BREACH is the Word, is the Word, is the Word that you Heard….

Peter Silva, 2009-31-07

…to the tune of $6.6 Mil per-r-r Breach. Yup – according to Ponemon Institute the average cost of a data breach is $6.6 million and they also report that it costs about $215 per compromised record (pdf). McAfee estimates $1 trillion in losses yearly, due to data theft – that's 10 to the 12th dollars. Imagine if IT budgets could get that back?

The past two years saw a significant increase in large scale attacks with the January 2007 TJX breach starting the massive flurry. As of October 2007, TJX said that more than were 94 million accounts affected at a cost of over $256 million. At the time it was the largest data loss incident to date. The crooks kept it up, however. Hannaford Grocers was hit Dec 2007 but they didn't discover it until February 2008 and announced in March 2008 that 4.2 million cards had been exposed leading to over 1800 cases of fraud. In both cases thieves were able to capture the data, in clear text, as it traveled over the network. December 2008, at the height of the economic crisis, both Checkfree.com (online bill pay) and RBS Worldpay (payment processor) announced they had been infiltrated. Checkfree with a DNS switcheroo and RBS Worldpay with a straight up 'they broke in.' RBS had 1 million accounts compromised and Checkfree, 5,000,000. Payment card data was the top target in 2008.

Then at the start of 2009, instead of hitting individual retail chains, hackers decided to go after the big score – and boy was it. Heartland Payment Systems, which processes about 100 million credit card transactions a month was compromised and it unseated TJX as the largest breach ever in the US. This too was a case of malware planted on the network and thieves able to capture clear text data in transit. In addition to Heartland, initially over 220 issuing banks were affected by the breach and that grew to 656 by June 2009. The total number of accounts compromised is still unclear. The common theme in many of these breaches is that the hit companies were PCI compliant. Currently, PCI does not require encryption during transmission of sensitive data on internal networks – where most of these occurred. Ignoring the lawsuits, fines and bad press, the bright spot in all this is Heartland has instituted end-to-end encryption of all data (although some question the overall effectiveness) and has developed new equipment in the wake of the fiasco. This one is still playing out.

One stat I remember but can't remember the source (sorry for forgotten reference) is that 60 percent of companies had experienced a data breach in last year. However, only a minority of six percent could say ***with certainty*** that they had not experienced any such breaches in the past two years. Yikes.

ps

Previous blogs covering some of these:

- Another Breach, another F5 Solution
- Encryption Anywhere and Everywhere
- Time the Avenger (also a great Pretenders song)

The 'lost' paragraph - added Aug 2:
I meant to include this thought in the original post but forgot. The other silver lining in all this is that the companies that have been breached, and the above just got the most press, are probably more secure than they ever were. The breaches have made them more aware of their vulnerabilities and they have taken additional measures to ensure it doesn't happen again. While brands can suffer after public disclosures, one could argue that the experience & knowledge gained - post breach - actually puts them in a better, more secure position moving forward. ps

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com