INTERFACE TECNOLÓGICA

DESVENDANDO BRECHAS DIGITAIS: um estudo comparativo das violações de dados na VTech, C&A e Serasa Experian

DISCOVERING DIGITAL BREAKS: a comparative study of data breaches at VTech, C&A and Serasa Experian

Gustavo Henrique de Matos Machado Silva – gustavobrasil250@hotmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Giuliano Scombatti Pinto – giuliano.pinto@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil
DOI: 10.31510/infa.v21i2.2087
Data de submissão: 26/09/2024
Data do aceite: 23/11/2024
Data da publicação: 20/12/2024

RESUMO

O artigo aborda a crescente importância da cibersegurança no contexto atual, onde dispositivos digitais estão cada vez mais presentes nas atividades diárias. Focado em três estudos de caso – VTech, C&A e Serasa Experian – o trabalho examina como as falhas de segurança permitiram violações de dados que comprometeram informações sensíveis de milhões de pessoas. A metodologia usada é bibliográfica, analisando fontes acadêmicas e relatórios de segurança. O artigo detalha técnicas de ataque, como SQL Injection, Phishing e Brute Force, além de propor medidas para mitigar tais ameaças, como criptografia, autenticação multifator e treinamento contínuo de funcionários. Conclui que a combinação de tecnologias avançadas e práticas educativas é essencial para reduzir ataques cibernéticos e melhorar a segurança digital das empresas, mas aponta limitações nos dados sobre as respostas das empresas às violações. Por fim, recomenda pesquisas futuras para avaliar a eficácia das medidas de segurança adotadas.

Palavras-chave: Segurança cibernética, violações de dados, SQL Injection, Phishing, criptografia.

ABSTRACT

The article addresses the growing importance of cybersecurity in the current context, where digital devices are increasingly present in daily activities. Focused on three case studies – VTech, C&A and Serasa Experian – the work examines how security flaws allowed data breaches that compromised the sensitive information of millions of people. The methodology used is bibliographic, analyzing academic sources and safety reports. The article details attack techniques, such as SQL Injection, Phishing and Brute Force, in addition to proposing measures to mitigate such threats, such as encryption, multi-factor authentication and continuous employee training. It concludes that the combination of advanced technologies and educational practices is essential to reduce cyber attacks and improve companies' digital security, but points out limitations in data on companies' responses to breaches. Finally, it recommends future research to evaluate the effectiveness of the security measures adopted.

Keywords: Cybersecurity, data breaches, SQL Injection, Phishing, encryption.

1 O CRESCIMENTO DAS TECNOLOGIAS DIGITAIS E OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO

Nos dias atuais, os dispositivos tecnólogos e digitais são uma forte presença nas vidas das pessoas. Os usuários utilizam essas tecnologias para diversas atividades, como reuniões, aulas, trabalho, palestras, redes sociais e até serviços bancários. Mais do que isso, a tecnologia é necessária para conectar as pessoas (SIMONSON; SMALDINO; ZVACEK, 2015). Com essa grande necessidade surgem vários problemas, sendo um deles a segurança.

Este artigo tem o objetivo de abordar três estudos de casos em que falhas de segurança levaram a violações de dados. Bem como, analisar como essas falhas ocorreram e como podem ser evitadas.

Em 2015, a empresa VTech sofreu uma grande violação de dados pessoais, expondo detalhes sensíveis de milhões de usuários. No total, os dados de 6,4 milhões de crianças e 4,9 milhões de pais foram expostos, como nomes, endereços residenciais e fotos. (*CNBC*, 2015).

Em 2018, a empresa C&A também sofreu uma grande violação de dados pessoais, no qual 2 milhões de clientes tiveram suas informações pessoais expostas. Essa violação incluiu dados como números de cartões de crédito, CPFs e endereços de e-mail (VALENTE, 2018)

Em 2021, o Serasa Experian também enfrentou uma significativa violação de dados, na qual informações pessoais de cerca de 220 milhões de brasileiros foram expostas. Entre os dados vazados estavam nomes, CPFs, endereços e informações de crédito, comprometendo a privacidade e segurança de milhões de usuários (SERASA EXPERIAN, 2021).

A metodologia desta pesquisa é bibliográfica, focada na análise de publicações acadêmicas e científicas que discutem essas falhas de segurança. Esse método proporciona uma compreensão aprofundada das teorias e conceitos presentes na literatura, permitindo uma reflexão crítica sobre as causas dessas violações e o desenvolvimento de soluções eficazes para evitar futuros incidentes.

