Study Reveals 61% Store Unprotected Credit Card Information

Even with emerging technologies, new emphasis on security and new mandates in place, many of today's businesses are still struggling with the storage of unencrypted card data.

By Brand Barney, Security Analyst at SecurityMetrics

It's safe to say no retailer wants to be the next Target, Home Depot, or Neiman Marcus – all victims of some of the largest data breaches in recent history. However, many merchants might as well paint a bull's eye across their storefront and post the sign, "Hackers Welcome."

Recent breaches resulted in millions of compromised debit and credit cards, and the incidents, which may have been avoided by simple software upgrades, are costing some retailers millions. In spite of this reality, and with new breaches continuing to occur, a large number of retailers remain unfazed, satisfied, and falsely reassured with the thought that it won't happen to them.

What's most interesting is that many of these companies, both large and small, are storing unencrypted customer credit and debit card information unknowingly.

In SecurityMetrics' fourth annual study, card discovery tool PANscan®, a comprehensive system scan that checks for unencrypted payment card data, found that 61 percent of businesses currently store customers' 16-digit credit card numbers, also known as the Primary Account Number (PAN).

Compared to last year's study on unencrypted payment card data, this is a two percent decrease. So does this mean the outlook is brighter? Unfortunately, no. Considering the abundance of hacks publicized in the news in the last six months, the fact that 61 percent of merchants still store unencrypted payment data is actually quite surprising.

The study also examined data from over 3,600 computers, and found that there are currently:

- A total of 332,263,315 payment cards unencrypted on business networks;
- An average of 91,608 payment cards per computer; and,
- Seven percent of businesses that store full magnetic stripe data, including PIN, CVV, service code, expiration date, cardholder name, and PAN.

What you don't know *can* hurt you

There are many ways in which card details can remain on a business's IT infrastructure unknowingly. For example, transaction logs sent back from banks, browser caches, and email duplications can hold sensitive data and can be used by hackers to swindle consumers.

Another example can be seen in error logs – one of the most common places unencrypted credit card data is unintentionally stored. When an error occurs during card authentication or processing, an error log is often generated. These logs can contain full credit card data in plain text.

Most of the time, unencrypted credit card data isn't properly protected simply because the business isn't aware it exists. How can you protect what you don't know you have?

Unencrypted card data can be found in various departments across an organization. Accounting departments, for instance, typically have processes for charge reversals that may store unencrypted credit card data in files on employee workstations. Sales and customer service departments may have emailed or printed forms containing credit card numbers.

Something else to chew on

Many in the payments industry assume that once EMV terminals become mandated on October 1, 2015, they will solve the problem of unencrypted card data at the swipe terminal. Unfortunately, they're wrong.

EMV-enabled technology will be a great tool to assist in reducing fraud for card present transactions. However, even though this technology is advanced, EMV-enabled payment terminals can still be used to make a payment transaction using an optional magnetic stripe swipe process. In fact, in the first phase of EMV implementation, most terminals and cards will have the magnetic swipe as an option. This means there's still an opportunity for misconfigured hardware and software to inadvertently capture and store full track data. An attacker could purposefully exploit these vulnerabilities and steal the stored card data.

As banks start ramping for EMV implementation (sending chip-enabled cards to consumers, setting up processes to handle payments, etc.,) malicious entities will scramble to grab as much unencrypted card data as possible, resulting in a dramatic jump in fraud.

It's crucial these misconceptions be remediated sooner than later; business owners must understand that EMV technology isn't going to solve the overall issue at hand.

So, what's the solution?

First, it's important to understand that routine checks (to see if card data is being stored) should be as frequent as anti-virus checks. Next, IT departments need to realize that it's impossible to manually locate the data themselves.

Fortunately, there are a number of cutting-edge card data discovery tools available on the market that can locate unencrypted card data in a matter of minutes. Many of these solutions, like PANscan, can simplify the process of identifying and directing users to unencrypted card data.

Here are some tips on how your organization can better secure customer credit card data on your network:

- **Limit storage**. Set limits when it comes to storage of card data, and only do it when absolutely necessary.
- **Run software**. Utilize card data discovery software on your computer networks and servers frequently to expose unencrypted card data and identify storage sources.
- **Patch leaks**. Once storage sources are discovered, patch the leak as soon as possible.
- **Remove data**. Securely remove or encrypt discovered card data.
- **Don't just delete, erase**. After locating stored credit cards, merchants often try deleting this data by emptying their computer's trash icon. Emptying your trashcan doesn't actually permanently delete its contents. To actually delete, you need to erase

(repeatedly overwrite) the file from your disk drive. There are software programs created exactly for this purpose.

- **Schedule scans**. In addition to regularly scheduled internal and external vulnerability scans, run card data discovery software after any changes to your payment processes.

When working to secure a payments system, merchants must understand that the most secure payment method is point-to-point encryption, or P2PE. P2PE encrypts account numbers at the credit card terminal and sends the encrypted data directly to the payment processor for decryption.

P2PE actually eliminates the risk of a breach because cardholder data is never in a merchant's system, even from the start.

Storing unencrypted payment card data remains a very real threat that merchants must address now. By leveraging today's card data discovery tools, organizations can reduce their business liability as these solutions find unencrypted card data that must be securely deleted.

These solutions also can help businesses achieve accurate Payment Card Industry (PCI) compliance, as unencrypted PAN storage is against the PCI DSS (Data Security Standard). Once a scan is complete, the results can then be used to help validate compliance with data security requirements.

Unencrypted card data storage creates major liability for today's merchants, and even less work for criminals. Let's face it: No one wants to be the next company splashed across the headlines. Today's businesses must reduce their risks by locating unencrypted payment card data on their networks, especially if they want to avoid a major data breach.

Brand Barney is a Security Analyst for SecurityMetrics and holds CISSP,QSA, and HCISPP certifications. With over 10 years of compliance, data security, and database management experience in a number of industries, Barney is responsible for auditing and consulting companies on their data security and compliance and has a passion for sharing his knowledge to encourage other professionals to maximize their business security success.