Vazamento de dados pessoais de 100 milhões de contas de celular. O que você precisa saber?

Quais dados vazados?

O vazamento expõe contas telefônicas e segundo a Psafe estavam disponíveis na Dark Web desde o dia 03 de fevereiro e envolvem informações como CPF, número de celular, tipo de conta telefônica, minutos gastos em ligação e demais dados pessoais. São 102.828.814 mil registros. Ao que parece pertencem as operadoras Claro e Vivo, mas é preciso investigação para se confirmar pois as empresas negam a responsabilidade.

Qual a motivação?

A motivação ao que identificado é financeira. Já que as informações estão sendo vendidas individualmente ou em pacotes, no valor de U$$ 1 cada.

As pessoas devem se preocupar?

As pessoas precisam se preocupar com vazamentos desta natureza, pois eles podem ser utilizados para criação de cadastros, falsa identidade, compras, aplicações de golpes e fraudes e até por tentativas de acessar contas bancárias e ativos das vítimas. É muito importante ficar atento a mensagens não solicitadas recebidas e caso receba abordagens de pessoas ou empresas que desconhece, questionar como o agente obteve os dados. Lembrando que nos termos da LGPD é direito do titular de dados confirmar a existência de tratamento, acessar os dados e até mesmo a eliminação dos dados tratados em desconformidade com a Lei.

Os cidadãos tem culpa?

Não. Os usuários não têm culpa alguma. Um dataset gigante com 100 milhões de registros, certamente veio de um agente de tratamento, este que pode ter negligenciado com seus deveres relativos à segurança da informação e proteção de dados. Lembrando que pela LGPD o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes. Assim, a ANPD precisa investigar adequadamente o caso. Conforme dispõe a LGPD, responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que deixa de adotar as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Como a Autoridade Nacional de Proteção de Dados (ANP) pode agir?

Compete à ANPD fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso. Neste caso, a ANPD poderá instaurar um procedimento administrativo para apurar a responsabilidade dos agentes de tratamento que seriam responsáveis pela base de dados. Embora as penas só possam ser aplicadas em agosto de 2021, nada impede, no entanto, que outras entidades atuem, como Procon, Senacon e até mesmo o Ministério Público, que tem se mostrado muito ativo nas questões envolvendo vazamento de dados pessoais.

Se comprovado, as empresas de telefonia respondem pelos danos?

Conforme dispõe a LGPD, responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador

que, ao deixar de adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Assim, as responsáveis poderão ser processadas por entidades de defesa do consumidor, associações de representação e Ministério Público, caso comprovada a negligência que permitiu o vazamento de dados. A ANPD também divulgou nota informando que oficiou outros órgãos, já que ainda não pode aplicar suas penalidades, e que promoverá, com estes órgãos competentes, a responsabilização e punição dos envolvidos. Procon e Anatel também estariam habilitadas a atuar nestes casos. O Procon poderia inclusive aplicar multa com base no Código de Defesa do Consumidor. Acreditamos que nestes casos a prova pericial em dados será fundamental para apurar se realmente os dados se originaram de vazamentos das operadoras de telefonia ou não.

Em síntese

Com a LGPD e o aumento da maturidade e consciência em relação à privacidade e proteção de dados, ganha relevância maior notícias de vazamento de dados. Por outro lado, nos últimos dois casos grandes no Brasil, os suspeitos negaram o envolvimento. Assim, a questão será probatória e técnica, sendo necessárias auditorias e perícias em informática para que, no processo administrativo, fique comprovado ou não o envolvimento.

José Antonio Milagre, advogado e perito em segurança da informação e dados pessoais, especialista em crimes cibernéticos e Presidente do Instituto de Defesa do Cidadão na Internet (IDCI Brasil).

Segurança em dois passos?

Nada mais é do que o aprimoramento da segurança tradicional, onde além da senha comum, exige-se outro código. Ou seja, uma camada extra de segurança Mesmo com uma senha fraca, tem-se uma camada de proteção adicional contra crackers. É muito comum você digitar uma senha e o sistema lhe enviar um código para algo que você tenha (um de seus dispositivos celulares, por exemplo).

Outra forma "ainda que relativizada" da segurança dois passos reside nos casos em que o usuário tem registrado seu navegador do computador que usa, sendo que qualquer acesso de outro navegador não será permitido ou exigirá a digitação de um código adicional.

