SRC Security Research & Consulting GmbH

Manuel Atug

Security in the cardholder data processing?!

Agenda

- SRC and PCI
- Motivation of and what is PCI
- Experiences and lessons learned when conducting PCI Security Scans and PCI Security Audits

SRC and PCI

- SRC was first company worldwide accredited according to SDP und AIS at both payment scheme
- Cooperation with acquirers
  - B+S Card Service GmbH
  - ConCardis GmbH
  - Lufthansa Airplus (Acceptance) GmbH
  - Pago eTransactions GmbH
  - Israel Credit Cards Ltd.
- ~ 3.000 merchants, 35 service provider in Germany, Austria, France, UK, Russia, Ukraine, Slowakia, Israel

Motivation of and what is PCI?

Captain E.J. Smith, 1911:

„If somebody asks me about my experiences within 40 years on the sea, I would answer: unevenful. Of course there were some hurricanes, windstorms, fog and others, but was never close to any incident. Neither I have never seen a derelict or shipwrecked, nor I was close to any incident that could have ended in a catastrophy.“

15 April 1912
Captain: E.J. Smith

Fallacious security

- Normally there is only little experience available for risks, that realize rarely.
- The past does not provide any clue about what will happen in the future.

The risk (of being compromised) is underestimated!

Examples ...

Federal Bureau of Investigation
Los Angeles Division

DATE: December 15, 2006

FBI Advises Victims of UCLA Computer Intrusion to Report Fraud to the FBI's Internet Crime Complaint Center

On December 12, 2006, UCLA alerted approximately 800,000 individuals that their names and certain personal information contained in a restricted database had been illegally accessed by a sophisticated computer hacker. This database contained certain personal information, including Social Security numbers, dates of birth and home addresses, regarding current and some former UCLA students, faculty and staff, some student applicants and some parents of students or applicants who had applied for financial aid.

The FBI has initiated an investigation into the illegal access of the computer network at UCLA to determine those responsible, the extent of the computer intrusion and potential related criminal activity.

The FBI is urging anyone who was notified by UCLA that their information has been compromised and who believe they may have been victimized further by identity theft or by other fraudulent means to contact the FBI's Internet Crime Complaint Center and submit an online report. Individuals submitting reports should clearly indicate the nature of their affiliation with UCLA including their department, major, position, the month and year of their initial affiliation with UCLA and, if applicable, the date that affiliation ended. The reports should also include information as to whether or not the complainant has had his/her identity stolen or has been the victim of other identity-related fraud since June 2005. All reports submitted will be analyzed and follow-up action taken where appropriate.

(credit cards compromised @ University of California/Los Angeles [UCLA])

Examples ...

AT&T Offers Credit Monitoring Service to Customers Whose Credit Cards Were Accessed

San Antonio, Texas, August 29, 2006

AT&T Inc. today said that unauthorized persons illegally hacked into a computer system and accessed personal data, including credit card information, from several thousand customers who purchased DSL equipment through the company's online Web store.

The unauthorized electronic access took place over the weekend, was discovered within hours and the online store was shut down immediately. AT&T also quickly notified the major credit card companies whose customer accounts were involved. The company is also working with law enforcement to investigate the incident and pursue the perpetrators.

Customer notifications are ongoing by email, phone and letter to fewer than 19,000 customers. In addition to notifying those customers who were affected, the company will pay for credit monitoring services to assist in protecting the customers involved.

"We recognize that there is an active market for illegally obtained personal information. We are committed to both protecting our customers' privacy and to weeding out and punishing the violators," said Priscilla Hill-Ardoin, chief privacy officer for AT&T. "We deeply regret this incident and we intend to pay for credit monitoring services for customers whose accounts have been impacted. We will work closely with law enforcement to bring these data thieves to account."

Customers who have been affected have been provided with a toll-free number to call for more information.

(19.000 credit cards compromised @ AT&T)

Examples ...

U.S. Department of Defense
Office of the Assistant Secretary of Defense (Public Affairs)
News Release

DoD Announces Detection of Intrusion into TMA Files

The Department of Defense announced today that routine monitoring detected unusual activity on one of the TRICARE Management Activity's (TMA) public servers.

