Payment Cards Processing at UNL

VOLUME 2, ISSUE 2 MAY, 2008

University of Nebraska —Lincoln
Bursar's Office

Common PCI DSS Violations

Per the February 2008 SAQ documentation issued by the PCI Security Standards Council, investigations after compromises revealed that some of the most common PCI DSS violations were:

- Storage of magnetic stripe data (Requirement 3.2). It is important to note that many compromised entities are unaware that their systems are storing this data.
- Inadequate access controls due to improperly installed merchant POS systems, allowing hackers in via paths intended for POS vendors (Requirements 7.1, 7.2, 8.2, and 8.3).
- Default system settings and passwords not changed when system was set up (Requirement 2.1).
- Unnecessary and vulnerable services not removed or fixed when system was set up (Requirement 2.2.2).
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the web site (Requirement 6.5).
- Missing and outdated security patches (Requirement 6.1).
- Lack of logging (Requirement 10).
- Lack of monitoring (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems) (Requirements 10.6, 11.2, 11.4 and 11.5).
- Lack of segmentation in a network, making cardholder data easily accessible through weaknesses in other parts of the network (e.g., from wireless access points, employee e-mail and web-browsing) Requirement 1.3 and 1.4).

While UNL does not store any cardholder data, we still need to look closely at our processes to ensure that we are not vulnerable to compromise in any of these areas.

Welcome to our newest merchant!

The ***International Quilt Study Center and Museum*** *opened their new facility on Sunday, March 30th.*

To learn more:

www.quiltstudy.org/

Terminology

Consumer —Individual purchasing goods, services, or both.

Non-Consumer User —Any individual, excluding consumer customers, that accesses systems, including but not limited to employees, administrators, and third parties.

Procedure —Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.

Information Security — Protection of information to insure confidentiality, integrity, and availability.

Information System — Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Access Control — Mechanisms that limit availability of information or information processing resources only to authorized persons or applications.

University of Nebraska —Lincoln
Bursar's Office

121 Canfield Administration Bldg
Lincoln, NE 68588-0412

Phone: 402-472-1734
Fax: 402-472-2959
E-mail: bursar@unlnotes.unl.edu

The Office of the Bursar is responsible for administering the University of Nebraska-Lincoln money handling policies and procedures. Don't ever hesitate to contact us with any receipting questions you may have.

Security Reminders—More on PASSWORDS

8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
- 8.5.1 Control addition, deletion, and modification of user Ids, credentials, and other identifier objects.
- 8.5.2 Verify user identity before performing password resets.
- 8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.
- 8.5.4 Immediately revoke access for any terminated user.
- 8.5.5 Remove inactive user accounts at least every 90 days.

For advice on creating passwords, go to: **www.unl.edu/security/passwords.html**

Staffing Change

Brent Adams is no longer with Enterprise Information Services (EIS). His duties in regards to credit card processing at UNL will now be handled by Zac Reimer. Brent was previously our technical support and network scan contact. Please contact Zac Reimer, Network Security Analyst -EIS, with any questions you may have in these areas. Zac will also continue to be our contact for server security. Zac can be reached via email at zreimer2@unl.edu or by phone at 472-4826.

2008 Self-Assessment Questionnaire

The Self-Assessment Questionnaire (SAQ) has been updated for 2008 reporting. This year's SAQ has been broken out to identify which questions are applicable to each type of merchant. This resulted in four different questionnaires — A, B, C, and D. The questions are the same on each questionnaire. It's just that some merchants may only need to respond to 11 questions while others may need to complete all 200+ questions. The new SAQ's are available for review on the PCI DSS web site at:

www.pcisecuritystandards.org

We have completed an SAQ with eight departments so far this year. These are being completed as we do our site visits. We will continue these visits throughout the remainder of the year. We've enjoyed getting to know your department's in more detail and look forward to visiting the remaining departments in the coming months.