Case Study: Protecting PCI Data in an Ecomm/Catalog Environment

Tim Alten – AmeriMark Direct June 2017
Agenda

- Disclaimer
- Background
- The pieces.....
Disclaimer

- While you should get some value or at least be entertained by this presentation YMMV if you apply any concepts or ideas to your environment
- This information isn’t supported by AmeriMark Direct, Progress Software or anyone else
Company Overview

- AmeriMark Direct LLC is a consumer goods retailer advertising through mailed catalogs, email campaigns, Ecommerce sites and various print media.
- Primary catalog titles include Anthony Richards, Healthy Living, FeelGoodStore, TimeForMe, Beauty Boutique, Windsor Collection, Essentials and Complements.
- Products include apparel and accessories, shoes, health products, small home goods, cosmetics, jewelry, AsSeenOnTV items, etc.
- Lots of value oriented product – some higher end in certain catalogs
- Customers are mostly women – generally mature demographic
- Typical orders 2 -3 items totaling $30 - $70 dollars
Order Channels

- Today customers order via mail form (40+%), call center (30+%) and web (20+%).
- Ecommerce sites:
  - www.timeformecatalog.com: Features TimeForMe catalog items
  - www.beautyboutique.com: Features BB catalog items
  - www.feelgoodstore.com: Features FeelGoodStore catalog items
- Some items also sold on Amazon
Presenter

- Tim Alten – IT Infrastructure Mgr / Sr Systems Analyst
- Why I might have something to say:
- Renaissance man - hands on:
- Programming 1990 – approx. 2001
- IT and Datacenter Infrastructure: 1996 – Present
- Sr DBA – 1990 - Present
- Networking and firewall guy....
- Sysadmin, OE installations and configuration
- Architecture and design....
- Responsible for PCI Compliance......
Key concepts:

- PAN = Primary Account Number is defining piece to determine PCI applicability
- Encrypt data at rest and in transit
- Limit access to data
- Segregate data to reduce compliance scope and aid protection
PCI Compliance – the beginning

- Begin working on 2010??
- Four levels of merchant – We are level 2 with 1 million – 6 million transactions per year on any 1 card brand – ex. VISA
- Level 1’s require certified PCI audit – rest can self-assess
- Evolutionary – continuous adjustment process
- First passing self-assessment June 2011 v1.0
PCI Compliance - Initial changes / needs

- Separate CC related zones from other stuff with firewall zones to protect and minimize scope
- Open public accessible access must stop in DMZ – no direct access to internal zones
- First focus on servers and CC database storage
- Step 1 - separate PPS / PPS DR in to separate zone
Initial PCI changes - continued

- Want to move CC out of order header table on PPS to protect it
- Also need to encrypt with industry standard encryption ex. AES
- OE DB TDE doesn’t exist yet, but language has AES encryption recently added
- Discussed ideas with Mike Jacobs PSC
- Add BehindCCINT network zone
- Install firewall that only allows traffic out from BehindCCINT
- Add network connections from PPS / PPSDR to private subnet connecting to firewall
Initial PCI changes - continued

- Add Linux system with OE databases – GILL
- data database has table with AES encrypted CC #, tie-id ex. order #, shopcart #, encryption key id - users include IT Operations
- key database has table with key-id, AES encrypted encryption keys
- encryption keys are encrypted using human entered passphrase as encryption key
- human passphrase is split knowledge – 3 IT staff know 1\textsuperscript{st} half, 3 IT staff know 2\textsuperscript{nd} half
Initial PCI changes - continued

- On PPS create new database for momentary CC storage – limited users – restricted OS security
- momentaryCC db table has AES encrypted CC and tie-id ex. order-no
- set up appservers to accept CC# and tie-id and store in records in momentaryCC db table
- change local character OE to pass entered CC to Appserver
- change Ecomm web servers to pass CC over to SSL encrypted Appserver
- batch program on GILL connects to databases there locally and client-server SSL to momentaryCC db on PPS – continuously scans for momentary CC records, pulls data over to GILL and deletes momentary CC record
- momentary CC record AES encrypted with hard-coded keys known to Appserver programs and GILL batch programs
Initial PCI changes - continued

