma precisão de aproximadamente 70% em suas análises, o que é razoavelmente bom, para uma ferramenta que executa um teste automatizado e rápido.

Para iniciar o processo de análise foi acessado o repositório da ferramenta *AndroBugs* e realizado *download* do framework, após isso instalado a versão 3.10.4 do Python, que necessário para execução dos testes. O *AndroBugs* realiza a análise dos aplicativos a partir do arquivo *Android Package Kit* (APK), para conseguir isso foi utilizado o aplicativo APK *Extractor*, que pode ser encontrado na Play Store, para extrair o arquivo APK dos aplicativos a partir de um dispositivo móvel Android e transferir esses arquivos para o computador onde será feita execução dos testes via cabo de transferência de dados.

Para executar a análise no *AndroBugs* primeiro é necessário adicionar uma nova variável de ambiente no Windows como "*AndroBugs_Framework*", após isso realizar a abertura do

terminal de comando na pasta da ferramenta e executar o comando python androbugs.py -f [Arquivo APK], substituindo o "[Arquivo APK]" pelo nome do APK extraído no celular e transferido para o computador. A figura 1 mostra a saída exibida no terminal do *Windows* após a execução do comando.

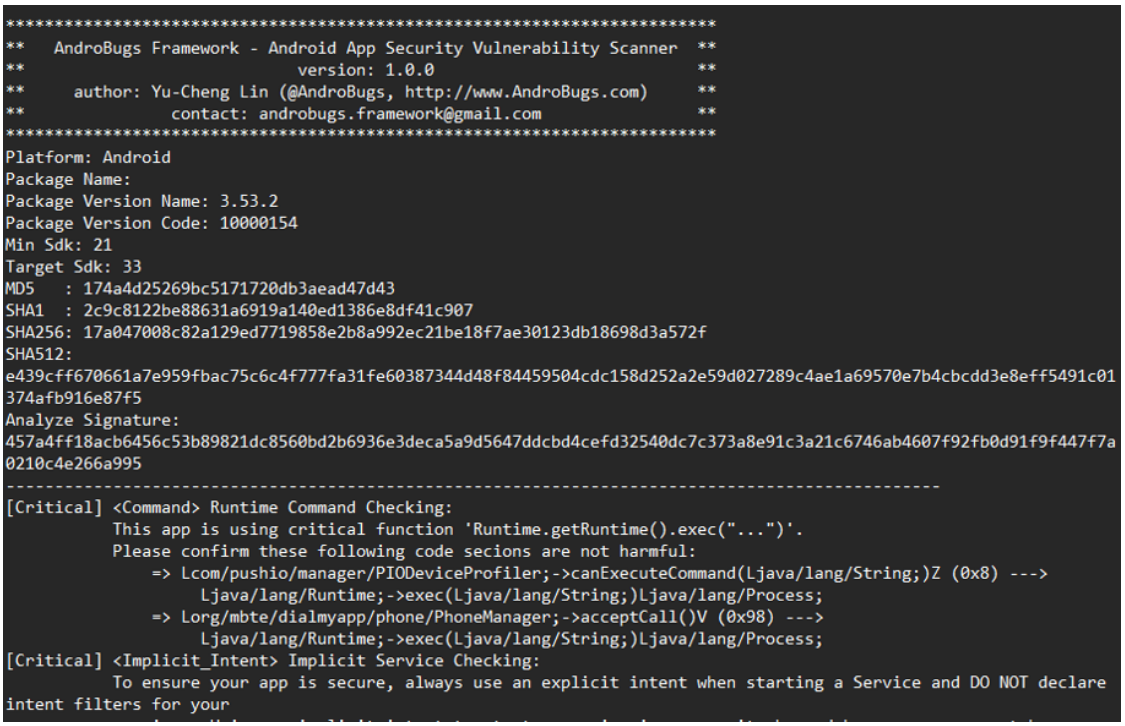
Figura 1 – Execução do teste automatizado



Fonte: Autoria própria.

Após execução desse comando será iniciado o processo de análise de vulnerabilidade automatizado do aplicativo, que após finalização irá gerar um relatório em arquivo texto com os resultados. A figura 2 mostra a saída do relatório em arquivo texto com os resultados do teste.

