Você está no LinkedIn? Cuidado!

© Rafal Olechowski/Shutterstock

O LinkedIn é um dos mais importantes sites de redes sociais na Web. Ele possui mais de 225 milhões de usuários, a maioria deles composta por profissionais de escritório atentos à própria carreira, e mais interessados em manter uma rede de relacionamentos do que uma rede social. Os usuários mantêm seus currículos on-line, estabelecem vínculos com seus colegas e contatos corporativos e pesquisam por especialistas que possam solucionar seus problemas empresariais diários. Os recrutadores corporativos, bem como pessoas que estão à procura de emprego ou progresso em suas carreiras, levam o serviço do LinkedIn muito a sério. De qualquer maneira, o LinkedIn tem sido uma das principais histórias de sucesso de tecnologia da última década. A empresa é avaliada atualmente em mais de US$ 21 bilhões.

Em junho de 2012, no entanto, a empresa sofreu uma violação de dados que expôs as senhas de milhões de usuários. Os hackers violaram a segurança do site e roubaram 6,5 milhões de senhas de usuários; em seguida, publicaram abertamente as senhas em um fórum de *hacking* da Rússia. Logo após a violação, usuários do LinkedIn e especialistas em segurança ficaram surpresos que uma empresa cuja principal função é coletar e gerir os dados do cliente havia feito tão pouco para protegê-lo. O LinkedIn lamentavelmente apresentou uma segurança do computador inadequada, especialmente para uma empresa de tecnologia tão bem-sucedida, com boas reservas de caixa, resultados consistentes e funcionários talentosos.

Especialistas em segurança criticaram o LinkedIn por não ter um executivo-chefe de segurança cuja principal função é proteger contra falhas de segurança. E, ainda mais surpreendente, era esperado que o LinkedIn tivesse uma proteção mínima de senha por meio de criptografia e, no entanto, ele não empregou várias técnicas de criptografia padrão usadas para proteger senhas. A maioria das empresas utiliza uma técnica conhecida como *salting*, que acrescenta uma série de dígitos aleatórios no final dos códigos *hash* das senhas para torná-las mais difíceis de decifrar. O *salting* pode ser realizado com pouco ou nenhum custo, com apenas algumas linhas adicionais de código. A maioria das empresas utiliza funções criptográficas complexas para acrescentar o *salt* às senhas, mas, incrivelmente, o LinkedIn não tinha acrescentado de modo algum o *salt* às senhas de seus usuários, fornecendo um nível de segurança equivalente a deixar abandonados os pertences de valor de alguém em uma área movimentada, com muitas pessoas.

A maioria das empresas armazena os códigos *hash* das senhas em servidores Web separados e seguros para dificultar ainda mais sua violação por parte dos hackers. O custo total para uma empresa como o LinkedIn implantar uma senha robusta, um servidor Web e segurança de aplicação seria de, no mínimo, algumas centenas de milhares de dólares, mas uma violação média de dados custa às empresas US$ 5,5 milhões, segundo um estudo do Instituto Ponemon, patrocinado pela Symantec. As perdas do LinkedIn poderiam ser ainda maiores do que isso, o que torna a sua total despreocupação com a segurança de dados ainda mais surpreendente.

Alguns especialistas em segurança acreditam que a falta da obrigação de indenizar das empresas como LinkedIn é uma das principais razões para suas fracas políticas de segurança. Ao contrário de outros setores, nos quais as proteções básicas do consumidor são supervisionadas e resguardadas, a segurança do computador e a segurança de dados das redes sociais não são reguladas e estão mal resguardadas por muitas empresas. Além disso, nas redes sociais, as pessoas tendem a não deixar o serviço por causa de uma violação de dados. Por exemplo, no abalo da quebra de sigilo, muitos usuários queriam deixar o LinkedIn, mas optaram por não deixá-lo porque é a rede social mais importante para manter a rede de relacionamentos profissionais.

Logo após o roubo das senhas, o LinkedIn rapidamente assegurou a seus clientes que a sua base de dados estava segura. A empresa desativou as 6,5 milhões de senhas publicadas e anunciou que tinha

começado uma iniciativa para acrescentar o *salt* às senhas para aumentar a segurança. No entanto, o LinkedIn foi atingido com um processo de ação coletiva no valor de US$ 5 milhões, que alega que ele não seguiu nem mesmo as práticas mínimas do padrão do setor para proteção de dados, especificamente as formas mais recentes de acrescentar o *salt* aos códigos *hash* das senhas.

Especialistas em segurança observaram que os procedimentos de segurança do LinkedIn teriam sido de última geração anos atrás, mas que haviam feito pouco para acompanhar e proteger-se da onda de violações de dados dos últimos dois anos. O LinkedIn não deve apenas atualizar sua segurança para os padrões mais modernos, mas também deve adotar a mentalidade de que a proteção dos dados do consumidor é um esforço contínuo, e não apenas um único evento de correção.

Fontes: Christa Joe, "Battling the Security Problem on Social Media", Ezine Articles, acesso em: 23 jul. 2013; "Top 10 Social Media Security Problems in 2013", *Social Media Revolver*, 23 mai. 2013; Jessi Hempel, "Everything You Need to Know about LinkedIn", *Fortune*, 1 jul. 2013; "LinkedIn Faces $5 Million Lawsuit After Password Breach", *CIO Insight*, 22 jun. 2012; "LinkedIn Defends Reaction in Wake of Password Theft", *The Wall Street Journal*, 10 jun. 2012; "Lax Security at LinkedIn Is Laid Bare", *The New York Times*, 10 jun. 2012; "Why ID Thieves Love Social Media", *Marketwatch*, 25 mar. 2012.

Os problemas causados pelo roubo de 6,5 milhões de senhas do LinkedIn ilustram algumas das razões pelas quais as empresas precisam prestar uma atenção especial para a segurança dos sistemas de informação. O LinkedIn oferece benefícios importantes tanto para os indivíduos quanto para as empresas, mas, do ponto de vista de segurança, ele não protegeu suficientemente seu site dos hackers, que foram capazes de roubar informações confidenciais do usuário.

O diagrama de abertura chama a atenção para pontos importantes levantados por esse caso e por este capítulo. Embora a administração do LinkedIn tenha alguns procedimentos e tecnologia de segurança em vigor, ela não tem feito o suficiente para proteger os dados dos usuários. Ela não usou técnicas de criptografia de senha padrão, incluindo o *salting*, para proteger as senhas dos usuários.

A natureza "social" desse site e o grande número de usuários o tornam extremamente atraente para os criminosos e hackers que têm a intenção de roubar informações pessoais e financeiras valiosas e propagar software malicioso. Por conta da grande base de usuários e da natureza social do site, a administração não fez o suficiente para proteger os dados do LinkedIn. Os fiéis usuários do LinkedIn impediram que as consequências da violação fossem muito maiores, e a maioria das pessoas decidiu que deveria permanecer no site, porque isso era muito valioso para suas carreiras. No entanto, a empresa enfrenta uma ação multimilionária, bem como danos à reputação. Para todas as empresas, a lição é clara: a dificuldade de erradicar software malicioso ou reparar danos causados por roubo de identidade aumentam os custos operacionais e tornam tanto os indivíduos quanto as empresas menos eficazes.

A seguir, estão algumas perguntas para refletir: quais fatores gerenciais, organizacionais e tecnológicos contribuíram para a violação dos dados do LinkedIn? Qual foi o impacto empresarial da violação de dados?