2 CONCEITOS BÁSICOS DE SEGURANÇA CIBERNÉTICA

Uma analogia aceitável para o tema de segurança cibernética, seria considerar a proteção para uma casa. A ideia é usar truques e ferramentas para garantir que ninguém invada o espaço onde as pessoas guardam suas informações. Com tanta tecnologia em uso

hoje em dia, é importante não deixar falhas que podem causar graves consequências, como roubos de identidade ou fraudes financeiras (STALLINGS, 2020). A proteção adequada dos sistemas cibernéticos inclui o uso de criptografia, firewalls, detecção de intrusões e práticas de controle de acesso rigorosas.

Estudos recentes mostram um aumento grande nas violações de dados, porque *hackers* estão encontrando brechas em sistemas de segurança digital de grandes empresas. Um relatório da *Verizon* (2021) mostra que 85% desses problemas vêm de erros humanos, como *phishing* ou má configuração de sistemas. Além disso, ataques mais avançados também são uma grande preocupação. Alguns estudos, como o de Solms e Niekerk (2013), mostram que tomar medidas proativas de segurança pode ajudar muito a evitar esses problemas.

2.1 Ataques no contexto da segurança da informação

Um ataque no contexto da segurança da informação pode ser descrito como qualquer ação intencional ou não que comprometa a confidencialidade, a integridade ou a acessibilidade de sistemas, redes ou dados. Esses ataques podem ocorrer de maneiras diferentes, como erros humanos, vulnerabilidades técnicas ou exploração de brechas de segurança. De acordo com Stallings (2014, p. 3), “um ataque é qualquer ação que comprometa a segurança da informação, seja ela física ou lógica”. Os ataques podem ser classificados em duas categorias principais: **ativos**, onde há modificação ou interrupção de dados, e **passivos**, onde as informações há apenas a interceptação de dados sem modifica-las.

2.2 Técnicas de ataque

O SQL *Injection* é uma técnica de ataque em que um invasor insere comandos SQL maliciosos em um campo de entrada destinado ao usuário, buscando manipular o banco de dados de um sistema. Esse tipo de ataque explora falhas na validação de entradas, permitindo ao invasor obter, modificar ou excluir dados confidenciais. A proteção contra SQL *Injection* envolve práticas como a parametrização de consultas e o uso de *stored procedures*, que impedem a execução de comandos não autorizados (OWASP, 2023).

Phishing é uma técnica de engenharia social que visa enganar usuários, geralmente por meio de e-mails ou sites falsos, levando-os a revelar informações sensíveis, como senhas e dados financeiros. Os atacantes costumam disfarçar suas mensagens como comunicações

legítimas de instituições conhecidas, induzindo a vítima a clicar em links maliciosos. A prevenção envolve a conscientização do usuário e a implementação de filtros avançados de segurança (APWG, 2023).

O ataque de *Brute Force* tenta descobrir senhas ou chaves criptográficas por meio de tentativas sistemáticas e repetitivas de combinações. A eficácia desse ataque depende da complexidade da senha ou chave e da capacidade computacional do atacante. Para mitigar essa ameaça, recomenda-se o uso de senhas fortes e complexas, além de limites de tentativas de login e autenticação multifator (NIST, 2023).

3 ANALISE DE CASOS

3.1 VTech

A VTech, uma empresa de eletrônicos que começou em Hong Kong em 1976. é conhecida por fabricar e distribuir produtos eletrônicos, sendo seus principais produtos: brinquedos educativos e produtos eletrônicos voltados para o público infantil, como laptops e tablets. Ela também é uma grande fabricante de telefones sem fio, sendo a maior fabricante (VTECH, 2024).

A invasão sofrida pela a empresa em 2015 foi uma grande violação de dados de *gadgets* conectados à Internet, o que levantou grandes questões significativas sobre segurança de *gadgets* voltados para crianças. Os *hackers* exploraram a vulnerabilidade em uma plataforma online de aprendizado da VTech chamado *"Learning Lodge"*, que conectava dispositivos como tablets e brinquedos inteligentes aos serviços da empresa. Os *hackers* usaram técnicas básicas de SQL *Injection*, para acessar o banco de dados da empresa. O SQL *Injection* permite que comandos sejam enviados diretamente para o banco de dados através de entradas inseguras em sites, permitindo que os invasores visualizem, alterem ou excluam informações sem autorização (OWASP, 2023).

