Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Saving SMBs from data leakage

In a discussion at the Computer Forensics Conference, some of the folks who track these things indicated that, while few large businesses are killed off from major data breaches, this is not the case for SMBs, and we tend not to hear about them when they fail. According to this source, when there is a successful breach on a computer operated by a small business (e.g., a local coffee shop), and assuming the attack is detected and traced back to the SMB (e.g., several of their clients had credit card information uses illicitly and the common factor was their use of those credit cards at that coffee shop), the SMB is likely to go out of business.

What drives these SMBs out of business?

The effect of these attacks are multifaceted. There are breach notification requirements of different states to consider, and liability problems lead to purchasing some sort of insurance for those clients for the next year (credit reporting, putting change holds on their credit reports, notifying the other cardholders and their issuing agencies, etc.). In addition, they might lose customers, end up with legal fees, lose use of credit card processing, have to pay for forensics or investigations, and so forth. The likely cost is on the order of several hundred dollars per customer information leaked, and for many SMBs this will put them out of business. It also takes a lot of time, effort, and pain to get all of these things done, and most SMBs don't have the excess personnel to handle all of this.

It's really not their fault and should not be treated as if it were

The underlying problem is that SMBs are not in the computer security business nor should they be. They buy a point of sale (POS) solution and use a PC for record keeping. They use the Internet like anyone else. They might have a spreadsheet with customer data used to send periodic email for marketing, they use the computer to generate posters, papers, menus, place orders, process payments, and so forth. They don't have the realistic ability to be PCI compliant but can do the paperwork necessary to process credit transactions. They may have a Web site, and process credit cards there using vendor-supplied software set to the default operating mode by a menu system they entered a few pieces of data into, along with their list of items and prices. They cannot afford or support a computer services department, and even if they could, the workers are unlikely to defend against serious external attacks.

The solution

The solution for most SMBs is pretty simple. They don't run their own bank, shipping company, programming house, or flooring company, but they have bank accounts, shipping, software, and floors. They shouldn't have their own computer security department? Storage and processing of personal information can be readily outsourced, and should be, to companies that take liability for the data (which is harder to find). Backup copies in usable form should be available to protect the SMB from the outsourcer, and the SMB should be able to do what they need to do without having to hold personal, credit card, or other sensitive information and be put at risk. The 1-3% they pay for processing is a good deal.

