



# PCI Compliance

by: David Koston

Simplify.

# PCI DSS

Payment Card Industry Data Security Standard

»» American Express

»» Discover

»» JCB

»» MasterCard

»» VISA

# Why?

- » Continue to do business
- » Retain Customers
- » Legal Standards are Coming!

Texas' House of Representatives voted 139-0 in favor of a bill that puts PCI requirements into a state law. **Under HB 3222 a breached entity will have to reimburse banks and credit unions the cost associated with blocking and reissuing cards if the merchant was not PCI compliant at the time of the compromise.**

- Is your state next?



## Disclaimer

I'm not a PCI Compliance Assessor or a member of the Payment Card Industry. This information is meant to be used for informational purposes in order to help those with a cPanel server become PCI compliant. No warranty of any kind is provided with this information. This information does not guarantee security or compliance of any kind. Follow the included steps at your own risk.

Simplify.

# The Standard

[https://www.pcisecuritystandards.org/tech/pci\\_dss.htm](https://www.pcisecuritystandards.org/tech/pci_dss.htm)

- »» Data Storage
- »» Information Security Policies
- »» Network and Server Security
- »» Securing a cPanel / WHM Server

# Data Storage

»» What data is stored

»» Data Security

# What to Store

## »» Store

- Primary Account Number

## »» You can store (must be protected)

- Cardholder Name
- Service Code
- Expiration Date

## »» Do Not Store!

- Full Magnetic Stripe
- CVC2 / CVV2 / CID
- PIN / PIN Block

## Protect Stored Data

- On all fronts
  - Physical Protection
  - Electronic Protection

All the encryption in the world won't save you if someone can waltz into your server room and access your stored card numbers.

# Physical Data Protection

- »» Need-to-know disclosures
- »» Secure Facility
  - Locks
  - Cameras
  - Cages
  - Visitor Log
  - ID cards
- »» Off-site, **secure** backups!

## Electronic Protection - Data

- »» Encrypt all traffic and all data
- »» Mask PAN when displayed
- »» Limit access to servers with secure data
- »» Dedicated data storage machines?
  - Drawbridge or stone hut?

# Information Security Policy

A strong information security policy is important so that all employees are aware of the sensitivity of stored data.

# Your Information Security Policy

- Easily Available
- Daily Procedures for Staff
  - Clear list of staff with access
  - Who can be trusted?
- Where can we put data, servers, etc?
- What software can be on these machines?
  - Workstation vulnerabilities
- Read-only data, no local storage
- **Audit your policies and procedures frequently**

# Network and Server Security

- »» Denying access
- »» Hello, Administrator!
- »» Where's that data going?
- »» 3<sup>rd</sup> Party Application Security
- »» Access Control
- »» Tracking and Testing

# Denying Access

## »» Firewalls

- Block all traffic
- Explicitly allow necessary traffic
- Don't forget the workstations!
- <http://www.cpanel.net/security/firewalls.html>

## »» Services

- Turn off all unused services

# Hello, Administrator!

Vendor supplied defaults are bad, mmmkay!

- »» Logins and passwords
- »» WEP keys
- »» Ports
- »» URLs

# Where's that data going?

- Simple network setups are easy to keep under wraps
- Does the data need to leave the subnet, the firewall, the DMZ?
- What other systems can locate or talk to the data storage system(s)?



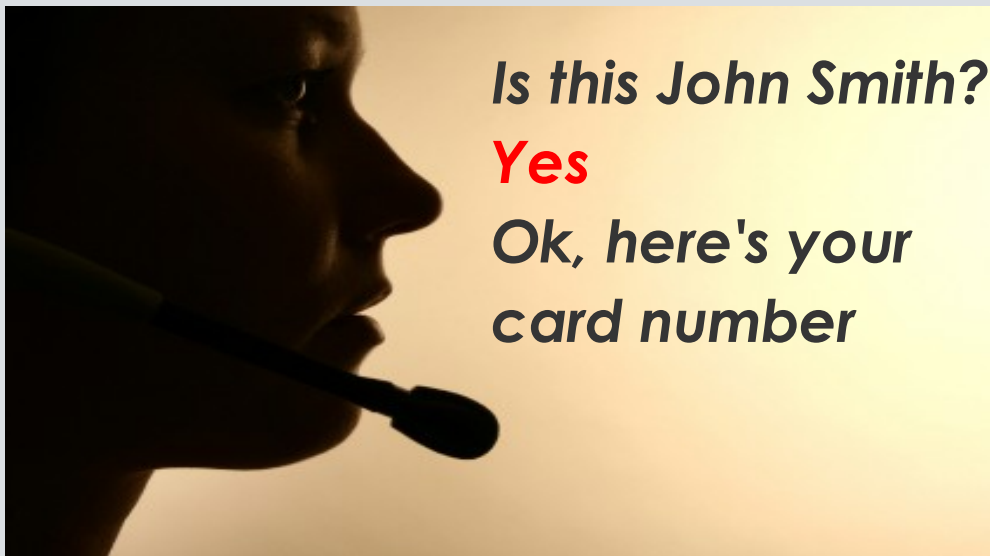
# 3<sup>rd</sup> Party Application Security