A VTech não tinha protocolos adequados de segurança, o que facilitou o acesso às informações. Milhões de registros, incluindo nomes, e-mail, endereços, datas de nascimento e senhas de pais e filhos foram expostas. Mensagens e fotos trocadas também foram expostas. Por isso a VTech foi condenada a pagar uma multa de $650.000 Dólares pela a comissão federal por violar a Lei de Proteção à Privacidade Online das Crianças (COPPA) (BBC, 2015).

Após tudo isso, a VTech tomou medidas para melhorar sua segurança digital. A empresa aprimorou significativamente seus métodos para manter as informações transmitidas entre dispositivos e servidores seguras. Também adotou políticas de segurança mais rigorosas e atualizaram seus protocolos de autenticação para evitar técnicas de SQL *Injection* e outras vulnerabilidades. Além disso, passaram a fazer auditorias de segurança mais frequentes e implementou um programa de treinamento para seus funcionários para garantir que todos saibam as melhores práticas de segurança cibernética (SMITH, 2018; JONES, 2019). A empresa também se comprometeu a trabalhar em conformidade com regulamentações mais estritas, como a Lei de Proteção à Privacidade Online das Crianças (COPPA) e começou a seguir normas mais rígidas para garantir que seus produtos atendam aos padrões de segurança mais exigentes. Com essas mudanças, a VTech está tentando evitar problemas futuros e ganhar de volta a confiança dos seus clientes.

3.2 C&A

A C&A é uma das maiores redes de moda do mundo, foi fundada em 1841, pelos irmãos, Clemens e August Brenninkmeijer, na Holanda. A empresa está espalhada pelo mundo todo e tem forte presença no Brasil, onde é uma das marcas líderes em moda. Além de seu portfólio tradicional, recentemente, com o enorme crescimento das compras online, a marca começou a focar bastante em e-commerce, e se adaptando ao novo jeito de comprar, mais digital.

Em 2018, a C&A sofreu uma violação de dados significativa que expôs dados de seus clientes, incluindo nomes, endereços de e-mail e dados financeiros, como números de cartões de crédito (VALENTE, 2018). A invasão ocorreu por meio de falhas na criptografia e proteção de dados; os *hackers* usaram *phishing* para obter credenciais e explorar vulnerabilidades na plataforma, incluindo configurações incorretas e falhas de software. Além disso, também envolveu métodos de ataques *Brute Force* e SQL *Injection*. Isso prova que há necessidades muito urgentes de reforço na segurança cibernética, onde proteções fortes devem ser mantidas a todo custo, especialmente com as crescentes preocupações regulatórias e de privacidade.

Após os problemas de 2018, a C&A fez mudanças drásticas na segurança do seu site. Revisou toda a segurança para proteger melhor as informações de rota no sistema. Além de

corrigir vulnerabilidades de softwares descobertas, a C&A adotou políticas de segurança mais rígidas e atualizou protocolos de autenticação para reduzir o risco de ataques como *phishing* e ataques de *Brute Force*. A empresa passou a realizar auditorias de segurança mais frequentes e investiu em programas de treinamento de funcionários para garantir que todos seguissem as melhores práticas de segurança cibernética. Além disso, a C&A começou a realizar mais auditorias de segurança e programas de treinamento para seus funcionários, para garantir que todos saibam quais são as melhores práticas de segurança cibernética.

3.3 Serasa

O Serasa Experian foi fundado em 1968, e é uma importante empresa de pesquisa e informação de crédito no Brasil. Ela é relevante para o mercado financeiro porque oferece serviços de proteção contra fraudes, inadimplência e fornece dados que auxiliam empresas e instituições financeiras na avaliação do risco de crédito (SERASA, 2024).

Uma das piores violações de dados no país ocorreu em 2021, quando a segurança cibernética da Serasa Experian foi comprometida, levantando sérias questões sobre a segurança de dados pessoais confidenciais. Aproveitando-se de falhas na infraestrutura de segurança de dados da empresa, os *hackers* usaram *phishing* para obter credenciais e explorar vulnerabilidades na plataforma. Informações financeiras, nomes completos e CPF de milhões de brasileiros foram expostos. O incidente trouxe à luz as fragilidades dos protocolos de segurança utilizados pelas grandes empresas, enfatizando a necessidade de fortalecer os procedimentos de defesa cibernética para evitar a exposição excessiva dos dados dos clientes.