Figura 2 – Relatório do teste automatizado



Fonte: Autoria própria.

Para execução dos testes foram escolhidos dezesseis aplicativos que são amplamente utilizados no Brasil nas áreas de *delivery*, bancos, carteiras digitais e *marketplaces*, após a execução dos testes foram encontrados os seguintes resultados, onde o termo "NÃO" significa que não foi localizada aquela vulnerabilidade na aplicação e o termo "SIM" significa que no teste automatizado foi localizado aquela vulnerabilidade no aplicativo. Após a análise dos dados os nomes dos aplicativos foram anonimizados para exposição no artigo.

Dentro deste relatório possuem diversas informações sobre o aplicativo, no entanto para fins de análise neste artigo, foram escolhidas as seguintes vulnerabilidades:

Verificação de certificado SSL (VCSSL): Significa que o aplicativo não realiza a validação de certificados SSL, ou seja, permitindo assim comunicação com certificados auto assinados, o que pode ser uma brecha para ataque de *man in the middle*, onde dados são interceptados e coletados por um terceiro de maneira ilegal e para fins criminosos.

Implementação SSL (ISSL): Significa que o aplicativo permite que o verificador de nomes de host aceite todos os nomes comuns, o que implica que um invasor com certificado SSL válido poderá realizar um ataque de *man in the middle*.

Serviço implícito (SI): Significa que o usuário não pode identificar qual serviço dentro do aplicativo foi iniciado, usando assim um motivo implícito para iniciar uma tarefa.

Execução de comando *runtime* (ECR): Significa que é possível um usuário executar uma entrada no aplicativo a partir de um terminal de comando.

Permissão *Android manifest* (PAM): Significa que o aplicativo pode utilizar a permissão "*Mount_Unmount_FileSystems*", esse privilégio permite montar e desmontar sistemas de arquivos em armazenamentos removíveis, o que não é indicado que seja realizado por aplicativos.

Os resultados encontrados a partir da análise minuciosa dos dados obtidos a partir do teste automatizado estão expostos no quadro 1.

Quadro 1: Resultado do teste automatizado

NOME	**VCSSL**	**ISSL**	**SI**	**ECR**	**PAM**
BANCO DIGITAL 1	NÃO	NÃO	SIM	SIM	NÃO
BANCO DIGITAL 2	NÃO	NÃO	NÃO	NÃO	NÃO
BANCO DIGITAL 3	NÃO	NÃO	NÃO	NÃO	NÃO
BANCO DIGITAL 4	NÃO	NÃO	NÃO	NÃO	NÃO
BANCO DIGITAL 5	SIM	NÃO	NÃO	NÃO	NÃO
BANCO DIGITAL 6	NÃO	NÃO	NÃO	SIM	NÃO
CARTEIRA DIGITAL	NÃO	NÃO	NÃO	NÃO	NÃO
DELIVERY 1	NÃO	NÃO	NÃO	NÃO	NÃO
DELIVERY 2	NÃO	NÃO	SIM	NÃO	NÃO
DELIVERY 3	NÃO	SIM	NÃO	NÃO	NÃO
MARKETPLACE 1	SIM	NÃO	SIM	SIM	NÃO
MARKETPLACE 2	NÃO	NÃO	NÃO	NÃO	NÃO
MARKETPLACE 3	NÃO	NÃO	NÃO	NÃO	NÃO
MARKETPLACE 4	NÃO	NÃO	NÃO	NÃO	NÃO
MARKETPLACE 5	SIM	NÃO	SIM	NÃO	NÃO
TRANSPORTE	NÃO	NÃO	NÃO	NÃO	NÃO

Fonte: Autoria própria.

A partir dos resultados obtidos é possível observar que grande parte das vulnerabilidades não são encontradas nos aplicativos, o que significa que as empresas responsáveis por esses sistemas preocupam-se em manter suas aplicações seguras, outro aspecto que colabora com isso são os requisitos para submissão de aplicativos na *Play Store*, que realiza diversas verificações de vulnerabilidade e em casos de falhas que possam ocasionar em problemas críticos a submissão do aplicativo é rejeitada, ou seja, para um aplicativo estar disponível na loja para *download* ele já possou por diversos testes de segurança, que pelo menos em teoria, asseguram que ele não é nocivo para o usuário.

