UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO

Isadora Fontoura Pedroso

ANÁLISE DE CASOS FRAUDULENTOS DE SEGURANÇA CIBERNÉTICA EM ORGANIZAÇÕES

PORTO ALEGRE
2023

Isadora Fontoura Pedroso

ANÁLISE DE CASOS FRAUDULENTOS RELACIONADOS À SEGURANÇA CIBERNÉTICA EM ORGANIZAÇÕES

Trabalho de Conclusão de Curso apresentado à Escola de Administração da Universidade Federal do Rio Grande do Sul, como parte dos requisitos para a obtenção do título de Bacharel em Administração.

Orientador do TCC: Prof.º André Teixeira Pontes

PORTO ALEGRE
2023

Isadora Fontoura Pedroso

ANÁLISE DE CASOS FRAUDULENTOS RELACIONADOS À SEGURANÇA CIBERNÉTICA EM ORGANIZAÇÕES

Trabalho de Conclusão de Curso apresentado à Escola de Administração da Universidade Federal do Rio Grande do Sul, como parte dos requisitos para a obtenção do título de Bacharel em Administração.

Orientador do TCC: Prof.º André Teixeira Pontes

Conceito Final: B

Aprovado em: 03/04/2023

BANCA EXAMINADORA:

Examinadora - Profa. Dra. Daniela Francisco Brauner – UFRGS

ANDRE TEIXEIRA PONTES:09043326755 Assinado de forma digital por ANDRE TEIXEIRA PONTES:09043326755 Dados: 2023.04.05 12:36:08 -03'00'

Orientador - Prof. Dr. André Teixeira Pontes - UFRGS

PORTO ALEGRE
2023

RESUMO

O presente trabalho tem como objetivo analisar casos de fraudes relacionadas à segurança cibernética em organizações. Através de uma abordagem qualitativa, a pesquisa utilizou uma análise documental e entrevista com um especialista para analisar os casos cedidos pela empresa Axur. Foram identificadas as estratégias utilizadas para solucionar o problema e prevenir a recorrência. Além disso, foi discutido o cenário encontrado nos casos analisados frente aos desafios atuais da crescente digitalização dos negócios. Como resultado, ficou evidente a importância da segurança cibernética na atualidade, bem como a necessidade de as empresas estarem preparadas para responder a possíveis violações de segurança e ter um plano de resposta a incidentes bem definido e testado regularmente. Concluiu-se que a conscientização e educação sobre fraudes nos times de segurança são essenciais para avaliação constante dos riscos e vulnerabilidades, sendo fundamentais para a ação rápida e eficiente contra os possíveis incidentes.

Palavras-chaves: fraudes, segurança cibernética, segurança da informação, ataques cibernéticos

ABSTRACT

The present work aims to analyze cases of cyber security-related frauds in organizations. Using a qualitative approach, the research utilized document analysis and an interview with an expert to examine the cases provided by the company Axur. The strategies used to solve the problem and prevent recurrence were identified. In addition, the scenario found in the analyzed cases was discussed in light of the current challenges of increasing digitization of business. As a result, the importance of cyber security in today's world became evident, as well as the need for companies to be prepared to respond to possible security breaches and to have a well-defined and regularly tested incident response plan. It was concluded that awareness and education about fraud in security teams are essential for constant risk and vulnerability assessment, and are fundamental for quick and efficient action against possible incidents.

Keywords: fraud, cyber security, information security, cyber attacks

ESPAÇO PARA FICHA CATALOGRÁFICA

SUMÁRIO

1. INTRODUÇÃO 8
2. REVISÃO TEÓRICA 10
2.1 Transformação Digital 10
2.2 Segurança da Informação 11
2.3 Ataques Cibernéticos 12
2.4 Impactos negativos nas Organizações 14
3 OBJETIVOS 16
3.1 Objetivo Geral 16
3.2 Objetivos Específicos 16
4. METODOLOGIA 17
4.1. Obtenção dos casos analisados 17
4.2. Análise dos casos selecionados 18
5. RESULTADOS E DISCUSSÃO 19
5.1. Um prevê panorama sobre a atuação do especialista em casos envolvendo fraudes cibernéticas 19
5.2. O caso envolvendo a empresa Finamax 21
5.3 Casos envolvendo a empresa Polar 23
5.4 Casos envolvendo o grupo Lapsus$ 25
5.5 Prevenções e estratégias 26
6. CONSIDERAÇÕES FINAIS 30
REFERÊNCIAS 32
APÊNDICE 1 – QUESTIONÁRIO PARA A ENTREVISTA 36
APÊNDICE 2 – RESPOSTAS DO ENTREVISTADO 37

1. INTRODUÇÃO

Novas tecnologias estão trazendo avanços e modificações nos ambientes e formatos de trabalho, ocasionando em melhorias da ciência da computação como inteligência artificial, automação e robótica (BARRA, 2019). Segundo o site Monitora (2021), adaptar-se à transformação digital é a prática mais importante para os negócios, o que envolve preparar-se para lidar com casos de violação da segurança cibernética. Este contexto, reforça a importância da cibersegurança, definida pela FIA (2022) como:

> Uma soma de ações e técnicas que visam proteger sistemas, redes, programas e equipamentos de invasões, garantindo que dados valiosos não sejam violados ou vazados (FIA, 2022)

Em decorrência do crescente avanço tecnológico, segundo a Revista Target (TARGET REAL ESTATE, 2020), aumentou-se também o número de invasões em sistemas e venda de dados sensíveis, em mesmo grau e proporção. A digitalização forçada pela pandemia, a qual não foi seguida dos cuidados necessários em muitas organizações, contribuiu para um aumento de casos de crimes, fraudes e ataques cibernéticos de diferentes tipos (BARBOSA et al., 2021). Nota-se uma evolução tanto no nível dos ataques quanto na extensão, visto que são capazes de atingir diversas regiões e países (DE ARAÚJO E ROSSI, 2020). O Brasil, neste cenário, encontra-se em segundo lugar no ranking de ataques na América Latina, tendo um aumento no ano de 2022 considerável de 950% em relação ao ano de 2020 (OLIVEIRA, 2022).

Uma vez que as informações são ativos de grande valor para as organizações e que os ataques estão cada vez mais sofisticados, garantir a segurança cibernética é um verdadeiro desafio organizacional. A Lei Geral de Proteção de Dados (LGPD), aumenta a responsabilidade das empresas na proteção dos dados, visto que será penalizada a empresa que cause o vazamento, mesmo que acidental (NETTO, 2019). Desta forma, falhas de segurança em sistemas de informação afetam a credibilidade da empresa, além de causar prejuízo financeiro (SOFTWALL, 2019).

A conscientização das organizações é o primeiro passo para aprender a lidar com a cibersegurança, e por consequência agir estrategicamente para combater vazamentos e ataques oriundos de cibercriminosos. Além disso, sabe-se que na mesma proporção que a tecnologia avança, os ataques se atualizam, fazendo com que seja necessário estar sempre atualizado, reforçando assim a importância da segurança da informação. Porém, deve-se atentar que os investimentos em

segurança das informações não impedem a ocorrência de ataques, mas ajudam a identificá-los, diminuindo então as chances de algum prejuízo ligados às informações (CORTEZ E KUBOTA, 2012).

Além dos mecanismos de defesa internos que as organizações devem implementar (infraestrutura de tecnologia da informação, controle de acesso, firewall, etc.), torna-se necessário identificar e agir sobre os riscos externos, com ações como monitoramento de fraudes e riscos digitais tanto na web superficial como na *deep* e na *dark* web. Uma das táticas mais usadas por cibercriminosos é a criação de sites falsos, que imitam a aparência de sites legítimos de empresas conhecidas.

Neste âmbito, este trabalho analisou três casos de fraudes relacionadas à segurança cibernética cedidos pela Axur, uma empresa na área de *Cyber Threat Intelligence* (CTI). Buscou-se responder à questão “Que lições podem ser extraídas dos casos analisados para auxiliar as organizações a evitar fraudes relacionadas à segurança cibernética?”.

2. REVISÃO TEÓRICA

2.1 Transformação Digital

A Transformação Digital tem uma importância crescente para as organizações em todo o mundo, pois está mudando fundamentalmente a maneira como as empresas operam e se relacionam com seus clientes. A adoção da tecnologia digital está permitindo às empresas melhorar sua eficiência operacional, aumentar a produtividade, personalizar a experiência do cliente e criar novas fontes de receita (BARBOSA, COSTA E PONTES, 2020).

Esta transformação não se trata apenas de tecnologia, mas de como as empresas se relacionam com seus clientes, parceiros e funcionários. Ela oferece insights sobre como as empresas podem usar a tecnologia para criar novos modelos de negócios, melhorar a experiência do cliente e aumentar a eficiência operacional (ROGERS, 2018).

No entanto, a Transformação Digital também apresenta desafios para as empresas. Um dos principais desafios é a necessidade de investir em infraestrutura de tecnologia da informação (TI) e em capacitação de funcionários para que possam trabalhar com as novas tecnologias. Além disso, as empresas precisam lidar com preocupações de segurança cibernética, privacidade de dados e ética em relação ao uso de tecnologias digitais (ROGERS, 2018).

Para superar esses desafios, as empresas podem aproveitar as oportunidades que a Transformação Digital oferece. A adoção de tecnologias como Inteligência Artificial, Internet das Coisas, *Big Data* e *Cloud Computing* pode ajudar as empresas a coletar e analisar grandes volumes de dados em tempo real, permitindo que tomem decisões mais informadas e baseadas em evidências. A automação de processos e a robótica podem reduzir custos e melhorar a eficiência operacional.

A Transformação Digital também permite às empresas criar novas fontes de receita, como a venda de serviços digitais, o desenvolvimento de produtos personalizados e a exploração de novos mercados online. A personalização da experiência do cliente também pode aumentar a fidelidade e a satisfação do cliente, criando oportunidades para a construção de relacionamentos duradouros.

Segundo um estudo da consultoria McKinsey, a Transformação Digital pode aumentar a produtividade em até 20%, reduzir custos em até 30% e aumentar a receita em até 20%. No entanto, para alcançar esses resultados, as empresas

precisam estar dispostas a investir em tecnologia, capacitação de funcionários e infraestrutura de TI (MCKINSEY & COMPANY, 2017).