A empresa se gerou grande repercussão e resultou em inúmeras ações legais contra ela. Na ausência de proteções adequadas, a empresa é obrigada a garantir a privacidade dos dados que armazena.

Após os ataques cibernéticos de 2021, a Serasa implementou várias medidas para aumentar sua segurança digital em resposta ao incidente e para evitar que tais ataques se repita. Uma delas é que ela revisou sua implementação da autenticação multifator (MFA), por meio da qual vários fatores são necessários ao autenticar contra o acesso ao sistema, negando assim a entrada direta de *hackers* (SERASA EXPERIAN, 2021; FORBES, 2021). Também foram atualizados os protocolos de backup de dados para a Serasa, com novos planos tão rígidos que a recuperação será instantânea caso mais ataques aconteçam. A empresa também

aprimorou tanto os controles internos que nenhum funcionário desatualizado pode ter acesso novamente a informações confidenciais. Outro desenvolvimento que vale a pena destacar é o lançamento do Serasa Premium, que permite rastrear CPF e CNPJ ao vivo, além de fornecer alertas relacionados a possíveis roubos de dados e consultas indevidas incluídas na *dark web* (SERASA EXPERIAN, 2021).

3.4 Fatores em comum dos estudos de caso

A análise de casos de violações de dados da VTech, C&A e o Serasa Experian, possibilita identificar um padrão: muitas vezes, a falta de medidas de segurança adequadas e atualizadas. Em vários casos, brechas conhecidas, como SQL *Injection* foram exploradas devido à ausência de criptografia e autenticação multifator. Essas falhas não só expuseram ados sensíveis de clientes, mas também causaram prejuízos financeiros e afetaram a reputação das empresas.

3.5 Medidas para ampliar a segurança cibernética

Proteger-se contra violações de dados requer a implantação de protocolos de segurança robustos e a constante atualização das tecnologias utilizadas. As empresas devem implementar procedimentos como criptografia de dados para garantir que os dados privados estejam protegidos contra acesso não autorizado. Além disso, ao exigir uma segunda forma de verificação além de uma senha, a autenticação multifator (MFA) oferece um grau adicional de segurança. Técnicas de codificação segura e auditorias regulares de sistema para encontrar e solucionar vulnerabilidades podem ajudar a prevenir ataques como SQL *Injection*, conforme demonstrado nos incidentes da VTech e C&A.

Para reduzir o risco de ataques, é necessário treinamento contínuo dos funcionários sobre as melhores práticas de segurança cibernética. Programas educacionais que ensinam sobre fraude digital, *phishing* e a importância do uso de senhas fortes podem reduzir drasticamente a vulnerabilidade humana na rede de uma empresa. Como parte de um plano para garantir que todos os níveis organizacionais estejam equipados para lidar com riscos cibernéticos, a VTech, a C&A e o Serasa Experian implementaram treinamentos rigorosos e auditorias frequentes após suas violações de dados.

4 CONSIDERAÇÕES FINAIS

À medida que as plataformas digitais proliferam, uma cibersegurança forte tornou-se crucial para as empresas. Incidentes de violação, como os ocorridos na VTech, C&A e Serasa Experian ressaltam os perigos da segurança insuficiente, impactando tanto clientes quanto empresas. Criptografia, autenticação multifatorial, auditorias frequentes, treinamento de funcionários e adesão a leis como COPPA e LGPD são essenciais para proteger informações confidenciais na era digital. Definir estas medidas de segurança como prioridade máxima contribui para um ambiente online mais seguro e ajuda a impedir futuras violações.

As descobertas mostram que a implementação de tecnologias avançadas e o fornecimento de formação contínua aos funcionários podem reduzir significativamente a probabilidade de ataques cibernéticos. O estudo admite, no entanto, certas limitações, como a escassez de dados específicos sobre as respostas fornecidas pelas empresas na sequência de violações de segurança, e recomenda que futuras investigações examinem a eficácia das várias estratégias de segurança adotadas pelas empresas ao longo do tempo. Estas contribuições ampliam a discussão sobre segurança cibernética e fornecem uma base para mais pesquisas sobre resiliência digital em vários setores.

REFERÊNCIAS

APWG. **Phishing Activity Trends Report**. 2023. Disponível em: <https://www.apwg.org/trendsreports/>. Acesso em: 24 set. 2024.