O princípio está relacionado a ideia de que sistemas de autenticação funcionam com confirmação não só de algo que você sabe, mas de algo que você tem ou mesmo, algo que você é… Estes são os fatores de autenticação.

Segundo fator, hoje, é checar algo que você tem! Logins comuns checam apenas o que você sabe e muitas pessoas podem saber o que você sabe…

Algumas empresas que já implementaram a segurança em dois passos são:Apple, Google, Twitter (liberado em maio de 2013), Evernote, Microsoft, Dropbox…

É uma ótima solução contra ataques de pishing. E o exemplo clássico vem dos cartões de banco. Não basta a senha para uma transação bancária, é necessário ou usar um PIN, TOKEN, Cartão com letras ou ainda senha de letras previamente cadastrada. Ou seja, se dificultamos a atuação do criminoso bancário, temos hoje possibilidade de dificultar a atuação de crackers que querem violar nossa privacidade.

Lembrando que nos termos da Lei 12.737/2012 a invasão de

dispositivo informático, mediante violação de mecanismo de segurança, pode configurar crime previsto no art. 154-A, com pena que pode chegar até dois anos de reclusão. Quanto mais caracterizarmos a presença de mecanismos em nossos ativos, menos risco corremos de não sermos protegidos pela Legislação.

O Brasil, inteligência, e o custo do vazamento das informações governamentais

Não é de hoje que sabemos sobre certos episódios envolvendo espionagem, vazamento de informações e crime organizado dentro do setor público brasileiro. Com a tecnologia da informação, as formas de coleta indevida e difusão das informações facilitaram os crimes digitais, associado ao fato da ignorância de muitos servidores públicos na proteção das informações, a despeito das estruturações e títulos na área de segurança da informação.

Longe dos pomposos e não tão eficientes órgãos de segurança e inteligência do Governo Federal e dos Estados ricos da Federação, encontramos Estados, Prefeituras e orgãos manipulando informações sensíveis, diga-se, matéria prima para fraudes e golpes, sem qualquer proteção. São dados de concursos, de segurança, arrecadação, licitações, contratos, convênios, planilhas, imóveis a serem leiloados e outras informações aptas a serem exploradas para a fraude ou exploração ilícita. O resultado é previsível.

Não bastasse, sites institucionais hospedados em estruturas precárias ou servidores absolutamente mal configurados ou blindados em face da atuação do crime eletrônico. Como

resultado, a recente indisponibilização do site da Presidência da República **[1]**, por meio de um ataque de negação de serviço (DDOS), atribuído a um grupo denominado "Fatal Crew Error".

No Brasil, o gabinete de segurança institucional apresenta relatos de falhas, como no caso das câmeras do Palácio do Planalto, que não registraram as placas dos veículos que estiveram por lá no início de 2009 **[2]**. Na previdência, a fraude chega a 1,6 bilhões de reais, e conta com uso indevido de informações do sistema de óbito de segurados, o SISOB, bem como outras técnicas de uso indevido de dados, o que faz do país um dos que mais possuem "mortos-vivos" do mundo em termos previdenciários.**[3]** Estamos também entre os campeões de "empresas-fantasma", aptas a abocanhar licitações do norte a sul do país.

A própria Polícia Federal tem sua conduta questionada, no que cerne ao vazamento de informações de inquéritos e outros procedimentos, para a imprensa, televisões e outros privilegiados, o que gerou a indignação do ministro do Supremo Tribunal Federal, Gilmar Mendes, também em 2009 **[4]**, e que também motivou o pacotão da segurança pública que pretende suspender e até demitir o agente que se manifestar sobre investigação que participe ou tenha conhecimento.

No centro de São Paulo, é possível comprar senhas para o maior banco de dados da segurança pública do Brasil, o InfoSeg **[5]**, a custo irrisório de 2 mil reais, como já noticiado na mídia brasileira.

Outros entes públicos de nível federal, estadual e municipal já experimentaram a fraude resultado da associação entre maus servidores e particulares bandidos. A epidemia não é só pública, já que estima-se que no Brasil boa parte dos negócios fechados no mercado financeiro tenham como suporte o vazamento de informações**[6]**.

