CIBERSEGURANÇA E DIRETO MERCANTIL: LIÇÕES DO ATAQUE HACKER À UBER

Cybersecurity and Commercial Law: Lessons from the Uber Hacker Attack

Italo Rosendo Oliveira da Silva[1]
Pitágoras Unopar Anhanguera

Monique de Souza Arruda[2]
Universidade Católica Portuguesa – Porto

DOI: https://doi.org//10.62140/ISMA132024

Sumário: Introdução; 1 Uber: uma plataforma digital de trabalho; 2 Ataques e vulnerabilidades: a cibersegurança em ação; 3 Estudo de caso; 4 Implicações jurídicas decorrentes do ataque hacker à Uber; 5 Análise técnica em cibersegurança no que tange ataques cibernéticos às plataformas digitais; Conclusão.

Resumo: O presente artigo aborda a problemática da cibersegurança em plataformas digitais de trabalho, com foco no ataque hacker à Uber em 15 de setembro de 2022, que comprometeu a integridade e confidencialidade dos dados dos usuários e expôs falhas críticas na infraestrutura de segurança da empresa. O objetivo da investigação é analisar as vulnerabilidades exploradas no ataque, os métodos de mitigação adotados e as lições aprendidas, destacando a importância de uma abordagem interdisciplinar que combine cibersegurança e Direito Mercantil. A metodologia utilizada é qualitativa e exploratória, com revisão de fontes secundárias, incluindo artigos de jornais, relatórios de segurança e literatura acadêmica. A análise concentrou-se nas técnicas de engenharia social utilizadas pelos hackers, nas vulnerabilidades técnicas exploradas e nas respostas institucionais da Uber. O estudo conclui que a segurança da informação deve ser uma prioridade estratégica para todas as empresas, especialmente as do setor tecnológico. Recomenda-se a implementação de uma abordagem abrangente de cibersegurança que inclua sistemas de autenticação robustos, criptografia de dados, monitoramento contínuo e testes regulares de penetração para proteger informações sensíveis e garantir a continuidade das operações.
Palavras-chave: Cibersegurança; Plataformas Digitais de Trabalho; Ataque hacker; Proteção de dados; Tecnologias de Informação.

Abstract: This article addresses the issue of cybersecurity in digital work platforms, focusing on the hacker attack on Uber on September 15, 2022, which compromised the integrity and confidentiality of user data and exposed critical flaws in the company's security infrastructure. The investigation aims to analyze the vulnerabilities exploited in the attack, the mitigation methods adopted, and the lessons learned, emphasizing the importance of an interdisciplinary approach that combines cybersecurity and Commercial Law. The methodology used is qualitative and exploratory, involving a review of secondary sources, including newspaper articles, security reports, and academic literature. The analysis focused on the social engineering techniques used by the hackers, the technical vulnerabilities exploited, and Uber's institutional responses. The study

[1] Universidade Pitágoras Unopar Anhanguera-Rio de janeiro, Faculdade de tecnologia. Bacharel em cibersegurança. italorosendoo@gmail.com
[2] Universidade Católica Portuguesa - Porto, Faculdade de Direito. Doutoranda em Direito e Mestre em Direito Ambiental. s-msarruda@ucp.pt.

concludes that information security should be a strategic priority for all companies, especially those in the technology sector. It recommends implementing a comprehensive cybersecurity approach that includes robust authentication systems, data encryption, continuous monitoring, and regular penetration testing to protect sensitive information and ensure business continuity.

Keywords: Cybersecurity; Digital Work Platforms; Hacker Attack; Data Protection; Information Technologies.

Introdução

Com o aumento do uso de plataformas digitais de trabalho, a segurança cibernética tornou-se uma preocupação essencial. Essas plataformas armazenam uma quantidade significativa de dados pessoais e empresariais sensíveis e são, portanto, alvos apelativos para cibercriminosos. No dia 15 de setembro de 2022, a empresa Uber, uma conhecida plataforma digital de trabalho, foi alvo de um ataque informático por parte de um hacker que comprometeu a integridade e a confidencialidade dos dados dos usuários.

As plataformas digitais de trabalho, assim como qualquer empresa tradicional ou totalmente alocada a ambientes digitais, podem ser alvo deste tipo de *hacking*, na medida em que esses indivíduos atuam diariamente na procura de brechas ao nível de segurança da informação, para explorar vulnerabilidades e obter acesso não autorizado a informações pessoais sensíveis ou confidenciais.

Ocorre que, quando um negócio inserido nesse nicho digital se inicia e desenvolve as suas operações, nem sempre vislumbra o nível de segurança cibernética minimamente necessário. Muitas vezes, são negligenciadas não apenas as medidas básicas, como o uso de senhas fortes, mas também a implementação de sistemas de autenticação multifator, monitoramento contínuo, auditorias regulares, e, crucialmente, a formação e treinamento adequados dos colaboradores.

