PCI DSS Compliance ASA On-Site Summary

- for -

University of Oregon

3 November 2017
Summary
CampusGuard conducted an on-site review of three areas at University of Oregon on 3 November 2017. This is a summary of the visit and findings of each merchants’ PCI compliance status.

Parking
In addition to the current payment processes in the parking office for citation and parking passes, the parking office has pay stations located in the various lots and spaces around campus. For parking lots, UO uses Luke pay stations from T2 Systems. These devices are connected using a segmented network run to each pay station. Parking is looking to replace the current Luke pay stations with Luke II pay stations purchased from the City of Eugene. These new stations will use a cellular connection and therefore Parking will no longer need to provide a segmented and secured connection and no vulnerability scanning or penetration testing will be required.

Parking also employs Park Mobile for customers to complete parking transactions. This solution is web based and the user may add time as needed using a mobile application without having to go back to the parking space. No technical infrastructure is required to use this solution so none of the UO network is in PCI scope for this solution.

The parking office has added 280 meters for individual parking spaces around campus. These meters all contain a cellular modem for connectivity to process credit card transactions. These devices use unattended card readers and are built to withstand tampering. CampusGuard does recommend that Parking set a schedule to inspect these devices on either a regular interval or upon some other interaction with the devices. If setting a regular schedule, we suggest that each reader is checked at least quarterly. Inspection should include not only the card reader but also checking serial numbers to ensure they still match the inventory.

Parking also maintains a parking lot with an Amano McGann exit station. This device currently has a card reader that scans payment information and sends it to the iParc application. Once handed off to the iPark application, the credit card data is then sent using TLS to the payment gateway for processing. The concern is the connection between the card reader and the payment application. There are other devices that share this network segment behind the iParc application. The ideal setup for this process would include a card reader that, at least, performs encryption at card swipe or at most encrypts card data before it leaves the AMG Exit Station. CampusGuard received a diagram showing how data flows from the various AMG models and Parking should verify that card data is encrypted from the AMG Exit station to the iParc application. This can be done by running wire shark or some other packet capturing software to see what is leaving the AMG pay station. Once it is verified that the data is encrypted, Parking should be able to rest assured that plain text card data is not being transmitted across any part of the network.

For all of these parking solutions, ensure that an attention of compliance is obtained from IPS, T2, and Park Mobile. These are all handling credit card data either on behalf of UO or as a service against a UO merchant ID.
Oregon Bach Festival
The music department uses a tablet based solution to conduct an auction. Talech, supported by Elavon processing, uses an external Ingenico iCMP PIN pad to collect all credit card data. This device allows entry via magnetic stripe, a chip reader, or manual.

Validation for this can only be done using SAQ C, but only answering questions that are found in SAQ B. To ensure the most security using this device, update procedures stating that all transactions are completed only using the iCMP PIN pad and that no credit card data is ever written to complete any transaction. Also include in the procedures that the device is inspected prior to use. The PIN pad should show no sign of tampering and the inventory should match the serial number on the device.

Athletics Ticketing
Ticketmaster has completed the installation of the VX820 PIN pads used over the Archtics remote session hosted by Ticketmaster. The devices encrypt all data entered either manually, from a chip, or from a magnetic stripe.

Credit card acceptance include card present and card not present processing. Credit card information may be received over the phone. The order would be directly entered into Archtics or collected on paper and handed to a ticket processor to enter. Once the order is completed, the payment information may be blacked out or it may be blackout and put into the shred bin. Orders may also be accepted from a standalone fax machine or received in the mail. Information from these order forms are also entered into Archtics, the payment information is redacted, and then the order form is stored.

CampusGuard recommends that processes are updated to include the requirement to regularly check PIN pads to ensure no tampering or substitution has occurred. We recommend that these devices are checked before its first daily use. An update of procedures should also include how to use the PIN pads in conjunction with Archtics that details how UO Athletics uses the software and hardware to process a payment.

As a means of validation, when Iron Mountain comes to empty the shred bins that contain any sensitive data such as credit card information, someone should witness the on-site destruction verifying that it has in fact been destroyed. This will satisfy the PCI DSS destruction requirement.
Summary
Progress has been made to increase security, and there are still some areas require attention to reduce the risk of losing credit card data. CampusGuard will continue work with University of Oregon to move closer to full PCI compliance. Some items are administrative such as policy and procedure, and others are technical such verifying what data is being passed across the network and documenting that sensitive data is indeed properly encrypted on a data flow diagram.

CampusGuard thanks University of Oregon for taking the time to have us come out and evaluate the payment card processes, procedures, and technical implementations. It is a pleasure to work with you. We look forward to an ongoing relationship.

Jarvis Gilmore, CISSP, QSA
Security Advisor
CampusGuard