O que o vazamento de informações causa? Dano e desfalque ao

erário. Tomemos o exemplo do vazamento de informações que prejudicou uma operação policial no Rio de Janeiro, em 2007, nas favelas do Complexo São Carlos, no Estácio, onde a Polícia pretendia prender 100 pessoas. Um homem foi preso**.[7]**

Outro exemplo, o vazamento das provas do ENEM em 2009**[8]**. 500 mil reais era o que o funcionário da gráfica contratada pelo Ministério da Educação queria para fornecer as informações ao Jornal "O Estado de São Paulo". Resultado? O sabido cancelamento da prova, ato que custou nada menos que 30 milhões ao Governo. De observar, a reincidência veio em 2010, com mais um vazamento de dados das provas do ENEM.

Mais um exemplo, a venda dos caças ao Governo Brasileiro, fato amplamente noticiado em 2009, onde a despeito do termo de confidencialidade estabelecido pela Força Aérea Brasileira (FAB), ficou claro o vazamento de informações sobre o preço ofertado pela francesa Dassault **[9]**.

No Brasil, a Lei 9883/99 institui o Sistema Brasileiro de Inteligência, no âmbito federal, e cria a ABIN. Este sistema é responsável pela coleta e custódia de informações para servir ao Presidente da República em suas decisões. Todos os entes públicos que manipulam informações de interesse nacional compõem o SBI e estão sujeitos ao controle da ABIN. Ora, se existe permissivo legal para o monitoramento e auditoria, porque tantos escândalos?

Não bastasse, sabemos que fora do executivo federal, órgãos públicos municipais e estaduais ainda não atentaram para o risco da negligencia, imprudência ou imperícia na manipulação de informações confidenciais. O Código Penal brasileiro prevê em seu artigo 325 o crime de violação de sigilo funcional também para quem permite ou facilita o acesso de terceiros a sistemas de informações da administração pública, estabelecendo ainda uma pena de reclusão que pode chegar de 2 a 6 anos e multa. Ou seja, ser negligente com sistemas informáticos, na administração pública, é crime!

Já se o funcionário público é quem insere ou altera os dados nos sistemas da administração, pode responder pelo peculato informático, dependendo das circunstâncias, será enquadrado nos arts. 313-A e 313-B do Código Penal, com pena que pode chegar a 12 anos de reclusão.

Mas só punição adianta? Efetivamente que não, eis que como verificamos, o peculato informático foi criado em 2000 e nem por isto desestimulou o vazamento de informações públicas e pelo contrário, hoje são os particulares que praticam o crime de exploração de prestígio, ao se valerem das relações com funcionários públicos maléficos, na obtenção de vantagens.

A resposta é a efetiva gestão de segurança da informação, com a implementação de um sistema eficaz e que considere pessoas acima de ferramentas e softwares e leve em consideração que influências internas são as principais responsáveis pelo vazamento de dados na área pública e também privada. Uma pesquisa mais refinada no Google e descobrimos quantos servidores utilizam e-mails do governo para usos privados. Mais, sabemos de casos em que o servidor foi desligado e anos depois ainda detinha privilégios de acesso à rede VPN governamental, agenciando tais informações à seu critério. Documentos privados circulam na internet com timbres oficiais, e que podem ser utilizados por estelionatários para confecção de falsos documentos e aplicação de golpes.

Dados não são validados quanto ingressam nas bases da administração, acordos de confidencialidade não são cumpridos, funcionários não são conscientizados dos riscos, não existem perímetros físicos de proteção de ativos, funções não são segregadas e o pior, em alguns órgãos os gestores públicos sequer sabem quais os ativos informacionais são importantes para a empresa pública, e o quanto devem se esforçar para protegê-los.

Estas, são apenas algumas posturas inerentes à ausência de um sistema de gestão que preze pelos fundamentos da segurança:

integridade, disponibilidade e confidencialidade de dados, e principalmente, que seja testado e avaliado periodicamente, por meio de testes de intrusão, engenharia social e outras técnicas homologadas e válidas em segurança da informação.

Se você questionar a um gestor de segurança de um órgão público se ele tem uma ferramenta firewall licitada funcionando em sua área o mesmo afirmará que sim. Agora experimente questionar se ele tem uma política de gestão de continuidade do negócio, ou se adota gestão da segurança no desenvolvimento e suporte de seus sistemas, ou ainda se desenvolveu uma célula de forense digital vinculada a seu time de resposta a incidentes…

As proteções contra vazamentos devem ser objeto de avaliação periódica e a inteligência é fundamental neste ponto. Não acabaremos com o vazamento de informações públicas licitando firewalls, software de segurança e detectores de intrusão, mas aliando a rigorosa legislação brasileira já existente, com técnicas de monitoramento e screening dos funcionários públicos que lidam com informações críticas. A inteligência não deve estar só no âmbito federal, e principalmente, deve sair do papel e ser aplicada. Aquele que manipula informações públicas sensíveis deve estar ciente de que dada a responsabilidade que detém, pode ser auditado, sem que possa evocar a proteção conferida a um cidadão comum, no que tange à privacidade.

