A F-Secure anuncia que mais de 70% das empresas continuam vulneráveis a ataques por não atualizarem seu software. Trata-se de uma descoberta surpreendente, tendo em vista a disponibilidade de soluções de segurança para controlar e administrar a atualização de software nos dispositivos de uma organização.

Um recente alerta do United States Computer Emergency Readiness Team adverte que até 85% dos ataques focados podem ser evitados seguindo-se precauções simples de segurança. É essencial manter o software atualizado com as mais recentes correções de segurança.

Ainda assim, muitas empresas continuam a negligenciar a importância e o valor de atualizar seu programa. Uma enquete da F-Secure descobriu que apenas 27% das companhias possuem uma solução para gestão de correções. O problema foi particularmente evidente na França, onde apenas 15% dos entrevistados disseram que suas empresas tinham uma ferramenta para gestão de atualizações de software. Por outro lado, 46% das empresas nórdicas possuíam uma tecnologias para gerenciamento de patches, o que as deixava mais bem preparadas para proteger os ativos da empresa contra ameaças projetadas para tirar vantagem de vulnerabilidades de software.

Segundo Vitor Vianna, Sales Engineer da F-Secure para América Latina, a relutância das empresas em se empenharem na atualização de programas mostra quão desvinculadas do atual panorama de ameaças algumas organizações estão. “Muitas pessoas sentem que atualizar o software é apenas um trabalho extra que pode prejudicar o funcionamento de aplicações, entre outros problemas – a verdade, porém, é o oposto disso. Os criminosos contam com que as pessoas ignorem as correções de segurança; por isso, se empenham em desenvolver exploits voltados às vulnerabilidades expostas por esses patches. É comum que eles executem seus ataques antes de as pessoas instalarem a atualização; dessa maneira, o que se tem é toda uma estratégia de ataque que depende do uso de software não corrigido.”

O F-Secure Labs relatou um crescimento de 82% nos exploits focados em vulnerabilidade baseada no Flash, revelada após o roubo de dados pelo Hacking Team no último mês de julho. Vianna disse que são picos de atividade como esse o que faz com que os exploits constituam preocupações estratégicas de segurança e seja tão importante a atualização imediata e diligente do software.

Fonte: Risk Report, em 29.09.2015.