2.2 Segurança da Informação

A segurança da informação é um tema crítico para as organizações, especialmente em um mundo onde a digitalização dos processos e a crescente conectividade trazem muitos benefícios, mas também muitos riscos. A segurança da informação refere-se à proteção dos dados e sistemas da organização contra ameaças como acesso não autorizado, roubo de informações, sabotagem, entre outras.

Os principais desafios enfrentados pelas empresas em relação à segurança da informação incluem a complexidade dos sistemas, o aumento do volume de dados e a sofisticação dos ataques cibernéticos. A solução para esses desafios requer a implementação de medidas de segurança de TI, treinamento de funcionários e um comprometimento da alta administração com a segurança da informação.

Um estudo publicado em 2018 destacou que a adoção de medidas de segurança de TI pelas empresas pode ter um impacto positivo na percepção do cliente em relação à marca. Além disso, a pesquisa também indicou que os clientes estão dispostos a pagar mais por produtos e serviços de empresas que demonstram preocupação com a segurança da informação (KIM, KIM e SHIN, 2018).

No entanto, os riscos de fraude relacionados à segurança da informação continuam sendo uma grande preocupação para as empresas. Kumar, Bidwaik e Singh (2020) identificaram que as fraudes relacionadas à segurança cibernética são um dos principais tipos de ameaça cibernética enfrentadas pelas empresas. Estas fraudes podem incluir phishing, spoofing, ramsomware, entre outras técnicas usadas pelos criminosos cibernéticos para obter acesso a informações confidenciais.

Para combater essas ameaças, as empresas precisam adotar medidas de segurança robustas, como autenticação de usuários, criptografia de dados, controle de acesso e monitoramento constante de ameaças cibernéticas. Além disso, é fundamental que as empresas invistam em treinamento de funcionários para que possam identificar e relatar atividades suspeitas (NEOWAY, 2020).

Para Fontes (2006) qualquer organização está sujeita a vazamentos de dados, por isso toda informação utilizada pela empresa é um bem valioso e precisa estar protegida.

2.3 Ataques Cibernéticos

Segundo Garrett (2021), crimes cibernéticos são aqueles que geram danos por meio de extorsão de recursos financeiros, estresse ou à reputação de vítimas que podem ser indivíduos ou patrimônios. Para isso são utilizadas redes de computadores, computadores ou dispositivos eletrônicos conectados para ações criminosas.

De acordo com o site da Posesa (2021), os cibercrimes mais comuns no Brasil são furto e vazamento de dados, crimes contra honra e estelionato que ocorre através do Phishing.

A legislação brasileira tem evoluído para acompanhar esta problemática, destacando-se as seguintes leis:

- **Lei Carolina Dieckmann (12.737/2012)**, referente a invasão de celulares e computadores, violação de dados dos usuários e interrupção de sites (governamentais ou não)
- **Lei 12.965/2014**, que surgiu para regular os direitos e deveres dos usuários das redes, protegendo seus dados, assim possibilitando a retirada de conteúdos do ar, seja eles pornográficos, violentos ou ofensivos.
- **LGPD (13.709/2018)**, protege a captação, armazenamento e compartilhamento de dados pessoais que são coletados por sites e empresas de forma online.
- **Lei 14.155/2021**, pune crimes de invasão de dispositivos, furtos qualificados e estelionato no meio digital, além de destruição de dados e instalação de vírus para vantagem ilícita.

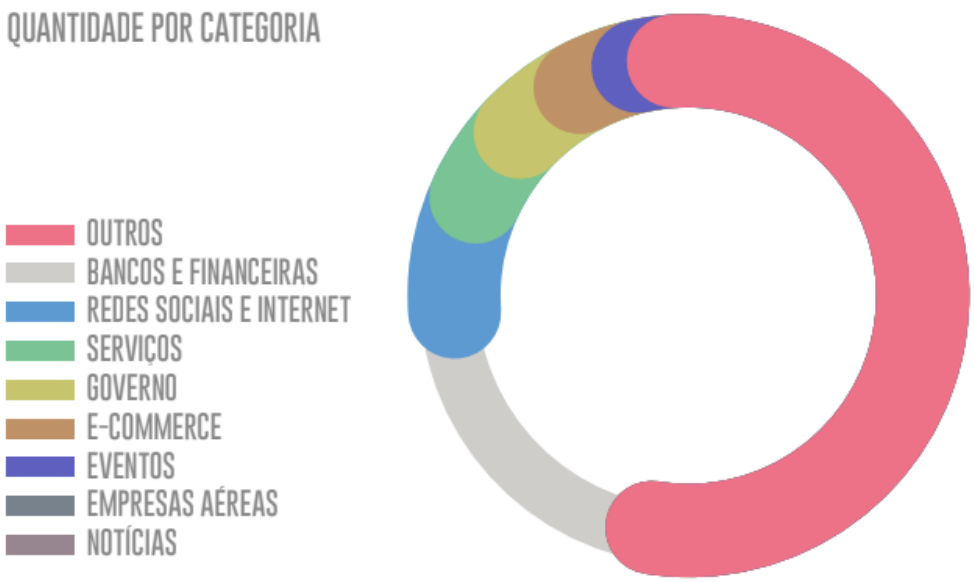
Schendes (2022) apresenta dados mundiais onde uma em cada quarenta empresas são vítimas de ataques cibernéticos por semanas, ocasionando em um aumento de 59% ao mesmo período de 2021. O Brasil ainda possui uma média de incidentes maior que a média global.

Frisa-se que nem sempre a utilização dos dados roubados tem por objetivo a comercialização. Nesse sentido, Nunes e Marques (2019) explicam:

> Diante desse cenário, constata-se a crescente agressão à privacidade dos indivíduos qualquer que seja a forma que o coletor de dados pretende utilizá-los. Pois, se o titular desses dados desconhecer, não há como haver legalidade no ato, somente se pode concluir que o usuário da internet representa o sujeito hipossuficiente frente aos demais atores virtuais, estando em evidente falta de mecanismos para combater o descontrole do direito à privacidade, no ambiente virtual (NUNES E MARQUES, 2019).

Conforme o Relatório Anual de Segurança de 2021, os setores mais atingidos por fraudes com e-mails maliciosos para atrair usuários a sites clonados ou roubo de informações, estão demonstradas na Figura 1.

Figura 1 – Setores mais atingidos por fraudes com e-mails maliciosos em 2021



Fonte: Relatório Anual de Segurança da Informação - RNP (2021)

De acordo com a autora Pinheiro (2020), foi estabelecido o significado de alguns ataques cibernéticos comuns na internet, onde possuem direcionamento para indivíduos, sejam eles direto ou em massa, outros corporativos e também a governos. Todos ocorrem por técnicas e falhas que são desenvolvidas. Para isso ela começa especificando o Phishing:

> Traduzido livremente como “pescaria” ou “golpe de pescaria”, consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um *link* falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados, ou acesso e elevação de privilégios. É uma técnica de engenharia social.

Ela ainda frisa que o e-mail ainda é o vetor mais conhecido para propagação dessa fraude, sendo o mais bem-sucedido ataque. Após ela fala sobre Malware:

> Os *malwares* normalmente visam à subtração de informações, ao controle da máquina e da infraestrutura de rede, à disseminação local ou remota, a ser um vetor de ataques e à extorsão por sequestro dos dados ou vazamento de informações, podendo ter um ou mais desses propósitos como funcionalidade.

O Malware se trata de um software malicioso, ou seja, suas fontes podem ser páginas de web comprometidas podendo ser oficiais já atingidas, ou criadas no interesse de propagar o vírus, ou arquivos, programas e anexos vindos de softwares “piratas”, além de equipamentos com vulnerabilidades. Algumas vezes o roubo

dessas informações é utilizado apenas para venda em canais de fraudadores para proveito próprio.

Seguindo com os ataques, ela traz o conceito de Ransonware, como um malware utilizado para o sequestro dos dados das vítimas. Nesse caso, após o roubo das informações esses dados são criptografados, o que deixa muito mais complicada a recuperação, pois após pedido de resgate nem sempre é enviado um código para o acesso novamente dessas informações, podendo até fazer o apagamento dos dados originais, impossibilitando a recuperação deles.

2.4 Impactos negativos nas Organizações

O crescimento do avanço tecnológico trouxe consigo consequências e dentre elas os ataques cibernéticos são os mais preocupantes. Primeiramente, segundo pesquisas, o Brasil é o país da America Latina que mais sofre desses ataques, tendo sofrido 88 bilhões de tentativas em 2021 (FIRST TECH, 2022).

> De acordo com uma outra pesquisa realizada pelo Allianz Risk Barometer, 64% dos brasileiros veem os incidentes cibernéticos como principal fator de risco às empresas em 2022 (FIRST TECH, 2022).

Segundo Demartini (2022), foi pontuado os setores mais atingidos globalmente pelos ataques e dentre eles são: governamentais e militares, de educação e pesquisa ou saúde, além de setores de atacado e varejo que também tiveram um aumento significativo no segundo trimestre de 2022 em 182%.

De acordo com o estudo feito por Nunes e Marques (2019) sobre um ataque cibernético no Hospital de Câncer de Barretos (SP), considerado um dos maiores ciberataques mundiais ocorrido em 2017, onde dados foram criptografados e mais de mil computadores bloqueados, impedindo o bom funcionamento do hospital nos processos de consultas, exames e sessões de radioterapia. Nesse caso, além do transtorno interno do ambiente, os pacientes também estavam sujeitos a terem seus dados pessoais expostos. Foi concluído então que deveria ser criado ações para proteção e vigilância digital, juntamente com legislações que asseguram a privacidade dos indivíduos.

Para que organizações evitem ataques diante de um cenário onde há um crescente volume de incidentes, é necessário que as medidas de proteção sigam um padrão: atualizar sistemas, realizar backups e manter rotinas de monitoramento e proteção de acessos (DEMARTINI, 2022)

Outro estudo realizado por Pinto e Grassi (2020), referente as ações tomadas pelo Brasil para enfrentar essas ameaças cibernéticas. Concluindo-se que há

vulnerabilidade e necessidade de atenção e incentivo financeiro que sejam direcionados para pesquisar e ferramentas avançadas, além de treinamentos e desenvolvimento de programas. Alguns quesitos foram pontuados também pelas autoras referente à alguns obstáculos encontrados:

> A dificuldade de rastreamento do agressor, a questão da atribuição de responsabilidade, a dificuldade em delimitar espaços soberanos e a falta de regulamentação internacional são considerados importantes entraves para sanções ou represálias em casos de ataques cibernéticos (PINTO E GRASSI, 2022).