Neste âmbito, o presente estudo examina o ataque informático à plataforma digital Uber, com especial enfoque nos detalhes da invasão, buscando evidenciar as fragilidades exploradas pelo cibercriminoso e identificar como a própria plataforma poderia ter adotado medidas preventivas para evitar ser alvo desse ataque. Na primeira parte da pesquisa, é realizada uma contextualização do modelo de negócios da Uber, seguida de uma análise sobre a importância da cibersegurança como um elemento essencial em um cenário de crescente digitalização dos negócios e adoção de ferramentas de inteligência artificial para aumentar a produtividade e reduzir custos.

Na segunda parte, o estudo apresenta o caso específico do ataque à Uber, refletindo sobre as vulnerabilidades exploradas, as ações dos hackers e as reações dos recursos humanos diante de possíveis ameaças maliciosas, além de outros aspectos relevantes. O objetivo do estudo é identificar

as vulnerabilidades que foram exploradas e fornecer recomendações para prevenir ataques futuros, aplicáveis não apenas a plataformas digitais de trabalho, mas também a instituições públicas e privadas em geral.

1. Uber: uma plataforma digital de trabalho

A Uber Technologies, Inc. é uma empresa de tecnologia que desenvolve e opera aplicativos para oferecer uma ampla gama de serviços por meio de sua plataforma digital. Entre seus principais serviços, destaca-se a conexão de consumidores (passageiros) com prestadores independentes de serviços de transporte (motoristas), proporcionando serviços de caronas compartilhadas. Além disso, a Uber conecta consumidores a restaurantes, mercados e outras lojas através de entregadores (couriers), facilitando a entrega de refeições, compras de supermercado e outros produtos. A empresa também integra redes de transporte público e atua no setor de expedição, conectando embarcadores a transportadoras, ampliando sua atuação para além dos serviços de mobilidade urbana. Geograficamente, a mesma opera em aproximadamente 70 países ao redor do mundo, com presença significativa nos Estados Unidos e Canadá, América Latina, Europa (exceto Rússia), Oriente Médio, África e Ásia (exceto China e Sudeste Asiático) (Uber, 2024)[3].

No contexto do Direito do Trabalho, a Uber é categorizada como uma "plataforma digital de trabalho" devido à sua função de mediação entre trabalhadores humanos e consumidores finais (Arruda, 2024; GINÈS Y FABRELLAS, 2021; Ojeda Avilés, 2022; Signes, 2019). Esta mediação ocorre principalmente através da sua aplicação, que utiliza algoritmos avançados para estabelecer contato entre os passageiros e os motoristas e, similarmente, entre os consumidores e os entregadores(Arruda, 2022). Essa discussão tem implicações diretas para os direitos trabalhistas e os benefícios associados, colocando a Uber no centro de debates legais e regulatórios (ILO, 2024).

A infraestrutura tecnológica da Uber inclui aplicativos móveis para iOS e Android, interfaces web, sistemas de geolocalização para rastreamento em tempo real, e uma variedade de métodos de pagamento seguros, permitindo transações rápidas e confiáveis. A operação da plataforma depende de grandes volumes de dados, incluindo informações pessoais de usuários, históricos de viagens, dados de pagamento e métricas de desempenho, que são utilizados para personalizar os serviços e otimizar as operações, garantindo a segurança e eficiência do sistema (Costhek Abilio, 2019).

[3] (*Uber Cities - Rides Around the World | Uber*, 2024).

Devido à sua dependência de dados e natureza digital, a cibersegurança é uma preocupação crítica para a Uber. A proteção de informações sensíveis contra acessos não autorizados e ataques cibernéticos é essencial, pois falhas na segurança podem comprometer dados pessoais de milhões de usuários, afetar a confiança no serviço e causar danos reputacionais significativos. A empresa precisa lidar com vulnerabilidades em sistemas de autenticação, infraestrutura de rede e ataques de engenharia social, destacando a necessidade de um compromisso contínuo com práticas robustas de cibersegurança.

2. Ataques e vulnerabilidades: a cibersegurança em ação

A cibersegurança pode ser definida como a prática de proteger computadores, servidores, redes e dados contra-ataques maliciosos. Ela envolve o uso de tecnologias, ferramentas, processos e controles para garantir a confidencialidade, integridade e disponibilidade das informações digitais, prevenindo acessos não autorizados, danos, divulgação e roubo de dados (Geers, 2011; Lezzi et al., 2018; Mohammadpourfard et al., 2020). Na essência, a cibersegurança atua como uma defesa digital que mantém informações e sistemas seguros contra ameaças internas e externas.

A cibersegurança é essencial para a proteção de dados e para a integridade dos sistemas de informação globalmente. Em Portugal, esse tema ganhou destaque devido a recentes intrusões em grandes empresas do país. Um exemplo marcante foi o ataque à Vodafone, que afetou serviços móveis, de televisão e internet em todo o país, expondo a vulnerabilidade de suas infraestruturas de telecomunicações. Apesar de suas tecnologias avançadas, a proteção pode não ter sido igualmente robusta. Durante essa brecha de segurança, a Vodafone Portugal precisou interromper serviços para milhões de clientes, evidenciando a necessidade de redes de telecomunicações mais resilientes (CNN Portugal, 2022.).