A lei geral de proteção de dados, sancionada em 2020, é outro fator que pode ter influenciado positivamente as empresas a preocuparem-se com falhas em suas aplicações que pudesse gerar ataques e vazamentos de dados, melhorando assim a segurança de seus aplicativos.

É importante observar que a presença de vulnerabilidades não obrigatoriamente condena

aquela aplicação como um meio inseguro, por exemplo quando se trata de vulnerabilidades relacionadas a protocolos SSL, pode ser que a aplicação utilize outros protocolos como meio seguro de comunicação.

4.6 Entrevista com profissional da área de segurança da informação

Para entender como a parte de segurança da informação é aplicada em empresas para tratamento dos dados e prevenções de casos de fraude, foi realizada uma entrevista com o engenheiro de cibersegurança onde foram realizadas perguntas sobre segurança de dados, aplicativos móveis e sistemas de pagamentos. Conforme está descrito no Anexo A - Entrevista com Engenheiro de Cybersegurança, os principais pontos estão expostos no quadro 2.

Quadro 2: Entrevista com profissional de Cybersegurança

Principais ferramentas que os times de segurança utilizam para garantir que esses dados sejam coletados e armazenados em segurança.	Os usuários devem ser alertados sobre os dados coletados, os dados coletados devem ser selecionados de maneira minuciosa pela empresa, uma vez que o armazenamento seguro destes gera custos, por fim devem ser utilizados sistemas de monitoramento para garantir a integridade dos dados.
Relação de segurança entre Android e IOS.	O sistema *Android* possui desvantagem por conta da vasta compatibilidade de *hardware*, ocupando assim grande parte do mercado, o que torna um atrativo para criminosos encontrarem vulnerabilidades. A *Apple* possui um controle maior sobre o *IOS*, uma vez que, o número de *hardwares* em que o sistema pode ser acesso é limitado, facilitando assim o tratamento de vulnerabilidades.
Impactos da LGPD em empresas.	O usuário final foi o maior beneficiado, pois a lei possibilitou maior controle do titular sobre os dados cedidos para terceiros. O profissional de segurança e da área jurídica passou a ter voz mais ativa nas empresas, uma vez que, as empresas passaram a ter que se preocupar mais com a segurança dos dados coletados e armazenados.

Detecção de transações fraudulentas e clonagens de cartões	Atualmente o meio de pagamento de cartão de crédito e débito se tornou o mais seguro para ser utilizado em compras, o avanço tecnológico possibilitou que sistemas de monitoramento que utilizam inteligências artificiais analisem constantemente o comportamento de usuários e em caso de ações suspeitas o bloqueio do cartão é feito de maneira automática.

Fonte: Autoria própria.

5 CONSIDERAÇÕES FINAIS

Conforme apresentado a realização de transações em aplicativos em dispositivos Android cresce em ritmo acelerado, a pesquisa apresentada anteriormente mostra que 49.1% das pessoas que responderam à pesquisa realizam mais de dez compras por meio de aplicativos em um único mês. Com o advento da pandemia de COVID-19 iniciada em 2020, as autoridades de saúde recomendaram que as pessoas evitassem grandes aglomerações. Essas mudanças fizeram com que as pessoas evitassem compras em locais presenciais, como resultado disso os números de compras online tiveram um aumento significativo.

Com o aumento do número transações via aplicativos um ponto que se tornou de grande preocupação para empresas e usuários é a segurança dos dados online, com as tecnologias cada vez mais integradas, manter dados como CPF, RG, telefone, tornaram-se um desafio ainda maior, leis como a lei geral de proteção de dados foram sancionadas como uma forma de proteger o titular dos dados e obrigar, legalmente, empresas a adotarem medidas para garantir a segurança dos dados que são coletados.