Em decorrência do alto índice de ameaças cibernéticas, a 3ª Pesquisa ANBIMA de 2020, compartilhou que 95% das empresas analisadas por eles contam com algum programa, política ou procedimento de cibersegurança, demonstrando que organizações estão evoluindo nas práticas que devem ser adotadas para prevenção. Ainda notaram que tais medidas são adotadas por responsáveis de áreas como TI, risco e *compliance,* que estão diretamente ligados a avaliações referentes a vulnerabilidade e ameaças que atingem as empresas. Nota-se também que entre 2018 e 2020, houve um aumento referente a planos de respostas sobre incidentes, comprovando que as empresas de forma geral, estão mais preocupadas com a cibersegurança.

3 OBJETIVOS

3.1 Objetivo Geral

O objetivo deste trabalho é analisar casos de fraudes relacionadas à segurança cibernética em organizações.

3.2 Objetivos Específicos

Para responder ao objetivo central deste estudo, foram estabelecidos os seguintes objetivos específicos:

a) Analisar os casos de fraudes relacionadas à segurança cibernética cedidos pela empresa Axur.

b) Analisar as estratégias utilizadas para solucionar o problema e para prevenir que ele se repita.

c) Discutir o cenário encontrado nos casos analisados frente aos desafios atuais da crescente digitalização dos negócios.

4. METODOLOGIA

Esta pesquisa tem abordagem de natureza qualitativa, baseada em análise documental e na entrevista realizada com um especialista.

Uma análise documental, se constitui a partir de documentos, escritos ou não, que servem como objeto de estudo e investigação de dado assunto. Por isso, a pesquisa documental possibilita formas de compreensão e auxiliar como instrumento metodológico complementar (SÁ-SILVA; ALMEIDA & GUINDANI, 2009). Já a entrevista, é um método para coleta de dados mais direta, permitindo ser mais eficiente com sua base de dados (SANTOS, 2018). Neste caso, ambas coletas de pesquisa qualitativa, podem se complementar para maior embasamento dos casos abordados.

4.1. Obtenção dos casos analisados

Inicialmente solicitou-se à empresa de *Cyber Threat Intelligence* a disponibilização de casos de fraudes relacionadas à segurança cibernética, informando os objetivos desta pesquisa. Após análise, a empresa indicou quatro casos que julgou representativos das situações mais relevantes e atuais de fraude, disponibilizando alguns materiais relacionados a estes casos. Destaca-se, portanto, uma limitação importante desta pesquisa, que possui um viés de seleção, uma vez que o pesquisador não teve autonomia para a escolha dos casos.

A despeito da limitação exposta, os casos selecionados, além de representarem casos de relevância no histórico de atuação da empresa, são utilizados em materiais de divulgação da empresa como “cases de sucesso”, o que reforça a relevância destes casos como exemplo para as organizações. Destaca-se também, que os materiais disponibilizados pela empresa não são sigilosos, estando presentes em peças de divulgação como vídeos no youtube e postagens em redes sociais da empresa.

Os casos disponibilizados foram:

- **Finamax:** trata-se de um caso de páginas falsas utilizando a marca da empresa. A Axur indicou este caso e o vídeo disponível no youtube (https://www.youtube.com/watch?v=zrHOU5kpdEo&t=14s).

- **Polar:** empresa de produtos esportivos alvo de anúncios online ilegais. Foi indicado como material de informação para esta pesquisa o vídeo disponível no youtube (https://www.youtube.com/watch?v=Ns_kPkcsktA).
- **Lapsus$:** trata-se de um grupo hacker que, em suas operações, atuou em roubo e vazamento de diversos sistemas na *deep* e *dark* web. Devido à sensibilidade dos casos, as empresas não autorizaram que seus nomes fossem expostos, apenas abordar sobre os vazamentos ocorridos. Para contextualizar mais as fraudes do Grupo Lapsus$, existem alguns casos expostos na internet, em sites de jornais, que serão também disponibilizados para maior entendimento do contexto e proporção dos ataques cometidos.

4.2. Análise dos casos selecionados

Foram analisados os casos indicados pela empresa, que representaram diferentes situações, para que se adquira um conhecimento mais amplo de acordo com a descrição destes problemas, com o tipo de incidente cibernético encontrado, desafios e como foi solucionado os problemas, além de entender quais estratégias foram levadas para que não ocorresse ataques futuros.

Considerando que os materiais fornecidos pela empresa podem não ter o nível de detalhamento desejado para a pesquisa, buscou-se complementar informações através da entrevista de um especialista em *Cyber Threat Intelligente,* que atuou nos casos analisados, além da busca por mais informações públicas sobre os casos. Para a entrevista, utilizou-se o questionário disponível no Apêndice 1. A entrevista foi realizada de forma remota, com o auxílio do Google Meet.

Através deles, será levantado informações que comparem a maneira como fraudadores agiram, como cada caso impactou internamente de forma negativa, de que jeito esses problemas foram resolvidos e quais estratégias foram adotadas para prevenir futuros ataques.

Com base nestas fontes de informação, será então discutido os cenários encontrados nos cases, demonstrado quais soluções foram tomadas e estratégias escolhidas também para solucionar e assim, entender como casos como estes estão cada vez mais presentes com o crescimento digital e ver como exemplo de que forma as empresas deveriam de prevenir contra ataques cibernéticos.

5. RESULTADOS E DISCUSSÃO

Neste capítulo são apresentados os resultados dos casos analisados a partir dos dados disponibilizados pela empresa Axur, juntamente com a visão do especialista entrevistado.

5.1. Um prevê panorama sobre a atuação do especialista em casos envolvendo fraudes cibernéticas

Na entrevista, o especialista iniciou apresentando um panorama geral da sua área de atuação, informando que houve um aumento de demanda nos últimos anos frente a fraudes digitais e ataques cibernéticos. Na sua visão, estas fraudes acarretam em diversos problemas não somente financeiros, mas também reputacionais ao nome das marcas, gerando um escalonamento de dificuldades para serem resolvidas.

Na entrevista foi levantado o quão desafiador é atuar na linha de frente principalmente porque existem diversos modelos de fraudes de acordo com múltiplos clientes e diversos modelos de negócio e é por isso que um especialista precisa entender tal complexidade para uma montagem de estratégia que faça sentido ao cliente e sejam eficazes. O especialista nesta área deve conhecer, portanto, não apenas os aspectos técnicos dos diferentes tipos de fraudes, mas os diferentes modelos de negócio que são atacados. Um ponto positivo, é que o comportamento do fraudador permanece o mesmo, o que se modifica é a migração por setor ou empresa.

> A gente percebe que o atacante não para de fazer a fraude quando o cliente bloqueia aquilo, ele vai pro vizinho e vai fazendo ataque no vizinho e ai o vizinho bloqueia, e ele vai para o outro vizinho, ele não vai deixar de parar, ele só para de fazer isso quando ele é preso. Então assim, o fraudador ele não para, ele da um tempo, é o que acaba acontecendo.

Segundo o entrevistado, é desafiante entender o comportamento do atacante, por isso há um TTP (tática, técnica e procedimentos) servindo como técnica de plano para que se atue na causa raiz do problema, para eliminação seja de um ecossistema inteiro, não apenas de um cenário de fraude.

Os TTPs descrevem como os golpistas virtuais orquestram, executam e gerenciam seus ataques. Assim, são definidos como padrões de atividades ou métodos associados a um ator de ameaça específico ou grupo de atores de ameaça.

Ou seja, o foco é no estilo e comportamento, e não tanto nas ferramentas (OSTEC, 2021)

Outro ponto levantado pelo entrevistado é que muitas empresas possuem total visibilidade daquilo que acontece internamente, mas possuem dificuldade de acompanhar fraudes externas à empresa, como a presença de um site falso. Neste cenário, o entrevistado citou que há empresas, como a Axur, que auxiliam no monitoramento e na resposta às fraudes externas. Por isso, a conexão entre a equipe de investigação junto com os times internos das empresas é um diferencial importante para a prevenção de fraudes e criação de valor para as empresas.

Anteriormente já abordada a visão de Barbosa et al., (2021) sobre a crescente digitalização no decorrer da pandemia e o aumento de ataques e fraudes, foi levantado na pesquisa a hipótese de estarem realmente ligados, aprofundando com uma visão mais direcionada sobre a causa. Neste ponto, o especialista trouxe um olhar pessoal sobre a situação:

> Pra mim, o maior reflexo não é porque as empresas digitalizaram, mas a gente teve uma adoção massiva de serviços digitais por pessoas que não estavam digitalmente incluídas.

Ou seja, nessa aceleração coube ali um espaço apropriado para fraudadores começarem a atingir pessoas mais vulneráveis ou com desconhecimento de ferramentas digitais. O especialista destaca que, neste cenário, não há diferenciação entre faixa etária, uma vez que pessoas de diversas idades possuem dificuldades com o uso de tecnologias digitais e serviços como pix, ecommerce ou transferências. A pandemia, na visão do especialista, trouxe uma mudança abrupta de hábito que abriu espaço para aperfeiçoar de forma negativa as fraudes, principalmente neste período em que o dinheiro não estava mais girando na rua e sim na internet.

O especialista também destaca que o perfil dos fraudadores mudou e com isso veio o aumento da sofisticação dos ataques:

> hoje não são fraudadores perdidos e isolados no mundo digital, hoje são pessoas que estão relacionadas a crimes organizados, que giram o dinheiro de ataques e fraudes digitais para tráficos de armas e drogas, por exemplo.