Investigation of the activity led to the discovery that an intrusion had occurred and information was compromised.

William Winkenwerder Jr., the assistant secretary of defense for health affairs, said the department's response was swift but focused. "As a result of this incident, we immediately implemented enhanced security controls throughout the network and installed additional monitoring tools to improve security of existing networks and data files," he said. "Such incidents are reprehensible, and we deeply regret the inconvenience this may cause the people we serve."

Information contained in the accessed files varied, and investigators do not know the intent of the crime or if any of the information will be misused.

TMA has sent letters to affected individuals advising them of the incident and that the compromise of their personal information may potentially place them at risk for identity theft. Additional information has been provided to assist them in understanding the potential risks and precautions they can take to protect their identities.

The Defense Criminal Investigative Service is participating in the investigation.

(14.000 credit cards compromised @ Department of Defense DoD)

Examples ...

Beginning in September 2005 and continuing through December 7, 2005, a hacker exploited the failures set forth in Paragraph 8 by using SQL injection attacks on respondent's website and web application to install common hacking programs on respondent's corporate network. The hacking programs were used to find sensitive personal information, including credit card numbers, expiration dates, and security code numbers, stored on the corporate network and to transmit the information over the internet to computers outside the network. As a result, the hacker obtained unauthorized access to information for thousands of credit cards.

(3.800 credit cards compromised @ Guidance Software, developer of the forensik Software Encase)

.. and consequences

- **Example merchant**
  - 250-300 transactions per month
  - card data storage of the last 3 years
  - 10.000 compromised cards
- **Costs**
  - Incident Fee: € 50.000
  - + Issuer Recovery Fee: € 50.000 (€ 5-15 per reissued card)
  - + Fraud: € 20.000.000 (~ € 2.000 per card)
  - + costs litigation ??
- **Loss >> 20 million EURO** (not including reputation)

Answer

- MasterCard Site Data Protection (SDP) since 2002 and Visa Account Information Security (AIS) since 2001
  - Self Assessment Questionnaire
  - Security Scan
  - Security Audit
  - Levels, deadlines, penalties
- Agreement of the requirements and foundation of Payment Card Industry Data Security Standard (PCI DSS) maintained by PCI Security Standards Council (PCI SSC) since September 2006

PCI Data Security Standard

- 12 PCI Data Security Requirements
  - structured into 6 areas
  - Version 1.1 dated September 2006
  - applicable to „*Member, merchant, service providers that store, process or transmit cardholder data*“

PCI Data Security Requirements

- 12 PCI Data Security Requirements
  - *Build and Maintain a Secure Network*
    - R1: Install and maintain a firewall configuration to protect data
    - R2: Do not use vendor-supplied defaults for system passwords and other security parameters
  - *Protect Cardholder Data*
    - R3: Protect stored data
    - R4: Encrypt transmission of cardholder data and sensitive information across public networks
  - *Maintain a Vulnerability Management Program*
    - R5: Use and regularly update anti-virus software
    - R6: Develop and maintain secure systems and applications

PCI Data Security Requirements

- 12 PCI Data Security Requirements
  - *Implement Strong Access Control Measures*
    - R7: Restrict access to data by business need-to-know
    - R8: Assign a unique ID to each person with computer access
    - R9: restrict physical access to cardholder data
  - *Regularly Monitor and Test Networks*
    - R10: Track and monitor all access to network resources and cardholder data
    - R11: Regularly test security systems and processes
  - *Maintain an Information Security Policy*
    - R12: Maintain a policy that addresses information security

Links

- PCI Security Standards Council Website
  www.pcisecuritystandards.org
- Visa EU AIS Program Website
  www.visaeurope.com/aboutvisa/security/ais/main.jsp
- MasterCard SDP Program Website
  www.mastercard.com/us/sdp/
- Visa USA CISP Webseite
  www.visa.com/cisp
- Paper, see 23C3 Proceedings or
  http://events.ccc.de/congress/2006/Fahrplan/attachments/1163-23c3Security.in.the.cardholder.data.processing.Paperv1.2.pdf

Experiences and lessons learned when conducting PCI Security Scans and PCI Security Audits

Experiences in general

- CVC2/CVV2 is stored after authorisation (not allowed at all)
- Full mag stripe data is stored after authorisation (not allowed at all)
- Systems are poorly managed and maintained
  - Approx. 2/3 fail to pass first PCI Security Scans due to significant vulnerabilities
  - Approx. 1/3 fail to pass re-scan
  - Irrespective of number of transactions or size of organisation!