Analisando aplicativos disponíveis na loja de aplicativos do sistema Android fica evidente uma preocupação em garantir a segurança das aplicações disponíveis para download, melhorias como deixar o usuário mais consciente de quais permissões aquele aplicativo que ele instalou está solicitando acesso e um processo de verificação para publicação de aplicativos na loja mais rigoroso são ferramentas utilizadas para que o usuário se sinta mais seguro, mesmo esse sendo um grande desafio, pela variedade de compatibilidade de dispositivos e marcas que utilizam o sistema, podendo cada uma fazer modificações no sistema base. Uma maneira de demonstrar a segurança dos aplicativos isso é analisar os resultados do teste automatizado realizado em diversos aplicativos onde ocorrem pagamentos, onde em sua maioria, não foram

encontradas nenhum tipo de possível vulnerabilidade.

No entanto ainda no entendimento do público o sistema da Apple, o IOS, ainda segue sendo uma alternativa mais segura, como demonstrado na pesquisa onde 62,3% das pessoas acreditam que o sistema IOS é mais seguro que o Android. Esse fato não é necessariamente verdade, mas conforme entrevista com um engenheiro de cibersegurança, a Apple tem um controle maior sobre seu sistema, isso se deve pelo fato dele estar disponível em uma variedade limitada de dispositivos, onde a fabricante é a mesma dona do sistema operacional, então toda e qualquer modificação é feita por uma única empresa. Outro ponto de atenção é que como a maioria dos dispositivos utilizados hoje rodam o sistema operacional Android, se torna um alvo mais atrativo para criminosos.

Portanto fica evidente que os aplicativos no sistema operacional Android vem se tornando cada vez mais seguros, a segurança se tornou um assunto crucial em empresas de tecnologia nos últimos anos, no entanto paralelo a isso existiram cada vez mais tentativas de ataques, que tentaram superar as barreiras de segurança impostas pelas desenvolvedoras.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. **O que é PIX.** 2023 (On-line). Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix. Acesso em: 12 out. 2023.

BODETTI, Roberto. Em alta, mercado de fintechs cresce 155% em 2021. Como é trabalhar em uma? **Exame**, 2022. Disponível em: Disponível em: https://exame.com/carreira/em-alta-mercado-de-fintechs-cresce-155-em-2021-como-e-trabalhar-em-uma_red-01/. Acesso em: 12 out. 2023.

CISO ADVISOR. **Ataques a dispositivos móveis disparam 187% em um ano.** 2023 (On-line). Disponível em: https://www.cisoadvisor.com.br/ataques-a-dispositivos-moveis-aumentaram-187-em-um-ano/. Acesso em: 12 out. 2023.

CABLE NEWS NETWORK BRASIL. **Brasil tem mais smartphones que habitantes, aponta FGV.** 2022 (On-line). Disponível em: https://www.cnnbrasil.com.br/economia/brasil-tem-mais-smartphones-que-habitantes-aponta-fgv//. Acesso em: 12 out. 2023.

DARVISH, Hesham; HUSAIN, Mohammad. Security analysis of mobile money applications on android. *In:* INTERNATIONAL CONFERENCE ON BIG DATA (BIG DATA). 2018. **Anais** […]. IEEE, 2018, p. 3072-3078. Disponível em: https://ieeexplore.ieee.org/abstract/document/8622115/. Acesso em: 12 out. 2023.

IFOOD NEWS. **Quanto cresce o uso de apps de delivery de comida no mundo?** 2022 (On-line). Disponível em: https://www.news.ifood.com.br/quanto-cresce-o-uso-de-apps-de-delivery-de-comida-no-mundo/. Acesso em: 12 out. 2023.

NUBANK. **Modo rua.** n.d. (On-line). Disponível em: https://blog.nubank.com.br/modo-rua/. Acesso em: 12 out. 2023.

PAVAN, Bruno. Brasil é um dos países com a maior taxa de celulares Android frente ao iOS. **Isto é Dinheiro**, 2023. Disponível em: https://istoedinheiro.com.br/brasil-e-um-dos-paises-com-a-maior-taxa-de-celulares-android-frente-ao-ios/. Acesso em: 12 out. 2023.

