PCI: A Four-Letter Word of E-Commerce

or:

How I Learned to Stop Worrying and Love the Standard

http://www.flickr.com/photos/shawnzlea/527857787/

PCI: A Four-Letter Word of E-Commerce

or:

How I Learned to Stop Worrying and ~~Love~~ Live With the Standard

http://www.flickr.com/photos/shawnzlea/527857787/

PCI: A Four-Letter Word of E-Commerce

or:

How I Learned to Stop Worrying and ~~Love~~ Live With the Standard

- **PCI** == **P**ayment **C**ard **I**ndustry
- We're talking about the PCI-DSS (Data Security Standard)
- Described with Many Words:
  https://www.pcisecuritystandards.org
- Not to be confused with the PA-DSS

PCI: A Four-Letter Word of E-Commerce

or:

How I Learned to Stop Worrying and ~~Love~~ Live With the Standard

“Why should I care. I don't do enough business to matter. It's not like anyone is going to catch little ol' me.”

-Some misguided merchant

Hackers breach Heartland Payment credit card system

Updated 1/23/2009 12:14 PM | Comments 80 | Recommend 90 E-mail | Save | Print | Reprints & Permissions |

By Byron Acohido, USA TODAY

Heartland Payment Systems (HPY) on Tuesday disclosed that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants.

Robert Baldwin, Heartland's president and CFO, said in a USA TODAY interview that the intruders had access to Heartland's system for "longer than weeks" in late 2008. The number of victims is unknown. "We just don't have the information right now," Baldwin said.

Tech security experts said the breach could set a record. Retail giant TJX lost 94 million customer records to hackers in 2007. With more than 100 million transactions per month, they could discover that several months' worth of transactions were captured, says Michael Maloof, chief technology officer at TriGeo Network Security.

Heartland processes card payments for restaurants, retailers and other merchants. It discovered the hack last week after Visa and MasterCard notified it of suspicious transactions stemming from accounts linked to its systems. Investigators then found the data-stealing program planted b thieves.

Share
Add to M
Facebo
Twitter
More
Subscribe
myYaho
iGoogle
More

seattlepi

Search seattlepi.com Web Search by YAHOO! Business

HOME LOCAL U.S./WORLD BUSINESS SPORTS A&E LIFE COMICS PHOTOS BLOGS

Personal Finance/Learnvest | Boeing/Aerospace | Microsoft | Business Wire | Tech Wire

Massive credit card data breach hits local banks, credit unions

WSECU says some customers affected

By JUDY VUE, P-I REPORTER
Published 10:00 p.m., Thursday, January 22, 2009

Comments (0)
Larger | Smaller
Printable Version
Email This
Font
0 tweets
tweet
0
Share

OLYMPIA -- Banks in Washington state are coming to with what has been described as one of the biggest cre data breaches ever.

Heartland Payment Systems Inc. -- the sixth-largest pay processor in the U.S. -- revealed this week that crimina installed spy software on its computer network.

Heartland, a corporation based in Princeton, N.J., that credit card and debit card processing to business locations nationwide, says it doesn't know hov

Sony Confirms Yet Another Credit Card Data Breach

By Phil Villarreal on May 3, 2011 7:30 AM

(Great Beyond)

As if it wasn't bad enough that 10 million credit card numbers may be at risk due to a hacker's takedown of PlayStation Network, Sony is also facing a data hemorrhage on another front. Sony Online Entertainment — maker of EverQuest — confirmed another data breach has left 12,700 non-U.S. credit card numbers and 10,700 bank account numbers exposed.

The Wall Street Journal reports the numbers came from a 2007 database, meaning many of the accounts may no longer be active. The hacker may have also nabbed users' names, birthdates, passwords and addresses.