Sobre um panorama frente as empresas trazidas como cases, foi abordado o questionamento das escolhas de empresas que sofrem ataques, para relacionar se

há algo em comum entre elas ou podemos justificar com aleatoriedade. Assim, o especialista trouxe um ditado próprio: “Qualquer coisa que possa ser monetizável, qualquer coisa que possa virar dinheiro, vai ser alvo de fraude.” E isso pode se relacionar com a Figura 1 demonstrada anteriormente referente ao Relatório Anual de Segurança da Informação (2021) sobre os setores mais atingidos por fraudes, tendo uma porcentagem muito maior a categoria Outros, excluindo áreas de atuação que giram bastante dinheiro como por exemplo, bancos e financeiras, ecommerce ou governo.

Foi explicado também que a razão do aumento de empresas menores estarem sendo cada mais atingidas, é porque fraudadores sabem que não há uma estrutura de segurança cuidando dessas organizações, ou seja, eles demoram muito para detectar algum tipo de ataque, e nesse meio tempo os atuantes ganham tempo para seguir retirando vantagem, com isso é explícito que qualquer empresa, independente do porte, é suscetível a ser alvo de ataque.

5.2. O caso envolvendo a empresa Finamax

A Finamax é uma empresa que atua na área de crédito, financiamento e investimento desde 1994 e faz parte de um grupo empresarial de Jundiaí (FINAMAX, 2023). No ano de 2019, a empresa cresceu significativamente aumentando suas agências abertas e automatizando o processo do crédito, conseguindo assim migrar para o mundo digital através do marketplace.

Com a migração, a marca ganhou visibilidade e começou a ser alvo de ataques cibernéticos. O caso analisado envolveu a criação de um site falso, que continham todas as informações oficiais da marca, como nome, logo e CNPJ. (AXUR, 2020a). Este tipo de fraude cria um atendimento falso ao cliente com o intuito de roubar informações pessoais ou valores financeiros.

Neste cenário, a Finamax, uma empresa tradicional que teve um crescimento digital recente bastante expressivo nos últimos anos, deparou-se com um novo desafio, que só foi descoberto após as reclamações de clientes que haviam sido prejudicados. Destaca-se que a fraude em questão gerou prejuízos financeiros e de imagem, o que demandou a procura por uma empresa especializada. Foi neste momento que a Axur deu suporte para a Finamax, a se tornar proativa e combater estes casos antes que chegassem ou atingissem seus clientes diretos (AXUR, 2020a).

Segundo o especialista da Axur, fraudes relacionadas a páginas e site falsos, que utilizam do nome e informações da marca, geram um problema reputacional inevitavelmente, porque uma reclamação ou acusação a tal empresa pode viralizar rapidamente, mesmo que ela não tenha culpa direta, mas podendo ser relacionada ao incidente sofrido ao consumidor. Outro problema relatado, é a perda financeira, visto que estes sites falsos podem estar sendo utilizados para Phishing.

> *Phishing* são ameaças virtuais, também chamadas de crimes cibernéticos, onde pessoas mal intencionadas aproveitam oportunidades para tirar proveito de outras pessoas na internet (HOSTINGER BRASIL, 2023).

O especialista ainda dividiu alguns tipos de uso do Phishing em: coletar dados financeiros e de cartões de crédito, coletar dados cadastrais e coleta de credenciais, porém o passo após o roubo dessas informações seguem maneiras diferentes.

Explicou que o roubo de informações financeiras e de cartão são utilizados para venda em fóruns ou uso próprio do fraudador, os dados cadastrais são aplicados em abertura de contas, cadastros em sites fakes ou também para extorsão da vítimas e por último ele aborda sobre o roubo de credenciais que acabam sendo usadas para invadir sistemas computacionais de certa empresa, pensando mais corporativo ou ela pode ser vinculada a uma rede social e, nesse caso, se utiliza de publicações com conteúdos falsos, mas que mesmo pouco tempo ativa, pode causar um impacto muito grande.

Ainda segundo HOSTINGER BRASIL (2023) esse tipo de crime acontece por diversos meios, mas em comum, todos possuem algo atrativo para alcançar a vítima. São utilizados: SMS, email, ligações, sites falsos e falsos pop-ups inseridos em sites desprotegidos, onde utilizam do nome de marcas para obter informações sigilosas dos usuários. Além disso, importante frisar que em 2022 o Brasil foi líder latinoamericano nos ataques de phishing, crescendo um total de 10% em relação a 2021 (COUTINHO, 2022).

A empresa Finamax, após um trabalho em conjunto com a Axur iniciou o monitoramento de todos os sites da rede e marca, detectando diversos casos e retirando essas informações e site do ar antes mesmo das fraudes conseguirem lesar alguém. A empresa ainda relata:

> A Finamax, antes de ter a ferramenta da Axur, ela só ficava sabendo dos golpes, a partir do momento que algum cliente que foi lesado, entrava em contato com a ouvidora ou com a central de atendimento, ou no procon e a Finamax tinha que explicar que realmente era um golpe e não tinha vínculo com a marca. Em alguns casos até recebia um processo e tinha que envolver a parte jurídica (AXUR, 2020a)

Segundo o especialista, a solução utilizada para o caso em questão foi a plataforma Axur One, que monitora todos os sites da rede, a marca da Finamax e CNPJ e entrega a lista de sites encontrados de forma automatizada, agilizando o processo da empresa de avaliação para solicitação da derrubada desse conteúdo do ar, antes que alguém seja lesado. Com isso, ajudou a marca em relação a seu cliente, aumentando a confiança e segurança e também conseguiu ter uma ampliação do alcance de clientes, visto que agora teriam disponíveis apenas os sites verdadeiros. Assim, podemos ter um resultado mensurado em cima da redução de custos, após setores não precisarem alocar seu tempo atuando nessas defesas e processos, se tornando essencial para Finamax, contar com essa automatização de proteção digital e combate à fraude, visando proteção a seus clientes e a própria marca.

5.3 Casos envolvendo a empresa Polar

A Polar é uma empresa Finlandesa, que atua no mercado de relógios esportivos com GPS e monitoramento de frequência cardíaca em um mercado B2C e B2B. Por atuarem bastante no *e-commerce* e terem grande renome no mercado, acabaram tornando-se mais uma marca visada por fraudadores onlines.

Sua maior dor era relacionada a anúncios falsos de produtos, ou seja, era uma divulgação mentirosa relacionada a seus produtos, mesmo que originais, utilizavam de meio ilegais e não autorizados da marca Polar para efetuar a venda. A empresa identificou essa fraude em diversos sites, como por exemplo: Mercado Livre, Enjoei, OLX, entre outros (AXUR, 2020b). Outro ponto importante é que nem sempre esse tipo de fraude está relacionada a um produto falso, mas também a um tipo de venda não autorizada legalmente, e foi esse problema enfrentado pela marca.

O desafio da Polar era conseguir derrubar todos os contrabandistas e revendedores ilegais que adquiriam o produto fora do país e decidiam vender eles em alguma plataforma do Brasil de forma ilegal. Segundo depoimento da Polar, estes

casos eram descobertos no momento que o cliente entrava em contato para tentar usufruir dos serviços da garantia, o que gerara uma grande frustação neste contato entre consumidor e empresa (AXUR, 2020b).

O especialista da Axur entrevistado ainda trouxe outros panoramas que podemos associar nesse tipo de fraude:

> No caso da Polar, foi apenas página falsa, eles não tiveram perda de estoque. Mas vamos supor que partiu de um Phishing e eles (fraudadores) conseguiram fazer compras no site da Polar com cartão de terceiro e mandar isso para outro endereço. Aí você tem alguns outros problemas: perda de estoque, perda financeira, porque você não vai receber essa grana que alguém pagou e dependendo do volume de fraude que você tem, a bandeira do cartão ela aplica uma multa no estabelecimento.

E completando a visão do especialista, ele menciona que assim o prejuízo da marca pode ser exponencial, onde se perde o produto, perde o valor, pode existir uma multa por parte da bandeira, além de problemas legais. Por isso, nesse *case* com um ecommerce ilegal, novamente se nota um prejuízo financeiro e reputacional.

A atuação da Axur então foi essencial para a marca ter impactos positivos e resultados mensurados. Foram evidenciados e mapeados logo no início do monitoramento mais de 6 mil anúncios online, e segundo depoimento da Polar (AXUR, 2020b), o resultado após esse mapeamento nas vendas de *e-commerce* foi imediato. Ainda afirmaram que estimaram através do número de anúncios derrubados um aumento de receita no *e-commerce* próprio de aproximadamente 20 a 30%. Esse resultado se explica pois a ação da Axur era derrubar esses anúncios ilegais que estavam relacionados à marca antes mesmo do consumidor encontrar eles na internet, fazendo com que sempre comprassem os produtos através do site oficial da marca ou site de revendedoras autorizadas.

Ademais, a contratação da Axur gerou também um impacto positivo na experiência do consumidor com a marca Polar ligado a confiança e também pela visão de revendedores tal parceria entrega bastante valor, porque assim ele tem a certeza de que quando o cliente for efetuar a compra online, ele não vai ter problema nenhum no final, pois tudo que está ativo na internet são realmente revendedores oficiais. Assim, ainda garante que a jornada do cliente, seja ela online ou offline, tenha a entrega de um produto oficial e legalmente vendido.

O maior movimento da Polar é alcançar o ecommerce como principal canal de vendas, e com isso tendendo que o serviço de demandas da Axur sobre riscos digitais tenha cada vez uma demanda maior e mais necessária. Por fim, a empresa concluiu que dentre seus prejuízos foram, o financeiro diretamente ligado a eles e também um desvio de possíveis consumidores dos canais oficiais.

A empresa Polar finalizou alertando demais empresas:

> "As marcas realmente precisam se atentar a oferecer online uma condição favorável pro consumidor ter confiança de comprar o produto de uma forma oficial, uma forma segura." (AXUR, 2020b)

5.4 Casos envolvendo o grupo Lapsus$

Lapsus$ era um grupo de cibercriminosos responsáveis por diversos ataques dentro e fora do Brasil, mirando vários setores. Dentre as empresas atingidas, o maior alvo eram grandes marcas relacionadas à tecnologia, e atuavam roubando e vazando dados de sistemas, códigos-fonte de softwares e materiais sensíveis. Alguns casos tiveram bastante notoriedade midiática como a invasão no site do Ministério da Saúde, conhecido como ConecteSUS. A empresa Axur também disponibilizou um material que fala sobre o grupo e que utiliza como forma de alerta para empresas parceiras, mas pela sensibilidade referente às invasões, as empresas não autorizam que seus nomes sejam evidenciados publicamente.