Esses incidentes ilustram como as empresas e instituições públicas estão sujeitas a diversas fragilidades informáticas que podem ser exploradas por cibercriminosos, tais como vulnerabilidades em aplicações web, incluindo injeção SQL, Cross-Site Scripting (XSS) e Cross-Site Request Forgery (CSRF). Essas falhas podem ser utilizadas para roubar dados, manipular informações ou comprometer a integridade dos sistemas. Hackers, motivados por desafios técnicos, ganhos financeiros, ativismo (hacktivismo) ou busca por notoriedade, exploram tanto vulnerabilidades técnicas quanto humanas, como a engenharia social, e estão constantemente à procura de novas brechas e métodos para superar as defesas de segurança (Mitnick & Simon, 2017).

A ênfase na cibersegurança é crucial para aumentar a proteção e prevenção contra esses ataques. Medidas preventivas fundamentais incluem: (i) implementação de sistemas de autenticação

multifator; (ii) criptografia de dados; (iii) monitoramento contínuo de redes; e (iv) treinamento regular de funcionários para reconhecer e responder a tentativas de phishing. Phishers usam engenharia social para acessar contas e informações pessoais das vítimas, podendo atingir indivíduos, grupos ou comunidades inteiras. A cibersegurança moderna deve incluir simulações realistas de ataques de phishing e outras ameaças de engenharia social para treinar usuários de forma eficaz (Kothamasu et al., 2023; Romano & Armelin, 2023).

Além disso, a realização de auditorias e testes de penetração (pentests) regulares é essencial para identificar e corrigir vulnerabilidades antes que sejam exploradas por atacantes (Hossain et al., 1 C.E.; Mitola & Prys, 2024). O uso de Inteligência Artificial (IA) e aprendizado de máquina tem se tornado cada vez mais comum para prever e mitigar ameaças cibernéticas proativamente. Essas tecnologias ajudam a detectar padrões anômalos e a responder rapidamente a possíveis ataques, aumentando a resiliência dos sistemas contra invasões (Wang & Liu, 2022).

Integrar essas medidas pode fortalecer significativamente a postura de cibersegurança das organizações, reduzindo o risco de comprometimento de dados e interrupção de serviços essenciais, como evidenciado pelos ataques recentes a instituições públicas e privadas.

3 . Estudo do caso

Em 15 de setembro de 2022, a Uber Technologies, Inc. foi alvo de um ataque cibernético significativo realizado por um hacker que comprometeu seus sistemas internos. Naquela quinta-feira, a empresa detectou uma brecha de segurança em sua rede de computadores e, durante a investigação, precisou desligar vários sistemas de comunicação e engenharia que foram claramente corrompidos pela violação (Euronews, 2022).

Um indivíduo assumiu a responsabilidade pelo ataque, enviando imagens de e-mails, armazenamento em nuvem e repositórios de código para pesquisadores de segurança cibernética e para o The New York Times (The New York Times, 2022). O ataque teve início com uma tática de engenharia social, onde o hacker, identificado como um jovem de 18 anos, se fez passar por um funcionário da área de tecnologia da empresa e convenceu um trabalhador da Uber a fornecer suas credenciais de acesso.

O invasor obteve acesso completo a ambientes de nuvem hospedados pela *Amazon Web Services* (AWS) e pelo *Google Cloud*, onde a Uber armazena seu código-fonte e dados dos clientes. Além disso, o hacker comprometeu ferramentas internas importantes, incluindo o painel de administração do *Google Workspace*, contas da AWS, o sistema de segurança *SentinelOne* e o serviço

de mensagens internas *Slack*. Ele utilizou a conta do funcionário para anunciar a violação no Slack da empresa, inicialmente interpretado pelos colaboradores como uma brincadeira (Reuters, 2022).

Durante o ataque, o hacker também acessou relatórios de vulnerabilidades na plataforma *HackerOne*, usada para gerenciar programas de recompensas com base na identificação de falhas de segurança, chegando a visualizar e comentar nesses relatórios, o que expôs informações sensíveis sobre as vulnerabilidades conhecidas da Uber. O impacto direto do ataque foi substancial, causando preocupação em todos os departamentos da empresa pela possível exposição de dados financeiros e pessoais de funcionários e clientes, além de gerar publicidade negativa e evidenciar falhas significativas na segurança da Uber.

Em resposta ao ataque, a Uber tomou medidas drásticas, desativando vários de seus sistemas internos para conter a invasão, e iniciou uma investigação abrangente para avaliar a extensão do comprometimento. A empresa afirmou estar em contato com as autoridades e trabalhando para restringir o acesso do hacker, além de reforçar as medidas de segurança para evitar futuras violações.