Tomemos o exemplo de Portugal onde o Serviço de Informações da República (SIS) e o Serviço de Informações Estratégias, em 2009, assinaram protocolos para a inserção de espiões nos serviços públicos. Mas qual a finalidade desta medida? Simples, combater a criminalidade organizada dentro do Governo, esta, que se vale de informações confidenciais e privilegiadas para movimentar um mercado negro de milhões de euros.

Aqui não é diferente.

No Brasil, algumas iniciativas ainda engatinham, mas servem de exemplo para todos os órgãos públicos da Federação, como o projeto de Lei que dispõe sobre o regime disciplinar do Departamento da Polícia Federal e da Polícia Civil do Distrito Federal**[10]**, que institui a chamada "sindicância patrimonial", destinada a averiguar e identificar servidores que ostentam patrimônio imensamente maior do que o compatível com a função. São medidas que podem auxiliar a redução dos crimes envolvendo vazamento de informações eis que quem tem acesso a informações sigilosas governamentais, com certeza não as cede gratuitamente.

Enfim, demonstramos que o vazamento de informações na administração pública em todas as suas esferas é realidade, motivada e impulsionada pelo vantajoso e lucrativo tráfico de informações e principalmente pela ausência de monitoramento dos ativos de tecnologia da informação e seus respectivos suportes. Igualmente, concluímos que não existe uma solução pacífica e incontroversa para amenização desta patologia, porém sabemos que esta solução passa longe da compra e mais compra de softwares e dispositivos de segurança, e que um caminho pode ser a aplicação da lei, em cotejo com a fiscalização e testes de intrusão para avaliar condutas dolosas e culposas, perícia digital para identificar a autoria de incidentes, além do monitoramento de ex-agentes e a chamada sindicância patrimonial.

Resta pacífico que serviços de inteligência em sua gênese são concebidos no escopo de apoiar a tomada de decisões governamentais, e mais que isso, de proteger ativos das ameaças, sobretudo digitais, antecipando problemas e identificando causadores. Porém, mais claro ainda, fica demonstrado que sem governança, análise de risco, conformidade e monitoramento constante, tais serviços podem se voltar contra o Estado e seus cidadãos, servindo, por ação ou omissão, interesses escusos e criminosos, de sabida alta lucratividade.

NOTAS:

[1] http://www.24horasnews.com.br/index.php?mat=354842

[2] http://www1.folha.uol.com.br/folha/brasil/ult96u613407.shtml

[3] http://montesclaros.com/noticias.asp?codigo=47003

[4] http://www.parana-online.com.br/editoria/politica/news/399422/?noticia=MENDES+COBRA+GOVERNO+POR+VAZAMENTO+SELETIVO+DE+DADOS

[5] http://www.youtube.com/watch?v=HA6Jpni03bE

[6] http://aeinvestimentos.limao.com.br/financas/fin38558.shtm

[7] http://ultimosegundo.ig.com.br/brasil/2008/07/22/policiais_civis_fazem_mega_operacao_no_rio_de_janeiro_1460079.html

[8] http://g1.globo.com/vestibular-e-educacao/noticia/2010/08/vazamento-de-dados-de-estudantes-do-enem-sera-apurado-diz-inep.html

[9] http://www.jusbrasil.com.br/politica/4112808/dassault-critica-concorrencia-por-vazamento-de-informacoes-e-nega-preco-40-maior

[10] http://www.google.com.br/url?sa=t&source=web&cd=1&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.sinpoldf.com.br%2Fsitenew%2Favisos%2Fimg%2Fpl1952-07.pdf&rct=j&q=disp%C3%B5e%20sobre%20o%20regime%20disciplinar%20do%20Departamento%20da%20Pol%C3%ADcia%20Federal%20e%20da%20Pol%C3%ADcia%20Civil%20do%20Distrito%20Federal%20sindic%C3%A2ncia%20patrimonial&ei=jE0lTYiFCoKKlwe23oS3AQ&usg=AFQjCNGVEGkEEKMzqx_XKA0F-GQH9HIUYQ&cad=rja