Research, Research, Testing, Testing, Research,  
Testing, Testing, Testing

Simplify.

# Access Control

- » All users must have unique logins
- » Easy vs. Secure
- » **Two-factor authentication**



## Tracking and Testing

- »» Log access, data transfer, system modifications, etc
  - Who, what, when, where from, where to, worked, and why?
- »» This is not a Ronco Showtime™ Rotisserie!
  - Testing, testing, and more testing!

# Securing a cPanel / WHM server for PCI DSS Compliance

- What to do after installation?
  - Lock down open ports
  - Shut off unneeded services
  - Restrict Service Access
  - All traffic over SSL
  - Turn off recursive BIND lookups
  - Turn off mod\_userdir
  - Use public key authentication for SSH
  - Other Measures

## Securing – Lock down open ports

➤➤ Limit open ports to those necessary

➤➤ Example APF configuration:

– INGRESS (inbound)

- IG\_TCP\_CPORTS="22,25,53,80,443,2083,2087,2096"

- IG\_UDP\_CPORTS="53,465"

– EGRESS (outbound)

- EG\_TCP\_CPORTS="25,37,53,80,113,465,2089"

- EG\_UDP\_CPORTS="53,465"

# Securing – Shut off unneeded services

WHM >> Service Configuration >> Service Manager

Turn off:

- Entropychat
- Interchange
- Melange
- Named?
- MySQL?
- FTP?



# Securing – Restrict Service Access

WHM >> Security Center >> Host Access Control

Restrict access to services such as SSH, FTP, MySQL, etc

Deny all traffic and only allow access from specific IP addresses

Simplify.

# Securing – All traffic over SSL

WHM >> SSL/TLS >> Change Server Certificates

➤➤ cPanel / WHM

➤➤ Exim

➤➤ Webmail

➤➤ Courier

➤➤ Apache too! (SSL Manager)

## Securing – Turn off BIND recursion

»» /etc/named.conf

»» Add the following lines to the options section:

```
Allow-recursion {"none"};
```

```
Recursion no;
```

```
#disables zone transfers
```

```
Allow-transfer {"none"};
```

## Securing – No mod\_userdir

WHM >> Security Center >> Apache mod\_userdir  
Tweak

➤➤ Enable mod\_userdir protection for all users

# Securing – Public Key Authentication

➤➤ 2 factor authentication – require a key and passphrase

- WHM >> Security >> Manage SSH Keys
- Create and Authorize your key
- Disable Password Authentication
  - WHM >> Security Center >> SSH Password Auth Tweak
- cPanel >> SSH/ Shell Access >> Manage SSH Keys



# Securing – Public Key Authentication

For detailed instructions:

<http://www.cpanel.net/security/publickeyauth.htm>

Simplify.

## Securing – Other Measures

- » Separate your services
  - Remote MySQL server on local subnet
  - Remote DNS only, no local BIND

## Securing – Other Measures

### »» cPAddons

- Limit Usage
- Keep up to date
  - WHM >> Manage cPAddons >> Upgrade all installs that need it
- Research and contact

## Caveats

- OpenSSL
  - 0.9.7a-43.16
  - Upgrade to 0.9.8??

## Next Steps

»» Contact an assessor

– ScanAlert

[www.scanalert.com](http://www.scanalert.com)

<http://www.scanalert.com/content/webhost/?hostId=4378>

Simplify.



Questions??

Ask Away!

Simplify.