4 Implicações jurídicas decorrentes do ataque hacker à Uber

O ataque cibernético à Uber de 2022 levantou questões jurídicas significativas, especialmente no contexto do Regulamento Geral sobre a Proteção de Dados (GDPR). A violação de dados pessoais expôs a empresa a penalidades severas, evidenciando a necessidade de uma abordagem integrada que alie segurança cibernética e conformidade legal. A seguir, abordamos as principais implicações jurídicas, com exemplos de casos semelhantes julgados pelo Tribunal de Justiça (TJUE).

O GDPR, em seu Artigo 5, n. 1, alínea "f" determina que os dados pessoais devem ser tratados com a devida segurança, protegendo-os contra acesso não autorizado, tratamento ilegal, perda, destruição ou danos acidentais. No caso da Uber, a incapacidade de proteger os dados dos usuários revelou fragilidades críticas na infraestrutura de segurança da empresa, configurando uma violação direta deste princípio (Regulamento (UE) 2016/679).

Além disso, o Artigo 32, n. 1, do GDPR exige que os controladores de dados adotem medidas técnicas e organizacionais adequadas para assegurar um nível de segurança proporcional aos riscos envolvidos no tratamento dos dados. Tais medidas incluem a pseudonimização e criptografia de dados pessoais, além de garantir a confidencialidade, integridade, disponibilidade e resiliência dos sistemas de tratamento. No caso da Uber, a ausência de autenticação multifator e de

monitoramento contínuo facilitou o acesso não autorizado aos dados, o que constitui uma violação clara dessas exigências (Regulamento (UE) 2016/679, Artigo 32).

O Artigo 33, n. 1, do GDPR estabelece que, em caso de violação de dados pessoais, a empresa deve notificar a autoridade de controle competente sem demora injustificada e, quando possível, dentro de 72 horas após tomar conhecimento da violação. O descumprimento desse prazo pode resultar em multas que podem chegar a 20 milhões de euros ou 4% do faturamento anual global da empresa, conforme previsto no Artigo 83, n. 5, alínea "a", do GDPR. Adicionalmente, o Artigo 34, n. 1, exige que, se a violação de dados representar um alto risco para os direitos e liberdades dos indivíduos, a empresa deve informar os titulares dos dados afetados sem demora. O não cumprimento dessas obrigações pode acarretar sanções adicionais (Regulamento (UE) 2016/679, Artigos 33 e 34).

O Artigo 24 do GDPR reforça a responsabilidade do controlador de dados em adotar medidas adequadas para garantir e demonstrar conformidade com o regulamento. A falta de uma infraestrutura de segurança robusta e de treinamentos adequados para os funcionários sobre práticas de cibersegurança pode resultar em penalidades financeiras e ações judiciais. Além disso, o Artigo 82 assegura aos titulares de dados o direito à compensação integral por quaisquer danos sofridos devido a violações do GDPR.

Casos julgados pelo TJUE ilustram as consequências práticas das violações ao GDPR. No caso *Google Spain SL* e *Google Inc. v. Agência Española de Protección de Datos* (AEPD) e Mario Costeja González (C-131/12), o TJUE determinou que as empresas são responsáveis por proteger os dados pessoais e por cumprir todas as disposições do GDPR, incluindo o direito ao esquecimento. Outro exemplo relevante é o caso *Schrems II* (*Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*) (C-311/18), em que o TJUE invalidou o *Privacy Shield*, que regulava a transferência de dados entre a UE e os EUA, por não oferecer proteção adequada conforme o GDPR. Este caso enfatiza a necessidade de garantir que transferências internacionais de dados estejam em conformidade com o GDPR e alerta para as sanções em casos de não conformidade.

No contexto do direito mercantil europeu, várias referências destacam a importância de uma abordagem robusta à proteção de dados e à segurança cibernética. Kuner (2020) discute os desafios legais dos fluxos de dados transfronteiriços e a legislação de privacidade, enquanto Lynskey (2015) analisa os fundamentos do Direito de proteção de dados da UE e sua aplicação jurisprudencial. Koops e Leenes (2007) exploram a erosão gradual da privacidade e suas implicações legais, e Hijmans (2016) avalia o papel da União Europeia como guardiã da privacidade

digital. Essas obras reforçam a interseção entre cibersegurança e direito mercantil, sublinhando a necessidade de conformidade contínua e proteção adequada.

O ataque hacker à Uber demonstra as graves implicações jurídicas de falhas na proteção de dados pessoais conforme o GDPR. As penalidades financeiras, a perda de confiança dos consumidores e as ações regulatórias são algumas das consequências enfrentadas pela empresa. Os precedentes do TJUE reforçam a responsabilidade das empresas em manter a conformidade com as regulamentações de proteção de dados, destacando a importância de uma abordagem integrada e rigorosa à cibersegurança e ao Direito Mercantil. É necessário que não apenas as empresas de plataformas digitais, como a do presente artigo, mas também todas as empresas que operam na Internet tenham um senso aguçado para a cibersegurança. A continuidade com êxito de suas operações mercantis depende dessa preocupação, tendo-se em consideração que os ataques dos cibercriminosos têm explorado e muito essa vulnerabilidade do conhecimento empresarial nessa perspectiva. Hoje, talvez o que tenhamos de mais valioso nas nossas empresas, não estão mais entre quatro paredes, mas armazenados em equipamentos informáticos, que, geralmente, estão alocados em uma nuvem.