- Result – CC are immediately separated from customer info making tying data together way more difficult
- No network connectivity in to long term storage system – firewall prevents incoming traffic
- New encryption keys can be created periodically and instituted for proper key rotation
- Use database trigger to create audit record to record when long term record is read, by what program and user
Initial PCI changes - continued

- How to use CC data?
  - PPS creates bank file for batch processing with sanitized XXXX1234 version of credit card, customer information and tie-id ex. order #
  - Computer Operations logs on to GILL system, runs scripts/programs to pull over bank file, read file look up CC using order #, rewrite file with full CC#, encrypt file with bank’s public GPG/PGP key and push file back over to PPS
  - Computer Operations logs on to PPS and SFTPs file using script to bank, script removes populated bank file from PPS
  - For answers back from bank file is GPG/PGP encrypted with our public keys – file is pulled to GILL – decrypted with our private key – processed to sanitize CC# - pushed back to PPS
  - lots of use of SUDO and shell scripts!
Initial PCI changes - continued

- All employees get ID badges – Computer room access controlled by ID badge swipe
- Employees handling CC need background check, IT background + credit check
- Multiple video cameras monitor computer room, recordings not under IT control
- Added SNORT listeners in DMZ, CCINT, BehindCCINT to meet requirements for IDS
- Use Tripwire Enterprise Server to monitor select files on PPS, Webservers, Development systems, etc. for FIM (File Integrity Management)
- Need a SIEM to collect logs, automate alerts and provide clean store for 1 yr retention – Add Arcsight logger with PCI module
- Send logs from PCI systems, firewalls, switches, etc. to Arcsight
- Do quarterly Nessus scans with Nessus Professional ($1200/yr -1 laptop) on all PCI zones
Initial PCI changes - continued

- Have McAfee Secure perform quarterly ASV scans on external IPs for security issues
- Daily McAfee scans also find input sanitization issues, cross-site scripting, etc.
- Hire local firm – Hurricane Labs to do periodic internal and external pen testing
- If pen testers don’t find creative, meaningful issues GET NEW PEN TESTERS!
Let’s look at some code

- ..........................
Other tricks

- For command line `_progress` startups want to hide password information

- `stty –echo  ## turn off echo`
- `read db1pass`
- `stty echo  ## turn echo back on`
- `_progress –db db1 –U $db1user –P $db1pass –p sec-save.p`

- `ps aux |grep _prog`
- `_progress –db db1 –U tim –P -p sec-save.p`
2013 – You thought PCI was bad before......

- MasterCard requires Level 2 merchants have full audit in addition to Level 1
- PCI versions now on V2.0 with more requirements
- AMK hires Halock Security to help with formal risk assessment and do PCI audit – cost approx. $40,000
- Lots of work on more formal policies, standards, procedures
- Tighten up all over........
2013, 2014 More PCI changes

- Protect Order Entry / Customer Service reps with network segregation behind firewall
- Create NOCCSAFE zone for key control/auth servers ex. DNS, NTP, AD for CS, WSUS patch server, Sophos AV server
2015 – More PCI and security turmoil

- V3.0 spec out – LOTS more documentation required
- SSL3 not safe – Implement OE 11.3.3HF013 internally on PCI systems and switch internal OE encrypted communications to TLS1.0 – no more SSLv3
- TLS1.0 needs to be replaced by TLS1.2 soon
2016 Finally OE 11.6

- Switch internal OE TLS connections to TLS1.2 only
- Better TLS1.2 encryption with SHA256 needs better certificate
- Generate certs on Linux and move to AIX – AIX openssl did not make format needed by OE
- Also:
  - Revise Apache web servers to use TLS1.2 only instead of TLS 1.0
  - Late 2016 begin replacing EOL Arcsight logger with Splunk solution
2017 Need Real Time Authorization

- Now need to authorize CC when order is received
- Use HTTPS call to payment processor
- Hold CC and CCV code in memory until auth attempt completed
- NEVER WRITE CCV CODE TO DISK – ONLY CC CAN BE STORED
- Web customers can have stored CC on file in long term
- Set up appserver on long term storage and make calls to it from PPS to retrieve CC and make authorization call
Thanks for attending!

- Hope you enjoyed!
- Questions??