Inzwischen gibt es erste Analysen des durch Hacker veröffentlichten Quellcodes von Norton's pcAnywhere. Die Erkenntnisse dürften eins zu eins auf die anderen Produkte übertragbar sein, deren Quellcode ebenfalls entwendet, aber anscheinend noch nicht für jedermann verfügbar gemacht wurde.

> „Any exploits in the code are now visible by all. The only hope for Symantec and PCAnywhere is that these days, users typically do not run their home or office computers with the ports required for this product open to the internet. So attacks for this particular product across the internet are minimal. However, hackers always seem to find a way."

So ein Analyst, der sich den entwendeten Quellcode von pcAnywhere angesehen hat.

> Frei übersetzt: Alle Lücken sind jetzt für jeden im Code sichtbar. Die einzige Hoffnung für Symantec und pcAnywhere in diesen Tagen ist, dass die Anwender ihre Rechner im Büro und zu Hause nicht nutzen. Die Gefahr eines Angriffs via Internet wäre dann minimal. Allerdings finden Hacker immer einen Weg.

Symantec beschwichtigt und gibt an, dass der Quellcode ja von einer Version aus 2006 stammt. Aus meiner Sicht, und dies wird durch Anmerkungen im Quellcode absolut bestätigt, begeht auch Norton nicht den Irrsinn, bei jeder neuen Version den Code komplett neu zu schreiben. Dies wäre in den meisten Fällen wissenschaftlicher und wirtschaftlicher Unsinn und höchstens durch Vorfälle wie den jetzigen Quellcodediebstahl zu rechtfertigen. Große Anteile des Kern-Quellcodes aller entwendeten Produkte dürften damit in den aktuellen Versionen mit der Version 2006 übereinstimmen. Das erklärt auch die Reaktion von Symantec, die gegen die eigene Beschwichtigung spricht. Man empfahl, pcAnywhere vorerst nicht mehr einzusetzen. Man darf gespannt sein, wann und auf welche Weise der Quellcode für die anderen verbreiteten Security Suiten im Netz auftaucht. Derweil dürften sich die Hacker bereits an die Analyse der Quellen gemacht haben. Es bleibt spannend…

Siehe dazu ZDNet Australia

 