REAVES, Bradley *et al.* Mo (bile) money, mo (bile) problems: Analysis of branchless banking applications. **ACM Transactions on Privacy and Security (TOPS)**, v. 20, n. 3, p. 1-31, 2017. Disponível em: https://dl.acm.org/doi/abs/10.1145/3092368. Acesso em: 12 out. 2023.

ANEXO A – Entrevista com Engenheiro de Cybersegurança

Entrevistador: Pergunta 1 - Quando pensamos na coleta de dados pessoais de terceiros, principalmente tratando-se de CPF, endereço e nome, há uma grande preocupação em como mantê-los em segurança. Pensando nisso quais são as principais ferramentas que os times de segurança utilizam para garantir que esses dados sejam coletados e armazenas em segurança? Quais são os principais desafios?

Entrevistado: Para responder a essas perguntas, há duas respostas fundamentais. Primeiro, a coleta de informações deve ser cuidadosamente considerada, levando em conta tanto o método de coleta quanto o propósito dessa ação. É imperativo alertar o usuário, como no caso do CPF no Brasil, sobre quais dados estão sendo coletados e qual o propósito dessas informações. Por exemplo, o CPF é amplamente utilizado como identificador único, mas sua relevância não transcende fronteiras. Dados de alcance global, como o e-mail e o nome, são os mais significativos na perspectiva da privacidade global. A primeira etapa na coleta de dados deve ser direcionada ao usuário, explicando o que será coletado e por que o aplicativo precisa destas informações, garantindo a segurança da coleta e da transferência dos dados do *front end* para o *back end*.

Segundo, após a coleta de dados, a questão crucial é como armazená-los da melhor forma e como recuperá-los quando necessário. Por exemplo, para campanhas ou para a identificação de usuários, pode ser necessário acessar as informações na base de dados. No entanto, o armazenamento seguro envolve desafios de segurança, já que a criptografia de dados requer recursos computacionais adicionais, o que pode aumentar a infraestrutura da empresa. Portanto, é fundamental analisar por que e como os dados estão sendo armazenados. Além disso, a decisão de armazenar dados criptografados pode ser afetada pelos custos operacionais,

levando à necessidade de controles compensatórios. Isso inclui a definição de quem tem acesso aos dados, onde eles serão armazenados e quais aplicativos e pessoas podem acessá-los, indo além da criptografia e se concentrando na gestão de acesso.

Além desses aspectos, a observabilidade e o registro de logs desempenham um papel importante na garantia da integridade dos dados. A maioria das empresas costumava incluir informações como CPF e e-mail em registros de log, mas isso raramente é necessário fora da área de segurança. Para garantir que os dados confidenciais não sejam expostos, é aconselhável anonimizar ou mascarar esses dados, evitando que informações sensíveis sejam acessíveis em locais inadequados, como em planos de teste abertos.

Para a equipe de segurança, essas informações são de grande importância, pois ajudam a detectar possíveis usos indevidos, fraudes e ataques, como o *Account Recovering*. Em resumo, a coleta e o armazenamento seguros de dados são cruciais para garantir a privacidade e a segurança das informações, requerendo uma abordagem cuidadosa que leve em consideração a necessidade de coleta, a criptografia, a gestão de acesso e a observabilidade.

Entrevistador: Pergunta 2 - Hoje o aplicativo está disponível nas versões de Android e IOS, existe um sistema operacional móvel mais seguro? Caso sim, por qual motivo você acredita que isso acontece? Existe diferença nas ferramentas de segurança utilizadas entre os sistemas?

Entrevistado: Em relação à gestão de registros, a empresa estabeleceu padrões distintos para logs gerais e logs de segurança. A principal complexidade reside em convencer as partes interessadas de que certos dados sensíveis não são necessários nos registros gerais. Isso requer uma abordagem de 'privacidade por design' para garantir o acesso restrito às informações sensíveis apenas para aqueles que realmente precisam delas, de maneira segura.

No contexto da segurança de sistemas operacionais, a vulnerabilidade do sistema Windows não está relacionada à sua qualidade, mas sim à sua ampla adoção e uso. Devido à sua popularidade, o *Windows* se tornou um alvo atrativo para ataques. Por outro lado, sistemas menos difundidos como o *Linux* e o *MacOS* são menos vulneráveis devido ao seu menor uso entre os usuários finais. Isso se deve em parte à facilidade de ataque aos sistemas de usuários finais, em comparação com servidores projetados para maior segurança.

