



CLOUD **COMPUTING** Hotsite especial do Convergência Digital



Segurança na nuvem: portais não se adequam à padrão mundial

Convergência Digital
Convergência Digital - 09/06/2014

Um estudo realizado com 40 grandes portais brasileiros para verificar se possuem vulnerabilidades já conhecidas, expondo os portais à ataques de hackers, chegou a um resultado preocupante: no geral, 72,5% deles estão vulneráveis e, entre os sites governamentais, há risco de captura de dados por meio de técnica conhecida como injeção de código ou por falta de criptografia na transmissão de dados, revela a ADTSys, empresa especializada em segurança da informação, com sede em Campinas.

"O grande dilema de muitas empresas para mudarem seus ambientes para nuvem hoje é estarem seguras e é importante reforçar que a segurança existe no cloud computing, desde que se sigam os padrões e normas já definidos para isso. O problema é que hoje, no Brasil, essa metodologia na maioria dos casos não está sendo colocada em prática. É preciso rever isso com urgência", diz Pascoal Baldasso, diretor executivo da ADTSys.

O levantamento - feito por especialistas da ADTSys - foi realizado em um período de três meses, nos quais foram verificados 40 portais nas áreas governamental, e-commerce, corporativos e de times de futebol. Na área governamental foram verificados prefeituras de cidades, em sua maioria capitais, de dez diferentes estados. Em e-commerce, foram dez empresas que trabalham nacionalmente nas áreas de venda de livros, lojas de departamentos, eletroeletrônicos, vendas gerais e hipermercados. Os sites corporativos incluem empresas de grande porte na área automobilística, agronegócios, aviação, eletroeletrônicos, investimentos, energia, tecnologia e até mesmo desenvolvimento de computadores e softwares - apenas um portal desta última área mostrou-se totalmente invulnerável.

Por fim, entre os times de futebol foram testados os portais de quatro times paulistas (entre os quais três dos chamados "grandes" do estado de São Paulo) e equipes do Rio de Janeiro, Santa Catarina, Minas Gerais e Rio Grande do Norte. "Simulamos a navegação nestes sites através de ferramentas específicas que enviam códigos prontos, conhecidos como assinaturas. As assinaturas servem para identificar se aquele portal possui ou não uma determinada vulnerabilidade conhecida. Nenhum acesso sem autorização ou alteração de dados foi executado. Na maioria dos casos, infelizmente, a resposta foi positiva", explica Diego Altheman, diretor de novas soluções da ADTSys e um dos responsáveis pelos testes.

Altheman conta que no estudo as vulnerabilidades foram classificadas basicamente em dois grupos: as oriundas de desenvolvimento - que incluem, por exemplo, a escrita de códigos vulneráveis - e as de infraestrutura, onde são computadas ações que até deveriam ser de simples execução, como a atualização de softwares e componentes de segurança. Nos sites de e-commerce, também foi verificado o PCI, norma criada pelas operadoras de cartões de crédito Visa e Mastercard com o objetivo de reduzir o risco operacional envolvendo transações com cartões de crédito. Neste campo, uma notícia mais tranquilizadora: o índice de vulnerabilidade ficou em apenas 10%.

Por outro lado, a ADTSys averiguou que nenhum dos sites está completamente dentro dos padrões recomendados pela Open Web Application Security Project (OWASP), entidade sem fins lucrativos e de reconhecimento internacional que contribui para a melhoria da segurança de aplicativos reunindo informações importantes que permitem avaliar riscos de segurança e combater formas de ataques através da internet. "A OWASP gera uma lista anual com os principais dez problemas de segurança de desenvolvimento. São critérios divulgados publicamente e vulnerabilidades amplamente conhecidas pela comunidade de tecnologia, problemas que são catalogados e que estão sendo ignorados no Brasil, gerando riscos totalmente desnecessários", lamenta Altheman.

Casa sem portão

Na área de desenvolvimento, foram testados diversos tipos de vulnerabilidades possíveis (injeção de código, quebra de autenticação; XSS; referência insegura e diretas de objetos, controle de acesso; falsificação de solicitação entre sites). "Os índices de vulnerabilidade em desenvolvimento são preocupantes. Pelo método de injeção, por exemplo, seria possível atingir 90% dos sites governamentais, 80% dos de futebol e 60% dos de e-commerce e corporativos. Na prática, o hacker pode injetar dados e códigos naquele portal e, em casos extremos, capturar dados de todos", diz Diego Altheman dos Santos.