Experiences and lessons learned when conducting PCI Security Scans

- X Display Manager Control Protocol (XDMCP) available
- running IRC Server
- Running Bittorrent, Amule and eDonkey
- SSLv2 protocol still active (only SSLv3 / TLSv1 allowed)
- SSL supports weak encryption (<128 bit)

Experiences and lessons learned when conducting PCI Security Scans

- Management Interfaces accessible on Cisco devices
- Webserver vulnerable to cross-site scripting
- Session-Fixation / session hijacking possible
- Webserver uses plain-text form based authentication
- Mail server accepts plaintext credentials

Experiences and lessons learned when conducting PCI Security Audits

- Key Management
  - Two consecutive encryptions rather then split key and four eyes principle
  - Split key/four eyes principle in processing environment, but generation and storage of the key handled by one employee
- Former patch providing masked PAN when displayed (6xxx4) reverted by new patch
- No shared account available but only one individual account existent. What about the substitute administrator?
- Deletion instead of wiping sensitive data

Experiences and lessons learned when conducting PCI Security Audits

- Single, company-wide intranet without segmentation, ~600 employees and visitors (meeting rooms) can access all servers, hosts and mainframes
- Development and productive environment on one system
- Physical audit trail didn‘t contain any entry within the whole last year (ideal remote administration and no hardware problems?)
- Backup tapes located at a third party without contract or policy

Experiences and lessons learned when conducting PCI Security Audits

- No system hardening:
  - compiler collection on database systems
  - Many different editors on database systems
  - Running inetd on productive systems
  - Software e.g. wget on productive systems
- No system maintenance:
  - SuSE / Red Hat / Debian / Windows NT distributions still in use, but no security patches available
  - Patches not installed:
    - „we will to do that (soon)™“ vs. „never change a running system™“

Experiences and lessons learned when conducting PCI Security Audits

- Full PAN within log files
  - forgotten to filter them
  - filtered GET requests, but forgot POST requests
- CVV2/CVC2 within database
  - After changing process to not store cvv2, ~500.000 forgotten former stored cvv2 found in database
- Storage of full Track2 data (magstripe) when transaction processing is interrupted (this was the big issue at Card Systems in USA)
- No deny all rule within the firewall rule set
- Historic firewall rules are still productive

Experiences and lessons learned when conducting PCI Security Audits

- Using real cardholder data on development system for testing and QA, but no patch management of the development system
- „Testing“ of new patches and releases with real cardholder data from an employee
- High secure data centre, but chargebacks handled on an employees workstation with Microsoft Access which contains some million transaction data without encryption
- No cross-cut shredder available (dumpster-diving)

Experiences and lessons learned when conducting PCI Security Audits

- Side wall of a rack could be opened using two plastic levers which have no lock, full access to the servers was possible
- Two racks next to each other, one higher then the other and no side wall on the higher one, access to the patch pannel was possible
- Rack was open on the back side, as the servers were longer then the rack and therefore couldn‘t be closed anymore

Experiences and lessons learned when conducting PCI Security Audits

- „We need no policies, it‘s all inside my head“
- „We never faced an incident since $years...“
- „We don‘t deal with shoes, of course we are secure“
- „This system is running since more than $number years, we can not touch this running system“
- „I am the CEO and of course need full access to cardholder data“
- „We are secure“

Contact

SRC
Security Research & Consulting GmbH
Graurheindorfer Str. 149a
53117 Bonn

Tel. +49-(0)228-2806-139
Fax: +49-(0)228-2806-199
E-mail: manuel.atug@src-gmbh.de
WWW: www.src-gmbh.de