Conforme De Oliva (2021), os hackers Lapsus$ Group foram responsáveis pela invasão ao site do Ministério da Saúde no ano de 2021, tendo se apossado de 50 *terabytes* de dados. Nos casos apresentados, todos foram administrados pela empresa Axur, que atualmente atua na área de segurança digital dando suporte às empresas auxiliando na solução dos problemas de fraudes.

A Axur informa que o grupo de hackers usa uma tática conhecida como "destruição de dados", que envolve a exclusão de informações importantes em vez de criptografá-las e exigir um resgate. Essa tática é particularmente preocupante, pois significa que as empresas e organizações atacadas podem perder informações valiosas permanentemente, sem a possibilidade de recuperá-las mesmo que paguem o resgate exigido pelo grupo.

Segundo Kleina (2022), outra empresa atacada publicamente pelos cibercriminosos foi a Microsoft, sendo responsável por acessar, coletar e divulgar

informações sigilosas, embora a empresa afirme que nenhum dado pessoal ou relativo aos clientes tenha sido roubado. Neste caso é importante frisar a expertise de uma empresa grande visto que foi relatado que já havia uma investigação por parte da equipe de segurança da Microsoft antes mesmo da declaração pública do grupo Lapsus$ sobre o ataque, e inclusive tal declaração do grupo sobre a invasão, auxiliou na ação preventiva.

O portal R7 abordou em uma reportagem a forma de atuação do grupo, a qual consistiu no roubo de logins de acesso em troca financeira pelas informações. Para efetuar de fato a invasão ao sistema das empresas, eles desenvolveram técnicas capazes de burlar métodos de segurança, como por exemplo a autenticação de dois fatores. Neste caso, o fraudador emite várias solicitações de autenticidade para o dispositivo legítimo do usuário até que ele aceite a autenticação, liberando o acesso à conta. (R7 NOTÍCIAS, 2022). Mesmo que tal estratégia tenha dado certo nos roubos da Lapsus$, a autenticação de dois fatores segue sendo imprescindível para os sistemas digitais.

O especialista entrevistado informou que este grupo começou seus ataques em novembro de 2021 e ainda exemplificou algumas empresas atingidas: Ministérios da Saúde, Correios, Polícia Rodoviária Federal, Claro, além disso ficaram atuantes não somente no Brasil, mas também começaram a atacar fortemente Portugal, como por exemplo o grupo Imprensa, além de outras empresas grandes como Nvidia, Microsoft e Okta. Em meados de maio de 2022, iniciaram as primeiras apreensões dos organizadores do grupo, finalizando em agosto. Ele ainda ressalta:

> Ficou algumas pernas soltas, que eram pessoas mais operacionais deles e ficou meio no limbo. Hoje não tem, com o nome Lapsus$, não tem mais nenhuma operação ativa, isso não significa que eles estejam atuando, ou fizeram rebranding do grupo para outro nome.

5.5 Prevenções e estratégias

Os cenários apresentados até aqui demonstram vulnerabilidade e por vezes falta ou pouca capacidade de conhecimento para prevenção e estratégia dentro das empresas frente a ataques e fraudes. Neste ponto o especialista traz de sua expertise e experiência no assunto para nortear sobre investigações, planos de emergência e pesquisas de relação de fraudes no mercado como um todo.

> Integrando com uma parte mais investigatória frente aos casos é sempre iniciar identificando o modelo de negócio da fraude, é por ele que é possível o tipo de comportamento do atuante e de fato gerar insights em busca do desenho de estratégia investigatória, procurando um norte sobre casos que já podem ter sido mapeadas anteriormente com um mesmo *threat actor* ou reconhecer estar lidando com algo desconhecido.

Por isso, é importante que as empresas adotem práticas de prevenção e conhecimento sobre mercado.

O especialista compartilhou uma opinião sucinta sobre uma primeira estratégia que deveria ser adotada para início de prevenção:

> São algumas análises que as instituições podem fazer que não envolvem cyber, nem Threat Intelligence, mas sim de conhecimento de negócio para tentar gerar alertas e identificar uma possível fraude. Esses comportamentos querem dizer que são fraudes? Não, mas são comportamentos anômalos, são comportamentos de risco, então são algumas que as instituições podem fazer hoje do lado delas.

Ele ainda expõe que compartilhar conhecimento é expor a fraude, mas muitas empresas acham que possa ser exposição de estratégia ou risco para seu negócio e é este meio de campo que empresas especializadas em CTI fazem, recorrendo a troca de informações entre empresas de forma mais delicada mas entregando conhecimento de ataques e fraudes do mercado para os times das organizações.

Sob uma sobre o despreparo de empresas, de acordo com a entrevista, podemos constatar que muitos estabelecimentos acabam focando no que são atingidas diariamente e acabam perdendo conhecimento de inteligência de fraudes para se prevenir de novas ações contra a marca, tirando proveito sobre isso. Além disso, hoje o acesso a informações, relatórios e trabalhos são fáceis, o que deveria ser proveitoso para equipes aprenderem e criarem maior aprendizado sobre situações de cibersegurança.

Em análise, a segurança cibernética é uma responsabilidade compartilhada, por isso, é importante que todas as empresas e indivíduos assumam tais responsabilidades a sério, para proteger sistemas e dados contra possíveis ameaças. Neste mesmo contexto, o especialista ressalta a necessidade do amplo conhecimento de ataques, como também a importância de intermediar entre empresas casos.

> O que falta principalmente nas empresas é primeiro, esse conhecimento mais do que acontece no mercado, não no umbigo dela (...) O nosso papel hoje ele é muito importante em ser essa zona neutra, consigo fazer essa troca de informação entre as empresas de uma forma sanitizada, então essa é umas das vantagens.

Como forma de mitigação dessas fraudes, segundo Pinheiro (2020), existem Sistemas de Gestão de Segurança da Informação (SGSI) que auxilia no monitoramento, análise, e ainda manter e melhorar a seguranças de informações dentro das organizações, que podem impactar na baixa de fraudes diretas à empresa. Neste formato ela utiliza o modelo de maturidade do COBIT 5, dividindo em cinco níveis de maturidade.

- Maturidade nível 1 – segurança reativa / inicial

Formato da empresa responder apenas a incidentes de forma proativa, sem ter um processo padronizado para responder as evidências de incidentes. Normalmente utiliza técnicas básicas como antivírus, controle de conteúdo da web, antispam e firewall.

- Maturidade nível 2 – políticas, normas e procedimentos / repetitivo

Neste modo, há uma escalada de políticas, normas e procedimentos referentes a segurança da informação, mesmo que ainda não sejam padronizados. Podemos perceber que o entendimento atinge fatores humanos, jurídicos e processuais.

- Maturidade nível 3 – análise de risco / processos definidos

Aqui inicia a padronização dos processos, pois existe uma antecipação sobre o risco e um gerenciamento das informações. Por ter decisões entre gestores e diretoria, os procedimentos são documentados e comunicados.

- Maturidade nível 4 – gestão do risco / gerenciados e medidos

A organização demonstra maior maturidade em seus processos e lida de forma adequada com os riscos, acontecendo um acompanhamento constante para garantir

a conformidade com os procedimentos, além das ações imediatas que seriam tomadas se houvesse falha nos processos. A empresa é proativa na identificação e mitigação de possíveis ameaças.

- Maturidade nível 5 – gestão da segurança da informação / otimizado

Existe um esforço de maximizar a eficiência dos recursos destinados a área de segurança da informação, tendo assim uma proteção mais ampla. Os processos precisam ser aprimorados em busca de melhoria contínua, e para isso as empresas integram uma automatização dos fluxos de trabalho, fornecendo ferramentas que melhoram a qualidade e efetividade das operações.

Por fim, sintetizando seus conhecimentos ele explica que existe a falta de capacitação de entender fraudes digitais por parte de times de segurança, que podem trazer transtornos por exemplo em uma investigação sobre ataques e por desconhecer modos operantes, gerar um relatório equivocado não trazendo bons resultados. É nessa situação que ele frisa a importância do suporte do *Threat Intelligence*, ajudando a mapear comportamentos estratégicos para estruturar sistemas e encontrar possíveis ataques o mais cedo possível impedindo um prejuízo para organização.

Case	Fraude	Solução	Impacto
Finamax	Phishing	Derrubada de sites que estavam usando as informações da marca, como nome, CNPJ e logotipo	Prejuízo financeiro e reputacional
Polar	Venda ilegal	Derrubada de anúncios não autorizados, e vendas irregulares de todos os sites	Prejuízo financeiro e reputacional
Lapsus$	Estelionato	Investigação, além de estratégia para garantir o resgate das informações roubadas	Prejuízo financeiro e alguns casos, perda de sistema e informações originais

6. CONSIDERAÇÕES FINAIS

Como previsto, neste estudo foram relatados análises de casos de fraudes relacionadas à segurança cibernética em organizações, para esclarecer foram utilizados cases disponibilizados pela empresa de *Cyber Threat Intelligence (*Axur) e também uma visão de experiência de um especialista na área de CTI englobando cenários e percepções. Após a realização fica evidente a importância da segurança cibernética na atualidade, principalmente com o avanço constante da tecnologia e a crescente dependência das organizações em relação aos sistemas digitais, que, assim os riscos de ataques cibernéticos, se tornaram cada vez maiores e mais sofisticados.

Ao longo do trabalho também foi possível identificar a necessidade de medidas de segurança preventivas e reativas, e também a constante atualização dos sistemas e a capacitação dos profissionais envolvidos. Segundo o especialista, "falta muita capacitação do ponto de vista de entender fraudes digitais dos times", ou seja, se torna fundamental que as empresas invistam em treinamentos e conscientização dos funcionários sobre as ameaças cibernéticas e as melhores práticas de segurança. Atualmente os funcionários são frequentemente o elo mais fraco na segurança cibernética de uma empresa e ataques de *phishing* podem ser muito eficazes em comprometer sistemas e dados.

Dessa forma, é importante que as organizações estejam sempre atentas à segurança cibernética, colaborando entre as equipes de segurança, TI e gestão de risco, garantindo a proteção dos seus sistemas e dados, bem como preservar a confiança e reputação junto a seus clientes e parceiros, conforme abordado durante o trabalho tamanho prejuízo pode ser causado por confiabilidade do cliente.