5 Análise técnica em cibersegurança no que tange ataques cibernéticos às plataformas digitais

O caso do ataque cibernético à Uber destacou diversas questões críticas relacionadas à cibersegurança, especialmente no uso de engenharia social, um método amplamente utilizado para manipular pessoas a revelar informações confidenciais. Esse tipo de ataque explora a vulnerabilidade humana, uma das camadas mais difíceis de proteger em sistemas de segurança cibernética (CyberSec UK). Rachel Tobac, CEO da SocialProof Security, afirmou que ataques de engenharia social têm aumentado significativamente, e técnicas semelhantes foram utilizadas em violações recentes na Microsoft e Okta, além do famoso ataque ao Twitter em 2020, onde adolescentes usaram engenharia social para invadir a empresa. Esses casos demonstram como a exploração da vulnerabilidade humana se tornou uma das ameaças mais desafiadoras para a cibersegurança moderna (Finger & Favero, 2024; Hadnagy, 2021).

Métodos de comunicação online, como e-mails, mensagens de texto via Telegram, WhatsApp e redes sociais, tornaram-se alvos frequentes de hackers. Com uma simples pesquisa em sites como "*who.is*[4]", informações sensíveis podem ser obtidas e utilizadas para realizar ataques de engenharia social, comprometendo sistemas sem a necessidade de conhecimento técnico avançado.

[4] (*WHOIS Search, Domain Name, Website, and IP Tools - Who.Is*, n.d.)

Isso evidencia a facilidade com que esses ataques podem ser realizados e a necessidade de medidas preventivas robustas para proteger contra tais ameaças.

Tanto pequenas quanto grandes empresas enfrentam tentativas constantes de ataques por indivíduos com diferentes níveis de conhecimento técnico, causando prejuízos financeiros significativos. Isso sublinha a importância de um desenvolvimento contínuo de empresas especializadas em segurança digital, focando-se no treinamento de funcionários e no desenvolvimento de soluções técnicas específicas para cada organização (CyberSec UK; Euronews; OWASP, 2022).

Um exemplo relevante foi o ataque à Rockstar Games, conhecida pelo jogo GTAV, que gerou mais de 6 bilhões de dólares em receita. O ataque envolveu o uso de um Firestick da Amazon, um celular e um teclado para obter acesso ao Slack, uma plataforma de comunicação interna amplamente utilizada. Utilizando técnicas de phishing, o hacker comprometeu os sistemas internos da empresa e ameaçou divulgar o código-fonte caso não fosse contatado via Telegram [5]. Phishing é um método de ataque cibernético onde os atacantes enganam as vítimas para revelar informações sensíveis, como senhas e números de cartões de crédito, por meio de comunicações eletrônicas fraudulentas que se passam por entidades legítimas. O phishing explora a confiança das vítimas, levando-as a agir com urgência sem verificar a veracidade das mensagens, resultando na divulgação de informações confidenciais (Kuraku et al., 2023).

Esses ataques reforçam a necessidade de uma abordagem holística para a segurança, que inclua não apenas proteções técnicas, mas também formação e treinamento contínuo dos funcionários (Adeboye Popoola et al., 2024; Alnajim et al., 2023). A capacitação em cibersegurança, por meio de programas educacionais e workshops, é fundamental para mitigar ataques e fortalecer as defesas internas das organizações. Isso promove uma cultura de segurança dentro das empresas, tornando os funcionários mais aptos a reconhecer e reagir a ameaças de forma adequada.

Geralmente, as empresas têm um departamento de TI responsável pela instalação e manutenção de sistemas, mas poucas destinam recursos exclusivos para a área de cibersegurança ou dividem responsabilidades entre diferentes equipes. No contexto da cibersegurança, é ideal que as empresas tenham três grupos distintos: a Equipe Azul (responsável pela defesa e monitoramento contínuo dos sistemas), a Equipe Vermelha (que simula ataques para testar a resiliência dos sistemas) e a Equipe Roxa (que combina as habilidades das equipes Azul e Vermelha, promovendo a colaboração entre defesa e ataque). Essa divisão permite uma abordagem mais robusta e

[5] (*GTA 6 | Hacker Que Vazou Trechos de Gameplay é Condenado a Internação Hospitalar Por Tempo Indeterminado - ESPN*, n.d.)

integrada, cobrindo tanto os aspectos defensivos quanto ofensivos da cibersegurança (ENISA, 2022; NIST, 2018).

