Vulnerabilidades de segurança devem ser noticiadas

10/07/2002

Os usuários finais estão apoiando, de maneira preponderante, a revelação (*full disclosure*) das vulnerabilidades e defeitos dos programas e sistemas, o que demonstra uma freqüente frustração com o retorno dos fornecedores ao se falar em segurança.

Com base em entrevistas com mais de 300 profissionais de segurança de software, o relatório do Hurwitz Group explica que os usuários finais apóiam de maneira decisiva a 'obrigação de informar' – as vulnerabilidades de segurança devem ser comunicadas assim que forem descobertas. Na análise, os usuários finais estão nitidamente aborrecidos com os fornecedores que estão liberando aplicações inseguras, e então não respondem quando as falhas são detectadas, relata a Hurwtiz. "Eles vêem a 'obrigação de informar', em fóruns públicos e na imprensa, como a única maneira de forçar os fornecedores a responder pelas vulnerabilidades causadas por códigos mal-escritos e inseguros. Na verdade, os usuários finais apóiam decisivamente o *full disclosure* – obrigação de dar conta – mesmo que isto signifique a exposição de falhas de segurança dentro das organizações, algo que poderia ter um impacto negativo nas empresas".

A pesquisa mostra também que a maioria dos usuários finais deseja que a informação seja divulgada, e muitos querem que seja divulgada imediatamente. Dos entrevistados, 39% disseram que as vulnerabilidades devem ser divulgadas assim que descobertas, e outros 28%, dentro de, no máximo, uma semana.

O estudo questiona as tentativas dos fornecedores, mais notadamente a Microsoft, de criar uma carta patente para a "divulgação responsável" (*responsible disclosure*) das informações sobre vulnerabilidades de segurança, que poderia restringir a liberação de informações sobre erros de programação (*bugs*). De acordo com esta linha de pensamento, a divulgação deveria ser adiada por até 30 dias, tempo suficiente para o desenvolvimento de um "remendo" (*patch*) adequado a cada sistema.

As discussões abertas sobre as façanhas (*exploits*) resultantes de erros de software estão conduzindo a uma "anarquia da segurança" e minando a informação da Internet, de acordo com a Microsoft. Mas de cada quatro profissionais de segurança de software, três discordam disso, Hurwitz descobriu.

O estudo indica uma frustração crescente dos usuários a respeito de problemas de segurança – e da qualidade geral – dos programas de computador. Os usuários acabarão por procurar a lei em busca da punição dos fornecedores por estes problemas de software, sugere Hurwitz.

No passado, os usuários finais tinham opções jurídicas limitadas, pois as leis sobre a responsabilidade do produto protegiam os fornecedores, mas isto poderá acabar logo. "As empresas estão tão irritadas que agora estão querendo levar os fornecedores a juízo," disse

Pete Lindstrom, diretor de estratégias de segurança do Hurwitz Group. “Eu acho que logo veremos ‘ações-teste’ nos tribunais tentando encontrar padrões e impôr exigências aos fornecedores. Será interessante ver se esses casos serão bem-sucedidos, e se esses padrões resolverão, finalmente, o problema dos usuários finais.”

As informações são do site britânico The Register (8/7).

(Nota do editor: vide arts. 8º, 12, 23, 25, 31, 51, entre outros da Lei nº 8.078/90 – Código de Defesa do Consumidor)