Também é importante que as empresas estejam preparadas para responder a possíveis violações de segurança, tendo um plano de resposta a incidentes bem definido e testado regularmente. Atualmente, assim como a empresa Axur utilizada no projeto deste trabalho, existem outras empresas que fornecem soluções de monitoramento de riscos digitais na web superficial e deep web, auxiliando empresas a tomarem medidas ou efetuar a remoção de conteúdos fraudulentos em um período rápido, antes mesmo que cheguem aos usuários. Isso ajuda a minimizar o tempo de inatividade e o impacto de um possível ataque cibernético.

Além disso, a adoção de boas práticas, tais como o uso de senhas fortes, firewalls, criptografia de dados e backups regulares, além de monitoramento constante de possíveis atividades suspeitas em suas redes e sistemas, concluindo uma implementação de medidas de segurança bem robustas, sendo crucial para minimizar os riscos.

Por fim, qualquer meio utilizado juntamente com uma ótima conscientização e educação sobre fraudes nos times de segurança, auxiliam na avaliação constante dos riscos e vulnerabilidade, sendo essencial na ação rápida e eficiente contra os possíveis incidentes.

REFERÊNCIAS

AXUR. Como a Finamax derrubou sites falsos e evitou que clientes caíssem em golpes. [S.l.: s.n.], 14 abr. 2020a. 1 vídeo (10 min). Disponível em: https://www.youtube.com/watch?v=zrHOU5kpdEo&t=14s. Acesso em: 16 mar. 2023.

AXUR. Como a Polar conseguiu remover vendas ilegais e aumentar a receita. [S. l.], 29 jul. 2020b. 1 vídeo (14 min 14 s). Disponível em: https://www.youtube.com/watch?v=Ns_kPkcsktA&t=4s. Acesso em: 16 mar. 2023.

BARBOSA, A.; COSTA, J.; PONTES, R. Cidades Inteligentes no contexto da quarta revolução industrial. Cadernos Adenauer, Rio de Janeiro, n.1, 2020.

BARBOSA, J. S. *et al*. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. Research, Society and Development, v. 10, n. 2, 2021.

BARRA, J. Avanços tecnológicos e o futuro do trabalho. AASP, 2019. Disponível em: <https://www.aasp.org.br/em-pauta/artigo-avancos-tecnologicos-e-o-futuro-do-trabalho/>. Acesso em: 30 jul. 2022.

CORTEZ, I. S.; KUBOTA, L. C. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. Revista de Administração, São Paulo, v. 48, n. 4, p. 757-769, 2013.

COUTINHO, D. Golpe phishing no Brasil: como se proteger. IG Tecnologia, 18 nov. 2022. Disponível em: <https://tecnologia.ig.com.br/2022-11-18/golpe-phishing-brasil-como-se-proteger.html>. Acesso em: 10 mar 2023.

DE ARAUJO, F. C.; ROSSI, J. M. A evolução dos ataques cibernéticos. São Paulo: Faculdade de Tecnologia de Americana Ministro Ralph Biasi, 2020.

DE OLIVA, B. Hackers que invadiram Ministério da Saúde dizem que não venderão os dados. Jornal O Povo, 2021. Disponível em: <https://www.opovo.com.br/noticias/tecnologia/2021/12/10/hackers-que-invadiram-ministerio-da-saude-dizem-que-nao-venderao-os-dados.html>. Acesso em: 19 ago. 2022.

DEMARTINI, F. Ataques cibernéticos têm aumento de 46% no Brasil. Terra, 2022. Disponível em: <https://www.terra.com.br/byte/ataques-ciberneticos-tem-aumento-de-46-no-brasil,47c5e8bf51099c72911da901a5fb0482d8ohsz0l.html>. Acesso em: 15 set. 2022.

FIA – Fundação Instituto de Administração. Cibersegurança: o que é, importância, tipos e carreiras na área. Disponível em: <https://fia.com.br/blog/ciberseguranca/>. Acesso em: 14 ago. 2022.

FINAMAX. Sobre a Finamax. Disponível em: https://www.finamax.com.br/a-finamax/. Acesso em: 26 mar. 2023.

FIRST TECH. O Brasil na mira dos ataques cibernéticos, inclusive de ransomware. First Tech, 2021. Disponível em: <https://first-tech.com/conteudo/o-brasil-na-mira-dos-ataques-ciberneticos-inclusive-de-ransomware/#:~:text=Mais%20de%2088%20bilh%C3%B5es%20de,somente%20no%20ano%20de%202021>. Acesso em: 15 set. 2022.

FONTES, E. L. G. Segurança da Informação: O usuário faz a diferença.1. ed. São Paulo: Saraiva, 2006.

GARRETT, F. Crimes cibernéticos: entenda o que são e como denunciar. Techtudo, 2021. Disponível em: <https://www.techtudo.com.br/noticias/2021/08/crimes-ciberneticos-entenda-o-que-sao-e-como-denunciar.ghtml>. Acesso em: 8 set. de 2022.

Hostinger Brasil. O que é phishing e como se proteger de golpes na internet. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet>. Acesso em: 16 mar. 2023.

KIM, H.; KIM, H.; SHIN, D. IT security investments and customer satisfaction: Evidence from the U.S. retail banking industry. Journal of Business Research, v. 89, p. 210-220, jun. 2018

KLEINA, N.. Microsoft confirma invasão e acesso a dados por grupo Lapsus. 23 mar 2022. Disponível em: <https://www.tecmundo.com.br/seguranca/235849-microsoft-confirma-invasao-acesso-dados-grupo-lapsus.htm>. Acesso em: 10 mar 2023.

KUMAR, D.; BIDWAIK, M. S.; SINGH, S. S. Cyber Security in Organizations: A Review of Literature. Information & Management, v. 57, n. 5, 2020, p. 1-16.

MCKINSEY & COMPANY. Transformação digital: repensando o seu negócio para a era digital. São Paulo: McKinsey & Company, 2017.

NEOWAY. Segurança da informação: O que é, e seus impactos e soluções nas empresas. Blog. 2020. Disponível em: <https://blog.neoway.com.br/seguranca-da-informacao/>. Acesso em: 8 set. 2022.

NETTO, T. Segurança da Informação: Ataques Cibernéticos e Cibersegurança. Instituto de Direito Legal, 2019. Disponível em: <https://direitoreal.com.br/artigos/seguranca-da-informacao-ataques-ciberneticos-e-ciberseguranca>. Acesso em: 31 jul. 2022.

NUNES, B. P.; MARQUES, M. R. “Ciberataque” enquanto uma análise da proteção de dados pessoais na internet: Estudo de caso sobre o ataque cibernético no Hospital

de Câncer de Barretos (SP). Rio Grande do Sul: Universidade Federal de Santa Maria, 2019.

OLIVEIRA, D. Cresce em 950% no Brasil as tentativas de ataques cibernéticos. AANPD – Associação Nacional dos Profissionais de Privacidade de Dados. Santa Catarina, 2022. Disponível em: <https://anppd.org/noticia/cresce-em-950-no-brasil-as-tentativas-de-ataques-ciberneticos-14-04-2022>. Acesso em: 31 jul. 2022.

OSTEC. Conheça as táticas, técnicas e procedimentos dos atacantes (TTPs) Disponível em: <https://ostec.blog/geral/conheca-taticas-tecnicas-procedimentos-atacantes-ttps/#:~:text=Os%20TTPs%20descrevem%20como%20os,e%20n%C3%A3o%20tanto%20nas%20ferramentas>. Acesso em: 11 mar. 2023.

PINHEIRO, Patricia P. Segurança Digital - Proteção de Dados nas Empresas. São Paulo: Grupo GEN, 2020. E-book. ISBN 9788597026405. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 08 abr. 2023.

PINTO, D. J. A.; GRASSI, J. M. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. Revista Brasileira de Estudos de Defesa, v. 7, n. 2, 2020.

POSESA. Crimes digitais: leis aplicáveis. Disponível em: <https://posesa.com.br/crimes-digitais-leis-aplicaveis/>.Acesso em: 11 set. 2022.

R7 NOTÍCIAS. Quem é e como age o Lapsus, o grupo que invadiu algumas das maiores empresas do mundo. R7 Tecnologia e Ciência, 29 mar. 2022. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/quem-e-e-como-age-o-lapsus-o-grupo-que-invadiu-algumas-das-maiores-empresas-do-mundo-29032022. Acesso em: 21 nov. 2022.

RNP – Rede brasileira para educação e pesquisa. Relatório Anual de Segurança 2021. Disponível em: https://www.rnp.br/noticias/confira-o-relatorio-anual-de-seguranca-de-2021>; Acesso em 31 jul 2022.

ROGERS, D. L. Transformação Digital: repensando o seu negócio para a era digital. São Paulo: Autêntica Business, 2018.

SANTOS, G. C. Entrevista: Técnica de coleta em pesquisa qualitativa. Portal De Periódicos Eletrônicos Científicos Da Unicamp (Blog), v. 8, n. 1, 2018. Disponível em: < https://periodicos.sbu.unicamp.br/blog/index.php/2018/08/15/entrevista/>. Acesso em: 6 de out. de 2022.

SÁ-SILVA, J. R.; ALMEIDA, C. D. de; GUINDANI, J. F. Pesquisa documental: pistas teóricas e metodológicas. Revista Brasileira de História & Ciências Sociais, *[S. l.]*, v. 1, n. 1, 2009.

SCHENDES, W. Ataques cibernéticos no Brasil cresceram 46% no segundo trimestre. Olhar Digital, 2022. Disponível em: <https://olhardigital.com.br/2022/08/09/seguranca/ataques-ciberneticos-brasil-cresce-46/>. Acesso em: 8 de set. de 2022.

SOFTWALL. Vazamento de dados e suas consequências para empresas. Blog. 2019. Disponível em: <https://www.softwall.com.br/blog/vazamento-de-dados-e-suas-consequencias-para-empresas/>. Acesso em: 10 set. 2022.