Na área de infraestrutura - usar componentes com vulnerabilidades conhecidas, configuração incorreta de segurança, dados sensíveis expostos - há dados igualmente alarmantes. "Não há atualização dos sistemas operacionais e servidores de aplicação por exemplo. Para fazer uma analogia, imagine uma pessoa que usa por exemplo um sistema Windows, que tem um programa de update que



DESTAQUES

Mercado de nuvem para PMEs deve passar de R\$ 20 bilhões

Estudo revela, porém, que apenas 3% das pequenas e médias empresas do Brasil já adotaram plenamente soluções de computação em nuvem.



Cloud massifica, mas sem estratégia definida pelas empresas

Empresas têm obstáculos a superar para tirar o real valor do uso da nuvem nos negócios. Nuvem híbrida é a opção preferencial.



VÍDEOS



Aprender usar os Dados Abertos é lição de casa para os Governos



PRODERJ vai para a nuvem e quer ser broker de serviços

Veja mais vídeos

OPINIÃO



De Byte a Yottabyte em muito pouco tempo...

Por Wilson Grava*

O Big data impulsiona os negócios, mas tem riscos. Eles passam pelo uso inadequado, pelas violações e perda de dados até a preocupação do usuário final com a privacidade e segurança desses dados.



Mitos e verdades sobre ERPs em nuvem

Por Grasiela Tesser*

Ainda que Cloud Computing esteja se popularizando e sendo cada vez mais natural nas operações das empresas, muitas companhias ainda relutam em utilizar sistemas de gestão - os ERPs - na nuvem. É o medo da inovação.



atualiza as falhas já encontradas, de maneira automática ou com autorização do usuário. As empresas não atualizam. São vulnerabilidades conhecidas, uma simples atualização resolveria", afirma Altheman.

Ele ressalta que ter uma vulnerabilidade não significa que o site obrigatoriamente vai ser invadido. "Eventualmente isso pode gerar um bug, por exemplo, uma tela de erro. Mas com certeza o risco de sucumbir a uma tentativa de ataque é maior. Um hacker explora a falta de atualização da infraestrutura e não seguir padrões de segurança facilita a vida dele, diminui o tempo de invasão. Ter infraestrutura desatualizada, inadequada aos dados, não é sinônimo de invasão, mas é, sim, um alto risco desnecessário: é como ter uma casa sem portão em uma cidade com grandes índices de roubo e furto à residência."

Ainda na parte de infraestrutura, a ADTsys detectou, entre outros problemas, configurações incorretas de segurança e falta de atualização de frameworks, por exemplo. "Outra questão que preocupa é a exposição de dados sensíveis. Em vez de estarem protegidos por criptografia, por exemplo, são transmitidos sem nenhuma proteção, podendo ser capturados de forma fácil. Em um site de um time de futebol, por exemplo, por meio de uma técnica chamada sniffer são facilmente interceptados os dados de autenticação (usuário e senha) fornecidos para acessar as áreas restritas do portal."

Na opinião de Pascoal Baldasso, diretor executivo da ADTsys, mais do que mostrar inseguranças que podem – e devem – ser solucionadas, o levantamento feito pela empresa deixa claro que o Brasil precisa ter uma maior consciência do que é segurança em termos de cloud computing. "Fica claro que o Brasil ainda está engatinhando e precisa ter mais maturidade nesta área, pois não tem o hábito de seguir padrões de segurança mundiais. Nenhum portal pesquisado se adequar ao padrão Owasp é um termômetro desta situação preocupante, que mostra que de maneira geral o país não está dando atenção devida à segurança na nuvem", conclui.

Fonte: ADTsys



LEIA TAMBÉM:

Cloud Computing ... 09/06/2014

Segurança na nuvem: portais não se adequam à padrão mundial

Cloud Computing ... 10/06/2013

Privacidade: Em março, agência dos EUA coletou 97 bilhões de dados

Cloud Computing ... 25/02/2013

Violação de dados: gestores de TI confessam erro na estratégia

Cloud Computing ... 17/10/2012

Segurança: Apenas 15% dos CIOs sabem o que querem no Brasil

Negócios ... 27/06/2012

Nuvem e tablets em alta, mas Segurança é minimizada nas corporações

Cloud Computing ... 14/02/2012

Nuvem pública ganha diretrizes de segurança

Cloud Computing ... 19/07/2016

Compartilhamento de senhas para serviços na nuvem chega a 58% nas empresas



Copyright © 2005-2016 Convergência Digital ... Todos os direitos reservados ... É proibida a reprodução total ou parcial do conteúdo deste site