SOE shut down its services Monday due to the breach, which has affected 24.6 million accounts. Between the

PCI: A Four-Letter Word of E-Commerce

or:

How I Learned to Stop Worrying and ~~Love~~ Live With the Standard

- More than 80% of the instances of unauthorized access to card data have involved small merchants

- These businesses account for 85% of the merchants

In Data Leaks, Culprits Often Are Mom, Pop
Wall Street Journal, 9/22/07

PCI: A Four-Letter Word of E-Commerce

or:

How I Learned to Stop Worrying and ~~Love~~ Live With the Standard

- The average total per-incident costs in 2009 were $6.75 million
- The most expensive data breach event included the study cost a company nearly $31 million to resolve.
- The least expensive total cost of data breach for a company in the study was $750,000.

U.S. Cost of a Data Breach Study.
PGP Corporation, and the Ponemon Institute,

@LiquidSullivan
Shaun Sullivan

If you have a Playstation 3, change all your passwords on all your Internet services. I already detected access from an IP in China on mine

28 Apr via web ☆ Favorite ↻ Retweet ↩ Reply


http://www.flickr.com/photos/in2thewoodz9/5061016510/

What does it mean?

“PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted.**”**

http://lb.cm/pci-applies

What does it mean?

“PCI DSS compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one.”

http://lb.cm/pci-myths

What does it mean?

Here's the bottom line:

Merchants should contact their processor (PayPal, Authorize.net, etc.) to determine how to proceed.

What does it mean?

- For a standard E-Commerce setup ('low' volume)
- Self Certify
- Annual SAQ A (13 Questions) or SAQ C (40 Questions) and the associated Attestation of Compliance.
- Quarterly network scans

Build and Maintain a Secure Network

Requirement 1:

Install and maintain a firewall configuration to protect cardholder data

- Establish firewall and router configuration standards
- Current network diagram with all connections to cardholder data
- A formal process for approving changes to the firewall and routers

Build and Maintain a Secure Network

Requirement 2:

Do not use vendor-supplied defaults for system passwords and other security parameters

- Always change vendor-supplied defaults before installing a system on the network
- Enable only necessary and secure services, protocols, daemons, etc.
- Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Protect Cardholder Data

Requirement 3:

Protect stored cardholder data

- Do not store sensitive authentication data after authorization (even if encrypted)
- (Sensitive data==Full Track, CV2, PIN)
- There's a right way to full CC #. I'ts hard. I don't recommend it.
- Other Requirements and suggestions for Data

Protect Cardholder Data

Requirement 4:

Encrypt transmission of cardholder data across open, public networks

• Use SSL/TLS, IPSEC, SSH, etc. to safeguard sensitive cardholder data during transmission over open, public networks.(The internet, wireless)

•Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

Maintain a Vulnerability Management Program

Requirement 5:

Use and regularly update anti-virus software or programs

Maintain a Vulnerability Management Program

Requirement 6:

Develop and maintain secure systems and applications

- Best practices for secure coding. (owasp … etc)
- Separation of duties between development/test and production environments
- Document processes for deployment/changes/backout procedures

Implement Strong Access Control Measures

Requirement 7:

Restrict access to cardholder data by business need to know

• Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities

Implement Strong Access Control Measures

Requirement 8:

Assign a unique ID to each person with computer access

Implement Strong Access Control Measures

Requirement 9:

Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10:

Track and monitor all access to network resources and cardholder data

- Log Stuff. (The actions of users with access to stuff)
- Know what time it is.
- Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis

Regularly Monitor and Test Networks

Requirement 11:

Regularly test security systems and processes.

- Perform quarterly external & internal vulnerability scans via an Approved Scanning Vendor (ASV)

Maintain an Information Security Policy

Requirement 12:

Maintain a policy that addresses information security for all personnel.

- Educate personnel upon hire and at least annually.
- You'll need an official policy for employee restroom breaks. (okay, maybe not, but you get the idea.)

Basic Principals

- Don't be dumb.
- Document Everything.
  If it's not written down, it doesn't exist.
- Don't store card data.
  (unless you're way cooler than us)
- Read. (I know...) The Docs are all on
  https://www.pcisecuritystandards.org/

Bed-time reading

- The Standard itself.
- Navigating PCI DSS
- Glossary of Terms, Abbreviations, and Acronyms
- PCI DSS Quick Reference Guide
- The Prioritized Approach to Pursue PCI DSS Compliance