Target Real Estate. O avanço da tecnologia e a vulnerabilidade de segurança. 22 jan. 2020. Disponível em: <https://blog.targetrealestate.com.br/mercado-corporativo/o-avanco-da-tecnologia-e-a-vulnerabilidade-de-seguranca/>. Acesso em: 31 jul. 2022.

APÊNDICE 1 – QUESTIONÁRIO PARA A ENTREVISTA

1. Como é a experiência de estar no mercado atuando nessa área e vendo o aumento de demanda de incidentes digitais?
2. Acredita que tal aumento é reflexo da pandemia?
3. Dentro do case da Finamax, qual foi a razão para acontecer o ataque?
4. No case da Polar, qual foi a razão para acontecer o ataque?
5. No case da Laps$us, qual foi a razão para acontecer o ataque? Esse grupo de hackers é bem atuante no Brasil nos últimos ano. Existe a possibilidade de bloquearmos esse tipo de atuantes?
6. Acha que elas tiveram algo em comum para serem visadas para um ataque?
7. As medidas para solucionar cada caso foi diferente? Como se avalia as medidas que devem ser tomadas em cada caso?
8. Quais estratégias as empresas deveriam sempre adotar para se prevenir desses tipos de ataque?
9. Dentro do cenário atual, acredita que as empresas ainda sejam muito despreparadas para encontrar estratégias de prevenção a fraudes?

APÊNDICE 2 – RESPOSTAS DO ENTREVISTADO

1. Como é a experiência de estar no mercado atuando nessa área e vendo o aumento de demanda de incidentes digitais?

Estar na linha de frente é bastante desafiador, ainda mais numa situação onde a gente atua com múltiplos clientes, então eu tenho que entender de diversos modelos de fraudes, de diversos modelos de negócios e isso dificulta bastante e complica também né, cria uma complexidade bastante grande pra gente, pra conseguir montar uma estratégia que faça sentido pra defesa do cliente. E em contrapartida, isso gera uma expertise bastante significativo pra gente porque, por vezes as fraudes elas migram de setor, ou elas migram de empresa, mas tipo o comportamento dela permanece. Ou seja, a gente percebe que o atacante, ele não para de fazer a fraude quando o cliente bloqueia aquilo, ele vai pro vizinho e vai fazendo ataque no vizinho e ai o vizinho bloqueia, e ele vai para o outro vizinho, ele não vai deixar de parar, ele só para de fazer isso quando ele é preso. Então assim, o fraudador ele não para, ele da um tempo, é o que acaba acontecendo. E esse é o grande desafio que a gente tem, entender principalmente como que esses fraudadores tão burlando não só sistemas, mas as vezes o processo da fraude ele ocorre por uma falha no processo de negócio, não é nem uma falha técnica, por vezes. Também são uns dos grandes desafios que a gente tem, de entender esse comportamento do atacante né que eu tenho tipo de um TTP (técnica do plano), táticas, técnicas e procedimentos ou modos operantes para que a gente atue na causa raiz, então assim, não é que o fraudador ta fazendo por exemplo uma compra com cartão de terceiro no ecommerce, por exemplo, a resposta que eu tenho que dar pro cliente é como que um atacante consegue utilizar o cartão de um terceiro no ecommerce, porque dai eu elimino a fraude não de um cartão, mas de todo o ecossistema. O nosso trabalho, ele consiste principalmente em entender isso, tirar de um caso individual e levar para um visão que isso possa ser replicado pra atuar em diversos outros casos. Quando a gente liga isso pro cliente, com o lado do cliente, da uma sinergia bastante significativa e esse é um dos grandes diferencias que os clientes estão vendo, como aproveitar esse lado de investigação que a gente tem, junto com os times internos pra conseguir responder algumas perguntas que ele não tem visibilidade, o cliente tem visibilidade do que ta da porta dele pra dentro e a gente tem visibilidade do que ta da porte dele pra fora, então quando a gente conecta esses dois mundos a gente consegue entender fim a fim o ciclo de uma fraude e é isso onde as empresas estão enxergando bastante valor hoje e tão debruçando os esforços.

2. Acredita que tal aumento é reflexo da pandemia? Com talvez um aumento de digitalização das empresas?

Pra mim, o maior reflexo não é porque as empresas digitalizaram, mas a gente teve uma adoção massiva de serviços digitais por pessoas que não estavam digitalmente incluídas, por exemplo, meus pai tiveram que aprender a usar a internet dentro, tiveram que aprender a usar o

ecommerce, tiveram que aprender a fazer o pix, a fazer transferências, tudo pelo computador ou pelo celular, e boa parte dessa população que foi digitalmente incluida ali, "a força" digamos assim por causa da pandemia, é um dos grandes alvos que eles tem. Então, não necessariamente pessoas de mais idade ta? a gente tem pessoas na casa dos 30, 40 anos que não tinham um hábito de usar serviços onlines, vejo por mim, quando eu ia comprar uma roupa um tenis, eu gosto de ir na loja, provar roupa, ver, mas hoje pra mim é muito natural entrar no site, escolher uma camiseta e comprar, então assim, mudou um hábito de consumo também. Então não é uma questão de faixa etária, mas sim de comportamento, tu não estava acostumado a fazer isso e agora tem que fazer e consequentemente os fraudadores foram pro Home Office também, não tinha dinheiro na rua, não tinha loja aberto, não tinha banco aberto, o dinheiro tava todo na internet e foi pra ai que eles foram. Hoje, quando a gente fala de fraude digital principalmente, a gente não ta mais falando que é um lobo solitário ali, um fraudador isolado que faz um ataque ou uma fraudezinha, hoje a gente tem crime organizado por trás, essa grana financia tráfico de drogas, tráfico de armas e outros problemas que a gente tem maiores, inclusive.

3. Dentro do case da Finamax, qual foi a razão para acontecer o ataque? E quais malefícios trouxe?

O primeiro deles é o problema reputacional, inevitavelmente você tem um problema reputacional que é um item a ser tratado, um outro é a questão de perda de market share, e tem a questão da perda financeira né que pode ocorrer. Existe hoje uma questão de (...) que é importante também, que é uma questão de risco legal de você ter que usar por exemplo uma fintech ser usada para lavar dinheiro, existe uma regulamentação muito forte hoje junto ao Banco Central para que as empresas façam todas as medidas possíveis e cabíveis para evitar uma lavagem de dinheiro. Na prática, um laranja, ele tá lavando o meu dinheiro. Sobre o Phishing, você tem dois caminhos né, você tem um modelo que vai ser um phishing para, por exemplo, coletar dados de cartão de crédito ou dados financeiros, você tem um modelo de phishing para coleta de dados cadastrais, você tem um modelo phishing pra coleta de credenciais. Cada um desses caras o próximo step é diferente, então por exemplo, o phishing que tem como foco coleta de cartão, o próximo step é vender esse cartão em fóruns ou utilizar esse cartão para benefício próprio, então fraude. Quando a gente fala de dados cadastral, ai isso abre um outro leque, pode ir pra por exemplo uma abertura de conta no seu nome, pode ir pra um cadastro em um site fake, pode ser pra usar essa informação para te extorquir depois, então tem algumas possibilidades. A de credenciais abre um leque maior ainda, você pode ir até para um lado corporativo, de permitir uma invasão ao sistema computacional de uma empresa que entra, por exemplo, a questão do Lapsus$, eles usavam coletas de credenciais corporativas para fazer os ataques as vítimas deles, então tem várias possibilidades. Esses são os principais problemas que a gente tem, isso pode ir pra uma questão legal, por exemplo, o meu dado foi vazado ou alguém conseguiu o meu login e senha de algum site qualquer, da minha concessionária de energia, conseguiu o login de la, o que o cara consegue fazer com isso? nada, mas ele tem consegue ver todos os teus dados cadastrais e a partir dali ele pode

mandar um phishing se passando pela empresa ou fazer usar isso para fazer outros tipos de de golpe, então não teve um vazamento de dados da empresa propriamente dito, foi uma falha no processo de autenticação né, e ai o usuário final que indiretamente permitiu que com o login dele fosse visualizado esses dados, então é uma possibilidade também que a gente tem e ai a LPD pode pegar um pouco em cima disso. Tem diversas possibilidades ali.

4. No case da Polar, qual foi a razão para acontecer o ataque?

No caso da Polar, o que pode acontecer é por exemplo, se foi só página falsa, eles não tiveram por exemplo, perda de estoque, mas se teve um phishing e os caras conseguiram fazer compras no site da Polar com cartão de terceiro e mandar isso pra outro endereço, ai você tem alguns outros problemas, porque você tem a perda de estoque, você tem perda financeira, porque você não vai receber essa grana que alguém pagou ali, dependendo do volume de fraude que você tem, a bandeira do cartão ela aplica uma multa no estabelecimento. Então assim, se você começa a ter muitos casos de fraude, muita contestação de compra que é o que a gente chama de *chargeback,* a bandeira do cartão ela coloco uma multa pra você pagar em cima das movimentações, então o seu prejuízo pode ser exponenciado ali. Você perdeu o produto, você perdeu a grana porque você vai ter que devolver esse dinheiro e nessa devolução você ainda pode ter uma multa por parte da bandeira, fora os problemas legais, de reputação e tudo mais. Mas se foi só a pagina falsa para coleta de dados, pode até ter sido um ecommerce fake que não entrega nem nada, segue o mesmo modo operante de Finamax.

5. No case da Laps$us, qual foi a razão para acontecer o ataque? Esse grupo de hackers é bem atuante no Brasil nos últimos ano. Existe a possibilidade de bloquearmos esse tipo de atuantes?

Na verdade eles foram, porque foi desmantelado o grupo. Eles fizeram uns ataques, ele começaram os ataques em novembro de 2021 no Ministério da Saúde, Correios, Polícia Rodoviária Federal, ai fizeram a Claro na semana entre Natal e Ano Novo, e ai eles ficaram atuantes assim em diversos outros clientes, não só no Brasil porque eles começaram a atacar Portugal muito forte, eles pegaram o grupo Imprensa, que é como se fosse a Globo daqui, um grupo muito grande la. Eles pegam big companys, eles pegaram a Nvidia, a Microsoft, pegaram Okta e ai putz, ai o negócio escalou pra FBI, foram construindo olhos pra cima. E ai, quando foi em meados de abril e maio de 2022, eles prenderam uma galera no Reino Unido, na semana seguinte prenderam um dos cabeças do grupo também no Reino Unido e passo algum tempinho, umas duas semanas, eles prenderam um brasileiro que era outro cabeça também e em meados de julho pra agosto, eles prenderam um outro cabeça também brasileiro. Então assim, a organização criminosa era composta por dois brasileiros, uma pessoa do Reino Unido, todos super jovens. Mas ficou algumas pernas soltas, que

eram pessoas mais operacionais deles e ficou meio no limbo. Hoje não tem, com o nome Lapsus$, não tem mais nenhuma operação ativa, isso não significa que eles não estejam atuando, ou fizeram rebranding do grupo para outro nome, mas essas pessoas seguem presas.