Comparando o *Windows* com o Android, a acessibilidade e a diversidade de dispositivos Android tornam-no mais suscetível a ataques em comparação com o IOS da Apple, que investe significativamente em segurança devido ao controle direto sobre seus dispositivos. A natureza de código aberto do Android e a variedade de fabricantes e modificações contribuem para sua

vulnerabilidade.

A segurança está fortemente relacionada ao controle do fabricante sobre o ecossistema, tornando os dispositivos Apple mais seguros do que os dispositivos Android, devido à sua natureza mais diversificada e aberta.

Entrevistador: Pergunta 3 - Existe diferença em relação aos requisitos e controles de segurança requiridos por cada loja de aplicativo? Existe diferença no processo de submissão de app entre elas?

De acordo com um informante em um artigo recente, a Apple é reconhecida por ser pioneira em relação aos requisitos e controles de segurança necessários para aplicativos disponibilizados em sua loja. A empresa é elogiada por manter um alto padrão de qualidade e privacidade para o usuário final. Ao contrário do *Google*, a Apple é mais criteriosa na avaliação dos aplicativos, verificando o conteúdo, a linguagem nativa e as permissões solicitadas. Ela também realiza testes abrangentes, incluindo geolocalização e testes multi-região, garantindo que o aplicativo seja adequado para diferentes públicos.

A Apple se destaca por sua abordagem de solicitar permissões aos usuários, tornando-a mais segura e preocupada com a experiência do usuário. Além disso, a empresa está atenta ao que é coletado pelos aplicativos e restringe algumas coletas de informações, exigindo justificativas para a coleta de dados que não sejam relacionados à segurança.

Em contraste, o *Google* está melhorando seus processos de avaliação, mas não se iguala à abordagem rigorosa da Apple. A Apple é elogiada por sua ênfase na qualidade do usuário e por garantir que os aplicativos sejam compatíveis com seus dispositivos. Em resumo, a Apple é vista como mais criteriosa em relação à segurança, qualidade e privacidade, demonstrando um compromisso contínuo com a satisfação do usuário.

Entrevistador: Pergunta 4 - Hoje pensando em sistemas de pagamentos vemos diversos aplicativos utilizando empresas terceirizadas em seus sistemas de pagamentos, na sua opinião quais são as vantagens disso?

Entrevistado: A utilização de parceiros especializados em pagamentos oferece vantagens significativas, como aprimoramento dos fluxos de transações e a segurança nas transações de cartão de crédito. A primeira vantagem evidente na utilização de empresas de pagamento é a expertise que elas oferecem. Essas empresas dedicam recursos significativos em tecnologia e profissionais, direcionados para a melhoria dos fluxos de transações, especialmente no que diz respeito às transações com cartão de crédito. Isso se diferencia consideravelmente de uma empresa que está apenas começando a criar um produto, como no caso do varejo. Ao

recorrer a um parceiro, a empresa não precisa se preocupar tanto com questões de segurança, regulamentações, regras e privacidade, pois o parceiro já lida com esses aspectos. Essa é, sem dúvida, a principal vantagem percebida ao utilizar um parceiro especializado.

No entanto, vale mencionar que, na minha opinião, uma desvantagem potencial pode estar nos custos associados. Muitas vezes, os preços cobrados por esses serviços especializados tendem a ser mais elevados devido à experiência e segurança oferecidas. Em algumas situações, o custo das transações pode ser significativamente alto, especialmente em setores onde o valor da transação é relativamente baixo, tornando-se um fator a ser considerado ao optar por parceiros de pagamento. Portanto, a escolha do parceiro de pagamento deve levar em consideração o valor agregado em relação aos custos associados, dependendo do ramo de atuação da empresa e do tipo de transações envolvidas.

Além disso, a taxa de processamento de pagamentos pode variar dependendo do setor e do tipo de produto sendo vendido. Em alguns casos, os custos associados às transações podem representar uma porcentagem significativa do valor total da compra, tornando essas parcerias mais onerosas para as empresas.