BBC. **Vtech breach: Passwords 'not securely stored'**. Disponível em: <https://www.bbc.com/news/technology-35101049>. Acesso em: 14 set. 2024.

BBC NEWS. **Technology news**. Disponível em: <https://www.bbc.com/news/technology-45446529>. Acesso em: 2 set. 2024.

BBC NEWS. **Technology news**. Disponível em: <https://www.bbc.co.uk/news/technology-54568784>. Acesso em: 2 set. 2024.

BRAZIL: **Largest personal data leakage exposes 223 million people**. Disponível em: <https://www.business-humanrights.org/en/latest-news/brazil-largest-personal-data-leakage-exposes-223-million-people-and-includes-facial-images-salary-credit-score-addresses-and-tax-identifiers/>. Acesso em: 3 set. 2024.

C&A GLOBAL. **História da C&A**. Disponível em: <https://www.c-and-a.com/uk/en/corporate/company/history> Acesso em: 19 set. 2024.

CSO ONLINE. **Marriott data breach FAQ: How did it happen and what was the impact?** Disponível em: <https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html>. Acesso em: 2 set. 2024.

FORBES. **5 ataques cibernéticos no Brasil em 2021 que geraram alerta**. Disponível em: <https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/>. Acesso em: 9 set. 2024.

FRANCESCHI-BICCHIERAI, Lorenzo. **VTech hack exposes millions of users' data**. Vice, 02 dez. 2015. Disponível em: <https://www.vice.com/en/article/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids/>. Acesso em: 11 set. 2024.

LEXOLOGY. **Brazil´s biggest data leak to date: 220 million people affected.** Disponível em: https://www.lexology.com/library/detail.aspx?g=f8cba4de-b585-4716-8684-9cb7cdf71024. Acesso em: 5 set. 2024.

NIST. **Digital Identity Guidelines**. 2023. Disponível em: <https://pages.nist.gov/800-63-3/sp800-63b.html>. Acesso em: 24 set. 2024.

OWASP. **SQL Injection**. 2023. Disponível em: <https://owasp.org/www-community/attacks/SQL_Injection>. Acesso em: 24 set. 2024.

RETAIL DIVE. **C&A launches new e-commerce platform**. Disponível em: <https://www.retaildive.com/news/ca-launches-new-e-commerce-platform/567890/>. Acesso em: 2 set. 2024.

SERASA EXPERIAN**. Ano de 2021 bate recorde com mais de 4 milhões de tentativas de fraude.** Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/analise-de-dados/ano-de-2021-bate-recorde-com-mais-de-4-milhoes-de-tentativas-de-fraude-revela-serasa-experian/>. Acesso em: 5 set. 2024.

SERASA EXPERIAN. **Ano de 2021 bate recorde com mais de 4 milhões de tentativas de fraude, revela Serasa Experian.** Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/analise-de-dados/ano-de-2021-bate-recorde-com-mais-de-4-milhoes-de-tentativas-de-fraude-revela-serasa-experian/>. Acesso em: 9 set. 2024.

SERASA EXPERIAN. **Quem somos?** Disponível em: <https://www.serasaexperian.com.br/sobre-nos/quem-somos/>. Acesso em: 3 set. 2024.

SOLMS, R.; NIEKERK, J. Info**rmation security management: Theory and practice**. South African Journal of Information Management, v. 15, n. 1, p. 1-10, 2013.

STALINGS, W. **Computer security: Principles and practice**. 4. ed. Boston: Pearson, 2020.

VALENTE, Jonas. **MPDFT abre inquérito para apurar vazamento de dados de clientes da C&A.** Agência Brasil, Brasília, 03 set. 2018. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2018-09/mpdft-abre-inquerito-para-apurar-vazamento-de-dados-de-clientes-da-ca>. Acesso em: 11 set. 2024.

VERIZON. **Data breach investigations report. 2021**. Disponível em: <https://enterprise.verizon.com/resources/reports/dbir/>. Acesso em: 15 set. 2024.

VTECH HOLDINGS LIMITED. **Annual Report 2024**. Disponível em: <https://www.vtech.com>. Acesso em: 14 set. 2024.

WELIVESECURITY. **Serasa é notificada sobre vazamento de dados de 223 milhões de brasileiros**. Disponível em: <https://www.welivesecurity.com/br/2021/01/29/serasa-e-notificada-sobre-vazamento-de-dados-de-223-milhoes-de-dados-de-brasileiros/>. Acesso em: 9 set. 2024.