Estudo de caso de ciberataques e vazamentos de informações na internet

Pedro Henrique Santos Morais, Luiz Otavio Aidar, Lucas de Araújo de Oliveira, João Paulo Lemos Escola

Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. pedro.morais@aluno.ifsp.edu.br

Ciberataques, Vazamento de informações, Vulnerabilidade, Segurança.

Introdução

A tecnologia está sempre avançando e presando pela segurança do usuário. Sites de compra e venda como Uber e Netshoes, estão sempre prontos para atender seus usuários (MARTINS, 2018).

Mesmo com a atenção na segurança, constantemente há incidência de vazamentos de dados pessoais de usuários, como arquivos, senhas, fotos, vídeos, contas bancárias entre outras. Os chamados ciberataques (DOMINGUES, 2015), ou cibercrimes, que são executados por *hackers*, são uma prática que se iniciou no fim do século passado tomando proporção de acordo com a evolução da tecnologia (MCCLURE, SCAMBRAY e KURTZ, 2014). Há livros que retratam essa realidade e mais sobre esse assunto, por exemplo "aprendizado de máquina para hackers" (CONWAY e WHITE, 2012)" e "Cuidado com hackers" (COLE e ERIC, 2002).

O principal objetivo do ciberataque é invadir *web sites* e aplicativos, para obter informações sigilosas dos usuários e disponibilizá-los na rede mundial de computadores (DOMINGUES, 2015).

Objetivos

Esse estudo de caso busca analisar os vazamentos de informações de usuários ocorridos em dois momentos da atualidade, envolvendo as empresas Uber e Netshoes. Além disso, pretende-se apresentar uma pesquisa quantitativa, com aplicação de um questionário sobre o assunto.

Material e Métodos

Foi realizada uma pesquisa de levantamento bibliográfico direcionada a ciberataques e vazamentos de informações, especificamente em relação à loja online brasileira Netshoes e ao aplicativo de transporte individual norte-americano Uber que foram vítimas de ciberataques recentemente, a Netshoes comprometendo 2 milhões de contas e Uber comprometendo 196 milhões de contas de seus usuários (MARTINS, 2018).

Resultados e Discussão

A Tabela 1, ilustra que entre 2016 e 2017 a Uber teve uma quantidade considerável de perda de dados sensíveis e sigilosos de seus usuários. A Netshoes em 2018 teve o mesmo descuido com 2 milhões de vazamentos sigilosos de seus usuários, por falhas em sua segurança.

Tabela 1 – Tabela com levantamento de dados Uber e Netshoes.

Aplicativo	Ano	Quantidade	Motivo
Uber	2016/ 2017	196 Milhões	Ponto de vulnerável na rede de segurança do banco de dados.
Netshoes	2018	2 Milhões	Ponto de fragilidade na segurança do banco de dados.

Ambos dos vazamentos ocorreram por motivos semelhantes, a Netshoes tinha brechas no sistema de segurança e o Uber parte de seu sistema de rede vulnerável facilitando a invasão de *hackers* (MARTINS, 2018).

Foi feito um questionário com perguntas para pessoas entre 14 e 45 anos em relação ao conhecimento dos perigos da internet como ciberataques e o uso dos aplicativos Uber e Netshoes, 23 pessoas responderam ao questionário cujos resultados estão dispostos na Tabela 2.

Foi questionado o tempo que a pessoa demora para atualizar a senha da conta em sites diversos: 53,8% responderam que dificilmente fazem alteração de senha e 46,2% alteram a senha da conta com frequência.

Em relação ao conhecimento do assunto “ciberataques”, 68,5% declararam que sabem o que isso significa e 38,5% não sabem.

Pessoas que já efetuaram alguma compra na Netshoes: 53,8% contra 46,2% que declararam que nunca compraram.

Dos indivíduos participantes, 50% são usuários do aplicativo Uber e 50% não são usuários.

Tabela 2 – Tabela com levantamento de dados do formulário.

Alternativas	sim	não
Usuários que sabem o que são ciberataques	0,69	0,39
Compraram na Netshoes	0,54	0,46
É cliente Uber	0,5	0,5
Pessoas que atualizam a senha com frequência	0,46	0,54

A partir dos resultados obtidos no questionário, considera-se entende-se que usuários, mesmo na maioria conhecedores do que são ciberataques e do nível de periculosidade não se atentam a mudança de senha a fim de aumentar a segurança de seus dados e contribuir para evitar acessos indevidos a suas contas online.

Conclusões

A vulnerabilidade de sistemas se tornou comum, facilitando para que o índice de ciberataques e vazamentos de dados alavanque e cresça a cada dia.

Uma alternativa para evitar esse tipo de ocorrência pode ser o investimento em pessoal, equipamentos e técnicas de segurança de dados do sistema.

Para trabalhos futuros pretendemos desenvolver um algoritmo para análise da vulnerabilidade em sites, com intuito de reduzir a incidência desse tipo de falha e aplicações que funcionam como um lembrete para o usuário fazer a alteração de senha de tempos em tempos.

Agradecimentos

Os autores gostariam de agradecer ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), Câmpus Barretos, para o desenvolvimento dessa pesquisa.

Referências Bibliográficas

COLE, Eric. **Cuidado com os hackers**. Editora Sams, 2002.

CONWAY, D.; WHITE, J. M. Machine Learning for Hackers O'Reilly Media. 2012.

DOMINGUES, Elisabete Júlio. **Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo**. 2015. Tese de Doutorado.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers Expostos-: Segredos e Soluções para a Segurança de Redes**. Bookman Editora, 2014.

MARTINS, Ana Paula Pereira. Vazamento e Mercantilização de Dados Pessoais e a fragilidade da Segurança Digital do Consumidor: Um Estudo dos Casos Netshoes e Uber. Anais do XIV Congresso Brasileiro de Direito do Consumidor. São Paulo, 2018.