Portanto, a utilização de parceiros de pagamento oferece benefícios em termos de expertise e alívio de preocupações regulatórias e de segurança, mas pode resultar em custos adicionais que as empresas devem considerar ao tomar decisões sobre processamento de pagamentos.

Entrevistador: Pergunta 5 - Em 14 de Agosto de 2018 foi sancionada a Lei Geral de Dados Pessoais (LGPD). Baseado na sua experiência de trabalho quais foram os principais impactos que essa nova lei trouxe nas empresas?

Entrevistado: Usuário final foi o principal beneficiado, por conta da preservação e confidencialidade dos dados. A LGP na minha opinião é uma cópia da GDPR “abrasileirada”, mas sem dúvidas o mais beneficiado foi o usuário final, o consumidor, tendo sua privacidade beneficiada e favorecida, no final do dia ele vai ser melhor ouvido caso algo aconteça com seus dados. Por exemplo, antigamente existiam pessoas vendendo dados, com os vazamentos de dados e o surgimento da LGPD, as empresas precisam se justificar em caso de incidente e até mesmo punidas, aumento assim o nível de cuidado com a segurança.

Pelo lado da empresa, o profissional de segurança e jurídico (DPO), é um pouco mais ouvido quando se trata de questões de segurança para o usuário, quando é solicitada a inserção de ferramentas de segurança, para garantir prevenção de vazamentos de dados e rastreabilidade de dados, para identificar se houve o acesso a uma informação sensível sem autorização, por

gestão de acesso e controles de logs e auditoria. Então as empresas precisam ouvir mais o profissional de segurança, para obrigatoriamente garantir a segurança nas tecnologias e solução que são desenvolvidas.

Entrevistador: Pergunta 6 - Hoje vemos com mais frequências as fraudes e clonagens de cartões. Hoje no sistema tem como saber se vai acontecer uma transação fraudulenta e se tem alguma prevenção para dados de cartões clonados?

Entrevistado: Tem sim, e é evidente que a evolução da tecnologia tem transformado o cartão de crédito em um meio de pagamento altamente evolutivo e seguro. Atualmente, existem diversas ferramentas e mecanismos de defesa que monitoram o comportamento do usuário em suas transações. Essas ferramentas levam em consideração a frequência de uso do cartão, a região em que ele é utilizado e o padrão de gastos diários do usuário, bem como o número de tentativas de uso e a velocidade das transações.

Além disso, os cartões de crédito oferecem mecanismos de defesa como bloqueio em caso de uso suspeito, desbloqueio para transações internacionais e códigos de segurança em constante alteração. Essas medidas de segurança visam a proteção das transações online, que representam a maioria das compras atualmente. Essas transações, embora mais difíceis de identificar, contam com mecanismos de detecção e identificação que asseguram a segurança dos usuários.

No entanto, é importante ressaltar que, embora o uso do cartão de crédito seja extremamente seguro, a clonagem de cartões ainda é uma ameaça, especialmente com a popularização das compras por aproximação via NFC. Nesse cenário, é fundamental que os usuários e as empresas estejam atentos a transações suspeitas e comportamentos não autorizados. No caso de fraude, o processo de estorno, conhecido como *chargeback*, pode ser acionado, permitindo que os usuários contestem compras fraudulentas.

A responsabilidade pela segurança das transações varia dependendo do contexto. Em compras online, a responsabilidade normalmente recai sobre o estabelecimento onde a compra foi realizada. Caso o estabelecimento tenha um parceiro de segurança, a responsabilidade é compartilhada. No entanto, a responsabilidade final de estorno recai sobre o emissor do cartão de crédito. Portanto, é crucial que as empresas, como varejistas online, garantam a segurança das transações para evitar multas e prejuízos aos usuários.

A evolução dos mecanismos de segurança no uso do cartão de crédito tem tornado esse meio de pagamento extremamente seguro. No entanto, é importante que os usuários estejam atentos a transações suspeitas e que as empresas garantam a segurança das compras realizadas

em seus estabelecimentos. Isso contribui para a prevenção de fraudes e a proteção dos direitos dos consumidores.