6. Acha que elas tiveram algo em comum para serem visadas para um ataque?

Eu tenho um ditado que diz o seguinte, qualquer coisa que possa ser monetizavel, qualquer coisa que possa virar dinheiro, vai ser alvo de fraude. Eu fui a pouco no mercadinho de bairro, uma portinha de garagem e tava assim: “não aceitamos mais pix pelo celular, somente pelo QRCode da maquininha”, ai perguntei por que né? E ai a atendente ela falou que eles estavam tendo muita fraude da pessoa simular que fazia o pix, mostrava um comprovante falso e mandava, isso em um mercadinho de esquina. Pode ser algo de milhares de reais, mas pode ser uma coisa pequena, então não é porque eu tenho uma quitandinha que eu não preciso. A gente ta com um caso agora de um malware que eu já acompanho ele a bastante tempo, que é o Prilex, um malware brasileiro que bloqueia transação por aproximação. O principal alvo desse malware, quando eles começaram eram grandes estabelecimentos então eles iam sempre pra grandes redes de supermercado, lojas de varejo, material de construção, hoje o negócio deles é tipo, padaria, restaurante, por que? Esses caras não tem um time de segurança, esses caras usam Windows pirata sem antivírus, ou quem cuida da rede é o primo do vizinho do conhecido do amigo, até detectar o ataque ali, já foi.. independente de uma padaria ou um restaurante, gira muita grana no dia, você movimenta muito durante o dia, não em valor de transação. Se eles irem pra um modelo onde o ticket médio passa de R$300,00 ou R$ 400,00, eles vão pra um modelo onde eles vão fazer muito mais com ticket médio de R$ 20,00 ou R$ 30,00. Hoje, qualquer empresa ela pode ser alvo de ataque nesse sentido.

7. As medidas para solucionar cada caso foi diferente? Como se avalia as medidas que devem ser tomadas em cada caso?

O primeiro passo é, tem dois cenários, um é o cenário mais simples que a gente atua que o cliente só quer uma sondagem ali pra entender o que o cara quer, não chega nem em cima de ser uma investigação profunda, mas tem casos de investigações mais profundas. Vou pegar o caso dessas investigações mais profundas, porque normalmente é onde ta a maior quantidade de valor, são casos mais interessantes. Nesses casos, em geral, o primeiro passo nosso é antes de entender o que buscar, a resolução, de tentar entender o que ta acontecendo, a gente tem que entender qual é o modelo de negócio. Ah eu quero comprar um produto, vamos supor que seja uma fraude no ecommerce, ah ele faz assim, clica aqui ou la, e o que a gente tem detectado de fraude é que o cara usa, esse tipo de comportamento, então ta, a partir dali a gente já começa a gerar alguns insights pro cliente: olha, você consegue ter visibilidade desse tipo de informação, você já correlacionou internamente essa informação com aquela? Você tem condições de monitorar se eu fizer isso externamente?

E ai nessa conversa com o cliente a gente vai desenhando nossa estratégia investigativa, que pode ser algo que a gente já tenha mapeado na nossa estrutura, um threat actor que a gente já detectou e já ta mapeado ali, é só infiltrar e contatar ele ou pode ser algo totalmente desconhecido. Cada caso é um caso.

8. Quais estratégias as empresas deveriam sempre adotar para se prevenir desses tipos de ataque?

Eu acho que algumas coisas daria pra se fazer com bastante facilidade e nem envolve questões relacionadas a segurança cibernética, assim a entendimento financeiro, então por exemplo, um caso de uma instituição financeira. Quando você instala um aplicativo do banco, o aplicativo ou uma parte deles hoje, cria uma assinatura do seu dispositivo do seu celular, por isso que ela detecta que você ta acessando a conta de outro celular e pede normalmente um recadastramento, não faz sentido uma pessoa, um celular por exemplo, tentar acesso a mais do que duas contas correntes, quem tem mais de duas contas correntes no mesmo banco? Acessando do mesmo dispositivo você pode ter, tipo você, seu esposo, seu filho, todos no mesmo banco mas cada um com seu celular ou por exemplo, eu tenho conta pessoa jurídica e pessoa física no mesmo banco então acesso os dois pelo meu celular, mas dificilmente eu tenho três contas. Então, eu tenho três acessos oriundos do mesmo dispositivo e três contas diferentes, é um alerta, esse número de telefone que ta fazendo cadastro comigo, já foi informado anteriormente que foi fraude por algum outro caso? De repente eu mapeie um cadastro falso no nome W com o dispositivo X e um CPF Y, e um número de telefone, eu posso trocar de celular e tentar fazer o mesmo cadastro com aqueles mesmos dados, existe uma revalidação? Não existe? As movimentações, putz o cara acabou de entrar e já começa a movimentar muita grana, é algo muito suspeito, então assim normalmente ele criou a conta, ele vai começar a receber pingadinho, depois que você tem uma movimentação mais significativa. Um outro comportamento de conta laranja, é o dinheiro entrar e já sair, então assim, entra R$ 1.000,00 e sai R$ 1.000,00, então sempre sai na mesma quantidade que entra, obvio que é uma conta transitória ali, então são algumas análises que as instituições podem fazer que não envolvem cyber, não envolvem threat intelligence, mas sim de conhecimento de negócio para tentar gerar alertas e identificar uma possível fraude. Esses comportamentos quer dizer que são fraudes? Não, mas são comportamentos anômalos, são comportamentos de risco, então são algumas coisas que as instituições podem fazer hoje do lado delas, e a gente por exemplo, fornece a lista de telefones que fazem parte de grupos de whatsapp que a gente monitora, e a gente só monitora grupo lixo, a gente não monitora grupo de conteúdo sem ser de fraude, então se eu tenho um cadastro sendo realizado na minha instituição financeira e o número de telefone faz parte de um dos grupos que a gente monitora, concorda que minimamente é um cadastro de risco? Por mais que o cara esteja abrindo a conta pra ele mesmo, não vai ter nenhuma operação ilícita ali, tudo bonitinho, mas pode minimamente ser um número de risco pra mim. Então eu posso não liberar um limite alto pro cara logo de cara, não vou abrir um limite de transação muito grande, não vou dar cheque especial,

vou segurar um pouco o volume transacional de pix, deixar rodar um tempo e depois você vai froxando e analisando ao longo do período. Então assim, o que falta, principalmente nas empresas, é primeiro esse conhecimento mais do que acontece no mercado, não no umbigo dela. Todo mundo olha bem o seu feudo, não olha o vizinho e a gente ta em um momento que assim, se não tiver essa troca de informação é insustentável, porque é todo mundo batendo cabeça no mesmo caso. Compartilhar conhecimento, por vezes não expõe estratégia de negócio, não expõe risco para o negócio, mas sim de fraude. O nosso papel hoje é muito importante em ser essa zona neutra, eu consigo fazer essa troca de informação entre as empresas de uma forma sanitizada, então essa é uma das vantagens que a gente tem ali e eu acho que é isso que falta um pouco para as empresas hoje.

9. Dentro do cenário atual, acredita que as empresas ainda sejam muito despreparadas para encontrar estratégias de prevenção a fraudes?

Sim, porque muitas delas não tem o mindsite de ter essa visão externa, então se ela não conhece o que ta rolando fora. Então, quais são os modelos de fraude que o setor delas sofrem? ela não conhece, ela conhece o que ela sofre e por vezes o vizinho ta sofrendo de um problema que ela não tem conhecimento. Hoje elas estavam despreparadas porque ela não tiram proveito desse conhecimento de inteligência, então hoje eu consigo pegar exemplo de fraude que a gente fez do Reboleto, que está público, que é um aplicativo pra fazer fraude em boletos. Nós produzimos esse relatório em 2021 e até hoje em 2023 esse programa é distribuído e as empresas ainda continuam sofrendo com esse problema. E é um problema que ataca quem? qualquer empresa que trabalha com boleto, seja ela emissora ou pagadora de boleto. Então você tem os dois lados ali, uma empresa que ela é vítima dos dois lados seja pagando ou recebendo, ou emitindo um boleto ou pagando, porque muitas empresas desconhecem que existe esse tipo de ataque numa investigação e às vezes até investigadores desconhecem esse modus operante e ai em uma investigação pode inclusive produzir um relatório equivocado pela técnica que é utilizada. Um outro ponto, é que falta muita capacitação do ponto de vista de entender fraudes digitais dos times. Ontem eu tava dando aula na pós graduação e ai um dos alunos falou assim: "Ah, a gente tá implementando sistema de biometria na empresa para abrir a conta agora, o aplicativo pede um vídeo aleatório da pessoa, fazendo movimento por exemplo para o lado e ai não tem como o cara colocar um vídeo ali, fazer o streaming de um vídeo fake né? que é o que acontece com o que a gente chama de burlador." e eu respondi, engano seu, porque quando o atacante hoje compra uma conta laranja, ele ja compra o kit completo, ele compra o laranja fazendo assim, o laranja piscando, afastando e aproximando o celular, segurando o RG, segurando a CNH, ele ja compra esse kit pronto e se o seu aplicativo pedir pro usuário fazer um sinal de sim com a cabeça, o cara vai injetar esse vídeo do laranja fazendo sim e vai entrar. Mostrei no meu celular em alguns grupos o vídeo do cara fazendo isso, porque eles vendem esses esquemas. E é ai que entra o nosso papel de Threat Intelligence, entender e mapear esses comportamentos estratégicos para

antecipar ao máximo eles e se blindar para que não ocorra na estrutura e detectar esses comportamentos no menor tempo possível.