Hacking at small businesses

The Cost of a Data Breach

Most merchants and many of their service providers don't fully understand the impact of a data breach. Nor do they realize that most breaches are entirely preventable.

Data Breach of only 22 Credit Card Numbers "Cost Me My Dream"

One such unfortunate case is that of a restaurant in Bellingham, WA, that purchased a noncompliant payment application on eBay, lost credit card information in a hacker attack, and temporarily went out of business due to financial penalties.

1. **Fines: Visa and MasterCard: $7000**
2. **Forensic examination: $5000**
3. **Resolution time frame: 11 months**
4. **Business disruption: Processing rights revoked**

According to industry reports, hackers are expanding their data breach efforts to beef up exploits of small businesses that store data in electronic form. Small companies, many of whom have converted their card processing to electronic systems, have now become hackers' main target.

In 2010, the U.S. Secret Service and Verizon Communication's forensic analysis unit responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer. Visa USA estimates that 95% of the credit card data breaches impact its smallest business customers, which they refer to as "Level 4" merchants.

Smaller merchants have limited budgets and few or no technical experts on staff. They generally have weak security and cyber criminals understand this. They also have less understanding of data systems and the risks that they are subject to when holding personal data. Smaller merchants offer the least resistance, and hackers get more bang for their buck.

Mark Brady, former Director of Compliance for a large Independent Sales Organization (ISO), recalls one small merchant data breach he handled. "It wasn't pretty," says Mark. "In the end I felt a lot of compassion for the owner, who was out of business for several months due to the incident."

The merchant, a Bellingham, Washington, restaurant had purchased through eBay a noncompliant Micros payment application. The noncompliant application had previously been listed on a Visa Alert that identified the software as improperly storing cardholder data. "We regularly distributed these Visa notices to our sub-ISOs," said Mark, but unfortunately these communications are often not acted upon." The merchant had its computerized cash register hacked and criminals made several fraudulent charges on customer credit cards.

"We received a Common Point of Purchase (CPP) letter from Visa stating that 22 Visa cards that had previously been used at the merchant subsequently had fraudulent transactions at other merchant locations," according to Mark. Hence, the restaurant was the point of compromise– the theft of the card numbers originated at the merchant location.

Visa demanded an investigation of the merchant and his point-of-sale system. "That alone took several weeks to pull together," said Mark. "Then we were asked to arrange several conference calls with the card processor, the sub-ISO that had contracted with the merchant, the member bank and Visa. As you can imagine, setting up and preparing for these calls took a lot of my time, as well as that of the poor merchant. Additionally, by this time, the merchant had accessed the Visa CISP website and learned of the possibility of fines. On the last two calls with Visa and the member bank, the merchant became very contentious. I recall it becoming very uncomfortable and hard to handle," said Mark.

"On top of all of this Visa required a forensic investigation of the compromised payment application. We went through the long process of pricing forensic investigator services and arranging for the merchant site visit. The forensic exam found that there had been unauthorized access to the payment application. One interesting finding was the existence of American Express numbers in the system," said Mark. "The restaurant did not accept AMEX, so the card numbers must have already been in the system when it was purchased through eBay."

The forensic investigation ended up costing $5,000 (Note: Our understanding is that forensic investigations have significantly increased in cost over the last year, and are now running closer to $15,000 in cost).

After several more months of discussion with Visa and the bank, the fines were assessed; the Visa fine was $2000 and MasterCard was $5,000. "Another interesting thing was that, throughout the complete course of the data breach and investigation we heard not one word from MasterCard - except for the fine letter," said Mark.

Had the merchant been compliant with the card brand's PCI Data Security Standard, the use of the noncompliant payment application would very likely have been identified. The merchant would have upgraded to a compliant payment application and the card data would have been protected.

The merchant's ISO stopped processing card transactions and the restaurant was out of business until they could find a new provider, which proved difficult and expensive. While $12,000 might not sound like a large sum, it was enough to significantly impair a small operation, coupled with the inability to accept cards for several months.

Additionally, the ISO was forced to absorb about half of the total data breach costs due to lack of funds in the merchant's checking account.

The cyber-attack "cost me my dream," said the former owner. The hacker who stole the data was neveridentified.

"I was able finally to find the merchant another ISO because I felt so badly for him," said Mark. "I can guarantee the new processing arrangement includes a compliant payment application and full PCI Data Security Standard validation."

"In the end, with all of the administrative work, the conference calls, and the investigation, this one incident involved many man-hours for all involved. The timeline from receiving the Visa letter, processing the fines, and arranging for a new ISO made for a very difficult eleven months."

See the Wall Street Journal story at:
http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html?KEYWORDS=pci