A conscientização dos funcionários é essencial para prevenir ataques bem-sucedidos. A utilização de modelos de *machine learning* para prever ameaças à segurança é uma área promissora, permitindo prever se uma vulnerabilidade é suscetível de ser explorada com base em dados coletados de fontes como a *dark web*. A disponibilidade de grandes volumes de dados externos torna o uso desses métodos de *machine learning* ainda mais promissor para prever ataques cibernéticos. Além disso, o uso de modelos de séries temporais para prever incidentes cibernéticos demonstra o potencial desses sistemas para aumentar a resiliência das defesas cibernéticas (Okoli et al., 2024; Sarker, 2023).

Embora o estudo de caso da Uber tenha sido escolhido pela sua relevância como uma plataforma digital de trabalho amplamente conhecida, a necessidade de segurança dos sistemas e dos dados é uma preocupação que se estende a todos os setores na era digital atual. Por exemplo, ataques a veículos autônomos mostram como hackers podem assumir o controle de funções críticas, como a direção, através de conexões simples como 3G, explorando falhas existentes nos sistemas. Um caso emblemático é o ataque ao Jeep Cherokee, onde hackers exploraram vulnerabilidades no sistema *Uconnect*, que controla a navegação e entretenimento do veículo, comprometendo não apenas os dados pessoais dos usuários, mas também a segurança física dos cidadãos (ProQuest, 2019).

Além de técnicas de engenharia social, outras vulnerabilidades comuns incluem injeção SQL, que explora falhas em consultas SQL para manipular ou roubar dados de um banco de dados; *Cross-Site Scripting* (XSS), que injeta scripts maliciosos em páginas web para roubar cookies ou redirecionar usuários para sites maliciosos; *Cross-Site Request Forgery* (CSRF), que induz usuários autenticados a executar ações indesejadas sem seu conhecimento; e *File Inclusion*, que explora falhas para incluir arquivos não autorizados no servidor, como *Local File Inclusion* (LFI) e *Remote File Inclusion* (RFI) (Augusto Lopes de Faria & Carlos -São Paulo, 2024). A mitigação dessas vulnerabilidades envolve práticas como validação de entradas, uso de consultas parametrizadas, codificação de saídas e restrições de acesso apropriadas (OWASP, 2022; SANS Institute, 2020; Mitnick & Simon, 2017).

A autenticação e autorização inadequadas também são preocupações críticas, pois falhas na implementação desses mecanismos, como senhas fracas ou falta de autenticação multifator, podem permitir acessos não autorizados. Medidas como autenticação multifator e políticas de senha forte são essenciais para mitigar esses riscos (ENISA, 2022).

Em resumo, os ataques à Uber e a outras grandes empresas demonstram que possuir sistemas tecnológicos avançados não é suficiente; é essencial protegê-los de forma eficaz contra-ataques maliciosos. As empresas devem adotar uma abordagem abrangente que inclua formação contínua dos funcionários, implementação de práticas robustas de segurança, e testes regulares de penetração para identificar e corrigir vulnerabilidades. A cibersegurança deve ser vista não apenas como uma questão técnica, mas como uma parte integral da cultura organizacional, exigindo vigilância constante e preparação para enfrentar as ameaças digitais (Appiah et al., 2022).

Conclusão

O ataque hacker à Uber em 15 de setembro de 2022 expôs falhas críticas na cibersegurança de uma das maiores plataformas digitais de trabalho, destacando a eficácia da engenharia social como um vetor de ataque capaz de explorar vulnerabilidades humanas. Esse incidente revelou que, apesar da presença de medidas tecnológicas avançadas, o fator humano continua sendo uma fraqueza significativa quando não há preparação adequada para reconhecer e responder a ameaças cibernéticas. A manipulação de funcionários para obtenção de credenciais de acesso sublinha a importância de uma abordagem abrangente e contínua em cibersegurança, que inclua tanto proteções técnicas quanto a formação constante dos colaboradores.

A análise revelou que a Uber, embora tivesse diversas camadas de segurança tecnológica, falhou em mitigar os riscos relacionados à engenharia social devido à falta de treinamento adequado dos seus funcionários. A resposta rápida da empresa, com a desativação de sistemas internos e a comunicação imediata com as autoridades, foi crucial para conter a invasão e minimizar os danos, mas evidenciou a necessidade de uma estratégia de cibersegurança mais robusta e proativa.

Para mitigar riscos futuros e fortalecer as defesas cibernéticas, é essencial que plataformas digitais de trabalho adotem medidas como: treinamento contínuo de cibersegurança para todos os níveis da organização, capacitando os funcionários a identificar e responder a ameaças; implementação de autenticação multifator para prevenir acessos não autorizados, mesmo que as credenciais sejam comprometidas; revisões regulares de segurança, incluindo auditorias e testes de penetração para identificar e corrigir vulnerabilidades proativamente; e desenvolvimento de um plano robusto de resposta a incidentes para detectar, responder e recuperar rapidamente de ataques cibernéticos.

