'Apps' e APIs geram desafios para segurança de redes sociais
Altieres Rohr

Recurso permite que programadores interajam com o site. Ao mesmo tempo, permite abusos de segurança e privacidade.

Jogos como Colheita Feliz e FarmVille são apenas exemplos do universo de recursos adicionais para redes sociais – ou "apps", como são mais reconhecidos. O que diferente um app do restante dos recursos da rede é que ele é normalmente desenvolvido por um terceiro, sem ligação com a rede social. Isso significa que a rede social e também o usuário devem confiar no aplicativo. Porém, confiança é às vezes a última coisa que eles merecem.

Reprodução

Número de Apps no Orkut se aproxima de 17 mil.

Problemas

O Orkut teve um problema recente com um app que redirecionava usuários para páginas de login falsas. Quem adicionava o recurso ao perfil – buscando assistir TV no computador, segundo a promessa do app - não percebia o redirecionamento. Os visitantes, porém, eram imediatamente levados à página falsa. Quem forneceu suas credenciais de acesso correu o risco de ter sua conta completamente comprometida e usada, por exemplo, para a disseminação de vírus.

O comportamento indevido demorou a ser notado. Mesmo depois de o caso vir a público, o app ficou mais uma semana disponível aos usuários.

O caso levou o Google a prometer melhorar seu processo de revisão. Antes de serem incluídos na rede social, cada app é revisado. Por algum, porém, a revisão não identificou o problema.

Mas a revisão não elimina todas as formas de ataque. Existe o risco de um desenvolvedor ter seu servidor comprometido e imediatamente código malicioso aparecer em milhares de perfis na rede social. Até o momento, não se tem registro de que isso tenha acontecido, mas é um cenário bem possível considerando a tendência de ataques a sites legítimos.

Os apps ficam interligados com a rede social por meio da Application Programming Interface (API), ou "interface de programação de aplicativos". Basicamente, é um canal de comunicação pelo qual o app e o site trocam informações na mesma língua. Alguns erros podem existir na própria API e serem de responsabilidade do site. Outros podem existir na maneira que os

desenvolvedores usam essa API; usando como analogia a língua, é usar as palavras erradas ou entender errado o que o site está dizendo, gerando erros de comunicação.

O Twitter teve muitos problemas com isso. Um pesquisador chegou a divulgar pelo menos uma falha por dia durante um mês em aplicativos que se baseavam no Twitter. Para diminuir o impacto de erros desse tipo, o site criou novas maneiras de interação dos aplicativos para com o site. Agora não é mais necessário, por exemplo, fornecer sempre a senha.

O Facebook também teve problemas com apps recentemente. Alguns desenvolvedores estavam coletando dados sem autorização do site. O Facebook prometeu mudar sua API de modo a reduzir as informações sensíveis que passam desnecessariamente pelos apps e punir os programadores que violaram suas regras.

Divulgação

Farmville, um dos aplicativos mais famosos do Facebook.

Redes sociais têm vantagem no combate aos ataques

No combate aos hackers, as redes sociais tem uma vantagem muito grande. Isso porque elas controlam tudo: a interação dos apps com o site, o perfil dos usuários e quaisquer outros comportamentos, como envio de mensagens, abertura e transferência de comunidades ou quaisquer ações realizadas. Uma rede social pode ser “inteligente” para perceber o que há de errado.

“Nós desenvolvemos sistemas complexos e automatizados que detectam e marcam contas do Facebook que podem estar comprometidas com base em atividade incomum, como o envio de muitas mensagens em um curto período de tempo, ou mensagens com links que sabemos que são maliciosos”, explica Simon Axten, gerente de privacidade e política pública do Facebook. Mensagens que o site detecta como sendo maliciosas são apagadas das caixas de todos os seus receptores, explica Axten, graças à vantagem que o Facebook tem por controlar os dois lados da comunicação.

Essa vantagem não existe, por exemplo, no e-mail, que trava uma luta sem fim contra o spam.

É verdade, portanto, que as redes sociais não têm motivo para serem tão anárquicas. Pelo contrário: os desenvolvedores têm o controle total sobre tudo o que acontece. É difícil achar justificativas que expliquem por que alguns ataques se repetem – como as comunidades no Orkut que roubam as credenciais de acesso.

Embora os apps deem algum controle sobre a rede social para um terceiro, o site ainda pode deter o canal de comunicação e integração dele com a rede. É perfeitamente possível criar

mecanismos que detectem atividade maliciosa e meios seguros de colocarem esses apps na rede.

Ainda assim, é de se esperar novos ataques envolvendo apps. Portanto, fique atento para apps maliciosos, que normalmente vão ter promessas mirabolantes, e pesquise antes de incluir um recurso adicional no seu perfil.

Fonte: G1, 15 nov. 2010. [Portal]. Disponível em: <http://g1.globo.com>. Acesso em: 17 nov. 2010.