Os casos recentes, como o da Uber e outras grandes empresas, reforçam que não basta investir em sistemas tecnológicos avançados; é fundamental criar uma cultura organizacional de vigilância e preparação, onde a cibersegurança seja entendida não apenas como um aspecto técnico,

mas como uma responsabilidade de todos dentro da organização. Esse cenário se torna ainda mais relevante quando consideramos a interseção entre cibersegurança e Direito Mercantil, onde a conformidade com regulamentações de proteção de dados, responsabilidade civil e práticas de segurança se tornam essenciais para a gestão de riscos e a proteção dos ativos corporativos.

Pesquisas futuras no campo da cibersegurança para plataformas digitais de trabalho podem focar no desenvolvimento de tecnologias de detecção de engenharia social em tempo real, abordando a necessidade urgente de identificar tentativas de manipulação antes que elas causem danos. Além disso, a investigação sobre o impacto psicológico da formação em cibersegurança pode fornecer insights valiosos sobre como o treinamento influencia o comportamento dos funcionários e contribui para a resiliência organizacional. A segurança em ambientes de nuvem, onde muitas plataformas digitais operam, também deve ser uma prioridade, com a exploração de novas estratégias para proteger dados e sistemas em um cenário cada vez mais digitalizado. Finalmente, a integração de inteligência artificial e machine learning na segurança cibernética apresenta um campo promissor para a automação da detecção e mitigação de ameaças, tornando as respostas mais rápidas e eficazes.

Este estudo reforça a necessidade de investir em cibersegurança como uma prioridade estratégica, especialmente para empresas do setor tecnológico. A falta de medidas robustas de proteção pode acarretar não apenas perdas financeiras e jurídicas, mas também danos irreparáveis à reputação, comprometendo a continuidade e a competitividade das empresas no mercado global. A interseção entre cibersegurança e direito mercantil deve ser explorada de forma a criar uma base sólida para a proteção de dados, a gestão de riscos e a construção de confiança com clientes e parceiros comerciais. Somente com uma abordagem integrada e proativa, que combine tecnologia, treinamento e conformidade regulatória, as empresas estarão realmente preparadas para enfrentar os desafios da cibersegurança na era digital.

REFERÊNCIAS BIBLIOGRÁFICAS:

Adeboye Popoola, O., Oladipo Akinsanya, M., Nzeako, G., Chukwurah, E. G., David Okeke, C., & Author, C. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and U.S. Initiatives. International Journal of Applied Research in *Social Sciences*, 6(5), 819–827. https://doi.org/10.51594/IJARSS.V6I5.1104

Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. Symmetry 2023, Vol. 15, Page 2175, 15(12), 2175. https://doi.org/10.3390/SYM15122175

Antunes Cruz, A., Roberto, J., & Andrade, S. (2021). *Lei geral de proteção de dados e general data protection regulation: um estudo comparativo de suas características*. https://repositorio.bahiana.edu.br:8443/jspui/handle/bahiana/6723

Appiah, G., Amankwah-Amoah, J., & Liu, Y. L. (2022). Organizational Architecture, Resilience, and Cyberattacks. *IEEE Transactions on Engineering Management*, 69(5), 2218–2233. https://doi.org/10.1109/TEM.2020.3004610

Arruda, M. de S. (2022). Unraveling the Algorithms for Humanized Digital Work Oriented Artificial Intelligence. In G., M. B., P. A., R. B., S. A. (eds) Marreiros (Ed.), Progress in Artificial Intelligence. *EPIA 2022. Lecture Notes in Computer Science*. (Vol. 13566, pp. 96–107). Springer. https://doi.org/10.1007/978-3-031-16474-3_9

Arruda, M. de S. (2024). *Algorithmic Management and Work on Digital Labor Platforms: Effects of Recommendation Algorithms* (pp. 443–457). https://doi.org/10.1007/978-981-99-8346-9_37

Ataque informático à Câmara de Gondomar: dados roubados estão em leilão na dark web | Gondomar | PÚBLICO. Retrieved June 14, 2024, from https://www.publico.pt/2023/10/09/local/noticia/ataque-informatico-camara-gondomar-dados-roubados-estao-leilao-dark-web-2066112

Augusto Lopes de Faria, R., & Carlos -São Paulo, S. (2024). *Desenvolvimento seguro em plataformas de fantasy game: InterREP manager*. https://repositorio.ufscar.br/handle/ufscar/20538

Equipe Roxa - AttackIQ.. Retrieved June 15, 2024, from https://www.attackiq.com/glossary/purple-teaming/

Finger, E. R., & Favero, S. (2024). O direito à proteção de dados sob a ótica das vulnerabilidades do usuário. *Academia de Direito*, 6, 129–152. https://doi.org/10.24302/ACADDIR.V6.4347

Geers, K. (2011). Strategic cyber security. *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE).

GTA 6 | Hacker que vazou trechos de gameplay é condenado a internação hospitalar por tempo indeterminado - ESPN. Retrieved September 15, 2024, from https://www.espn.com.br/esports/artigo/_/id/13024131/gta-6-hacker-vazou-trechos-gameplay-condenado-internacao-hospitalar-tempo-indeterminado

Hackers on the Highway: Are We Prepared? - ProQuest. (2019). https://www.proquest.com/openview/3b02a68f8e6d5dc6d308b69896c39c9e/1?pq-origsite=gscholar&cbl=1576347

Hossain, S., Rahman, L., Azad, R., Hasan, M. M., Jebin, M., Mahmud, M. S., & Sakib, M. S. (1 C.E.). *Penetration Testing and Cyber Security Studies in Bangladesh: Post-COVID-19 Managerial Issues*. Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-6684-3894-7.Ch008, 171–195. https://doi.org/10.4018/978-1-6684-3894-7.CH008

ILO. (2024). *Hacer realidad el trabajo decente en la economía de plataformas*. https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_910140.pdf

INSTITUTO SANS. Retrieved June 15, 2024, from https://www.sans.org/br_pt/

Kuraku, Dr. S., Kalla, D., Smith, N., & Samaah, F. (2023). *Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks*. https://papers.ssrn.com/abstract=4666794

Kothamasu, G. A., Venkata, S. K. A., Pemmasani, Y., & Mathi, S. (2023). *An Investigation on Vulnerability Analysis of Phishing Attacks and Countermeasures. International Journal of Safety and Security Engineering*, 13(2), 333. https://doi.org/10.18280/IJSSE.130215

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, 103, 97–110. https://doi.org/10.1016/J.COMPIND.2018.09.004

Lima, P. R. S., Ferreira, L. M. M., & Peixoto, A. L. V. de A. (2022). Gestão da segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira. *P2P E INOVAÇÃO*, 9(1), 206–221. https://doi.org/10.21721/P2P.2022V9N1.P206-221

Mitola, J., & Prys, M. (2024). *Cyber oriented digital engineering. Systems Engineering*, 27(1), 109–119. https://doi.org/10.1002/SYS.21710

Mitnick, K., & Simon, W. (2017). *The Art of Invisibility. Little, Brown and Company*.

Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M., & Mohammadi-Ivatloo, B. (2020). Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. *International Journal of Electrical Power & Energy Systems*, 119, 105947. https://doi.org/10.1016/J.IJEPES.2020.105947

Ojeda Avilés, A. (2022). Gig economy y trabajo con plataformas digitales el ámbito laboral. *Revista Española de Derecho Del Trabajo*, 81–114.

Okoli, U. I., Obi, O. C., Adewusi, A. O., Abrahams, T. O., Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024*). Machine learning in cybersecurity: A review of threat detection and defense mechanisms*. Https://Wjarr.Com/Sites/Default/Files/WJARR-2024-0315.Pdf, 21(1), 2286–2295. https://doi.org/10.30574/WJARR.2024.21.1.0315

Previsão de incidentes cibernéticos corporativos usando análise de redes sociais em fóruns de hackers da dark web no JSTOR. Retrieved June 4, 2024, from https://www.jstor.org/stable/26846122

Romano, M. R., & Armelin, S. R. (2023). Ameaças Cibernéticas em ascensão. *Prospectus* (ISSN: 2674-8576), 5(2), 187–200. https://doi.org/10.5281/zenodo.10083791

Sarker, I. H. (2023). Machine Learning for Intelligent Data Analysis and Automation in *Cybersecurity: Current and Future Prospects. Annals of Data Science*, 10(6), 1473–1498. https://doi.org/10.1007/S40745-022-00444-2/FIGURES/6

Signes, A. T. (2019). Plataformas Digitales y concepto de trabajador: Una propuesta de interpretación finalista. Lan Harremanak - *Revista de Relaciones Laborales*, 41, 17–41. https://doi.org/10.1387/lan-harremanak.20880

Uber Cities - Rides Around the World | Uber. (2024). https://www.uber.com/global/pt/cities/

Uber Investigating Breach of Its Computer Systems - The New York Times. Retrieved June 9, 2024, from https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html

Uber investigating "cybersecurity incident" after hacker breaches computer network | Euronews.. Retrieved June 9, 2024, from https://www.euronews.com/next/2022/09/16/uber-investigating-cybersecurity-incident-after-hacker-breaches-computer-network

Vodafone: tudo o que se sabe e o (muito) que ainda falta saber sobre o ciberataque - *CNN Portugal*. Retrieved June 14, 2024, from https://cnnportugal.iol.pt/operadora/hackers/o-que-se-sabe-e-o-que-nao-se-sabe-sobre-o-ciberataque-a-vodafone/20520131/620271150cf2c7ea0f17e148

WHOIS Search, Domain Name, Website, and IP Tools. Retrieved September 15, 2024, from https://who.is/